Microsoft.AZ-700.vSep-2024.by.Yande.135q

Number: AZ-700
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: AZ-700
Exam Name: Designing and Implementing Microsoft Azure Networking Solutions

Case

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question. Overview

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

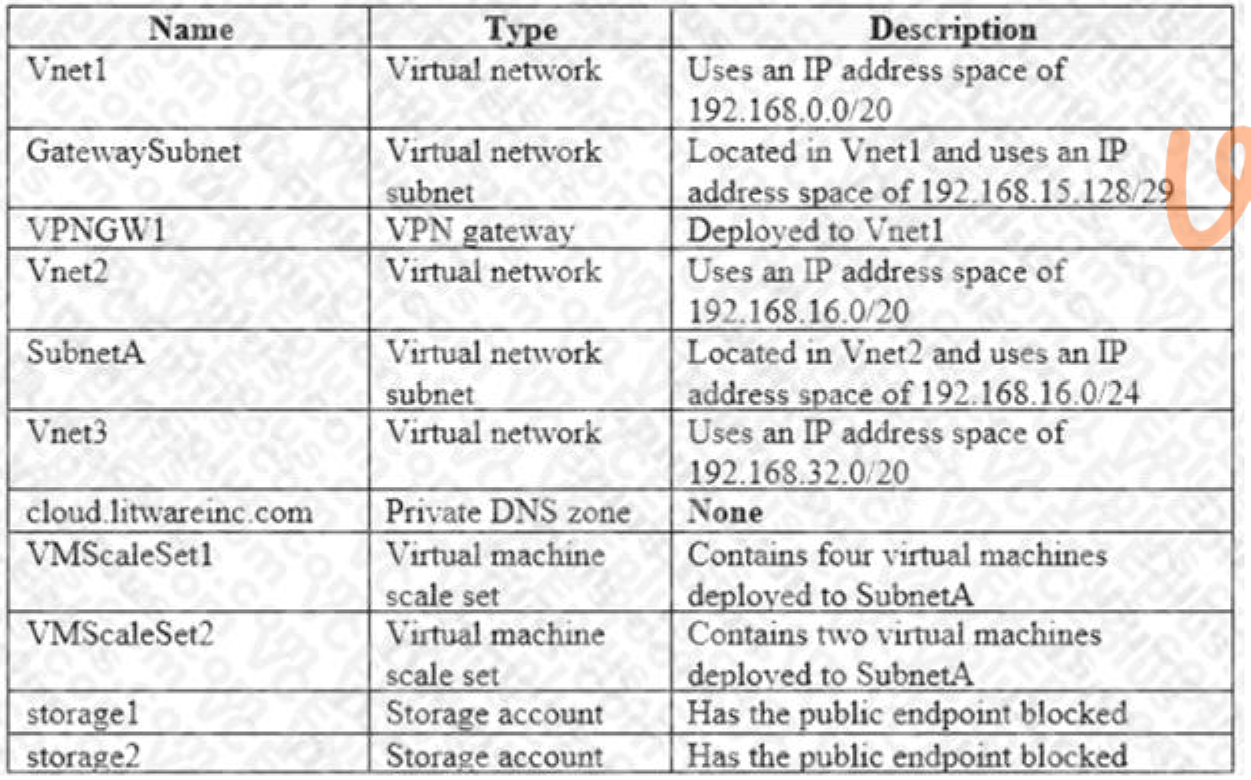
Existing Environment

Hybrid Environment

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect. All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment

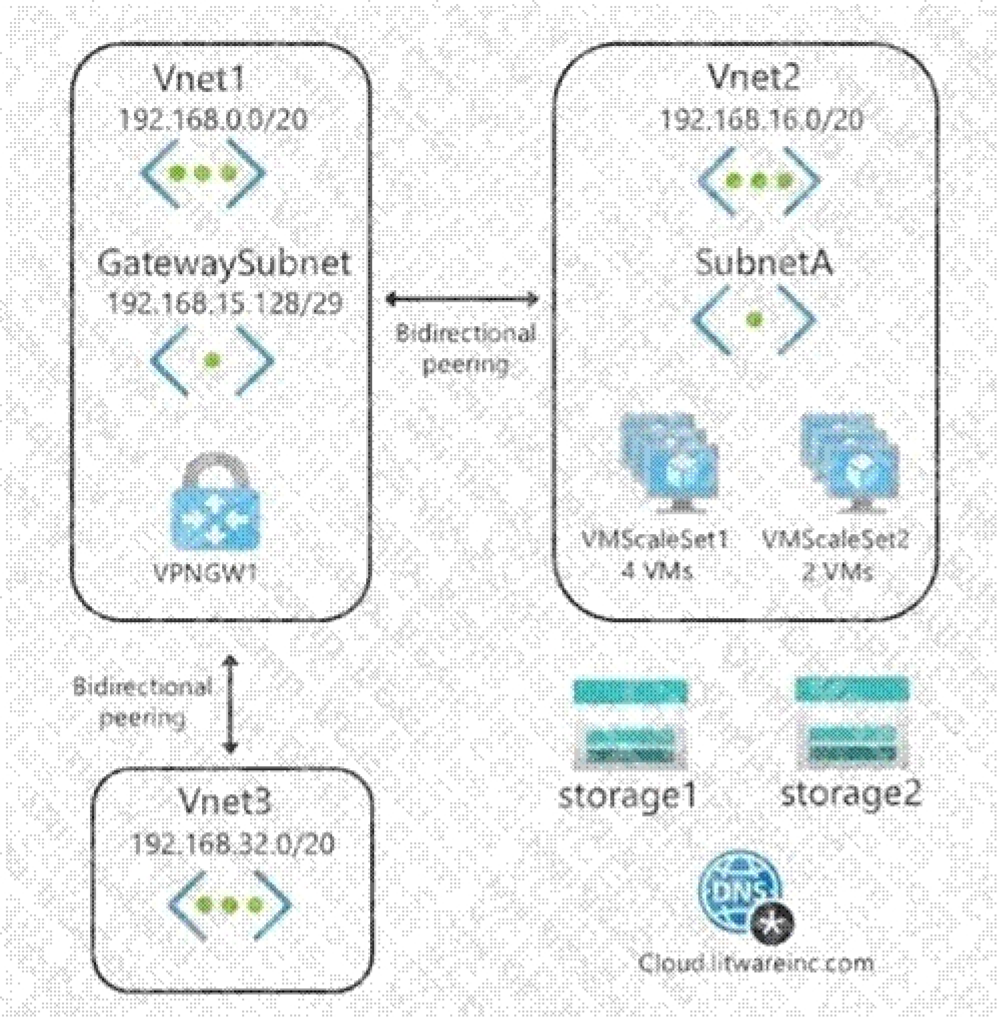
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.



Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly. Azure Environment Diagram



Requirements

Business Requirements

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit. Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD. Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection. Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1. The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

QUESTION 1

You need to configure the default route on Vnet2 and Vnet3. The solution must meet the virtual networking requirements. What should you use to configure the default route?

A. route filters

B. BGP route exchange

C. a user-defined route assigned to GatewaySubnet in Vnet1

D. a user-defined route assigned to GatewaySubnet in Vnet2 and Vnet3

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

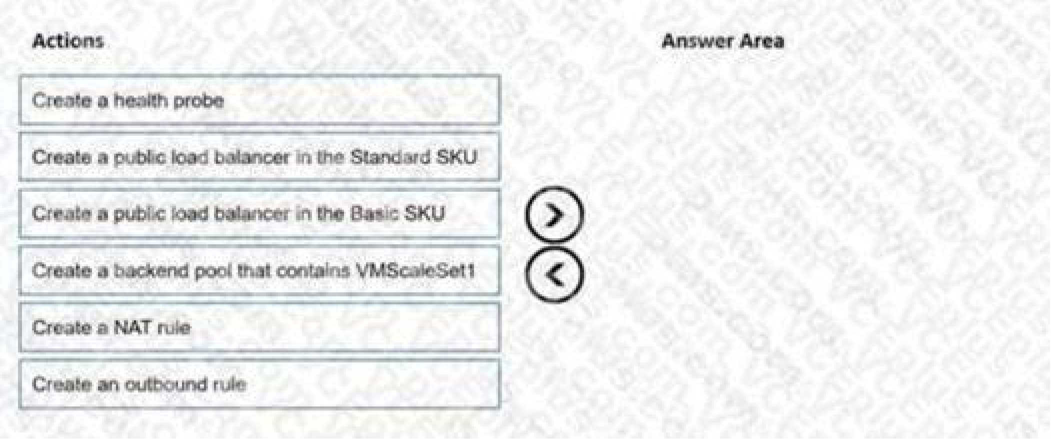
QUESTION 2
You need to configure the default route in Vnet2 and Vnet3. The solution must meet the virtual networking requirements. What should you use to configure the default route?

A. a user-defined route assigned to GatewaySubnet in Vnet2 and Vnet3
B. a user-defined route assigned to GatewaySubnet in Vnet1
C. BGP route exchange
D. route filters

Correct Answer: C
Section:
Explanation:

QUESTION 3
DRAG DROP
You need to implement outbound connectivity for VMScaleSet1. The solution must meet the virtual networking requirements and the business requirements. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

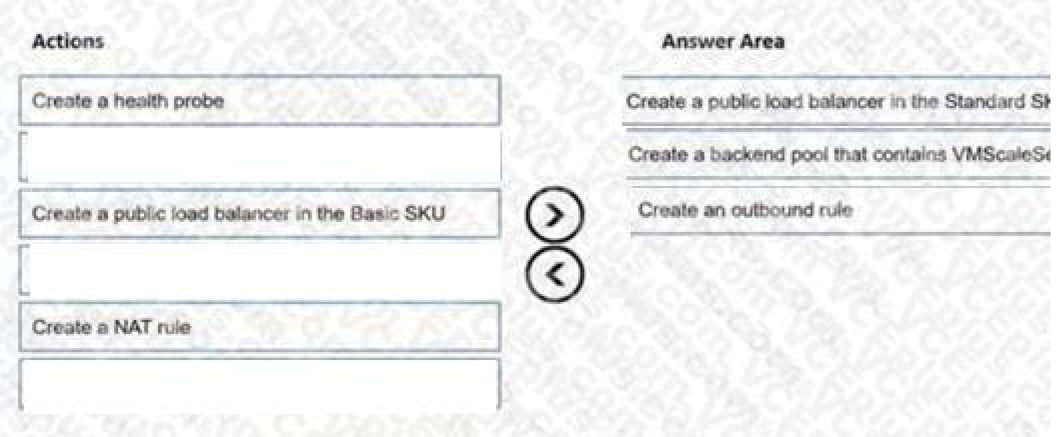
Select and Place:



Actions

- Create a health probe
- Create a public load balancer in the Standard SKU
- Create a public load balancer in the Basic SKU
- Create a backend pool that contains VMScaleSet1
- Create a NAT rule
- Create an outbound rule

Correct Answer:



Actions

Create a health probe

Create a public load balancer in the Basic SKU

Create a NAT rule

Answer Area

Create a public load balancer in the Standard SK

Create a backend pool that contains VMScaleSe

Create an outbound rule

Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/load-balancer/skus https://docs.microsoft.com/en-us/azure/loadbalancer/load-balancer-outbound-connections#outboundrules

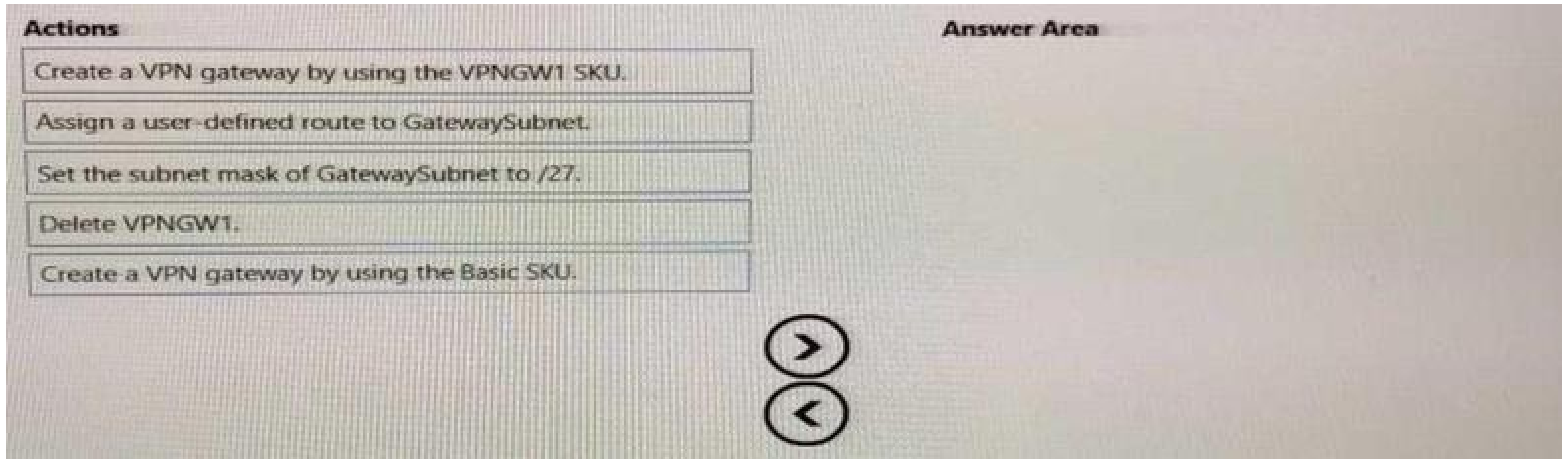
QUESTION 4
You need to connect Vnet2 and Vnet3. The solution must meet the virtual networking requirements and the business requirements. Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. On the peerings from Vnet2 and Vnet3, select Use remote gateways.
B. On the peering from Vnet1, select Allow forwarded traffic.
C. On the peering from Vnet1, select Use remote gateways.
D. On the peering from Vnet1, select Allow gateway transit.
E. On the peerings from Vnet2 and Vnet3, select Allow gateway transit.

Correct Answer: B, D
Section:

QUESTION 5
DRAG DROP
You need to prepare Vnet1 for the deployment of an ExpressRoute gateway. The solution must meet the hybrid connectivity requirements and the business requirements. Which three actions should you perform in sequence for Vnet1? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

Create a VPN gateway by using the VPNGW1 SKU.

Assign a user-defined route to GatewaySubnet.

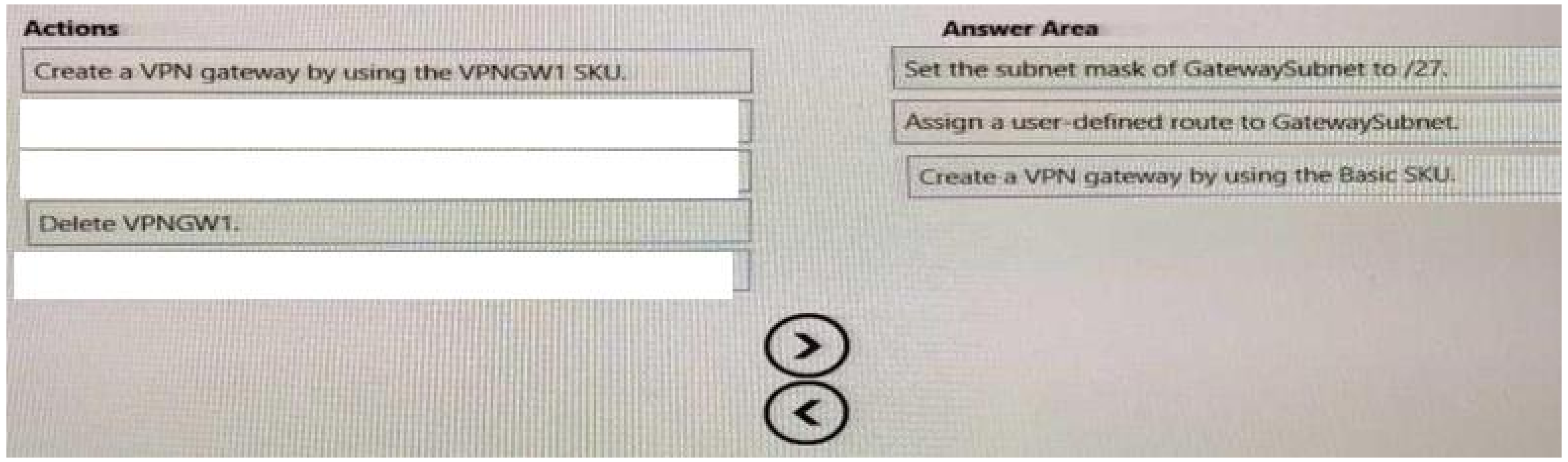
Set the subnet mask of GatewaySubnet to /27.

Delete VPNGW1.

Create a VPN gateway by using the Basic SKU.

Answer Area

Correct Answer:



Actions

Create a VPN gateway by using the VPNGW1 SKU.

Delete VPNGW1.

Answer Area

Set the subnet mask of GatewaySubnet to /27.

Assign a user-defined route to GatewaySubnet.

Create a VPN gateway by using the Basic SKU.

Section:
Explanation:

QUESTION 6

You need to provide connectivity to storage1. The solution must meet the PaaS networking requirements and the business requirements.

What should you include in the solution?

A. a service endpoint
B. Azure Front Door
C. a private endpoint
D. Azure Traffic Manager

Correct Answer: A
Section:
Explanation:

Case

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study. At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question. Overview

Litware, Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

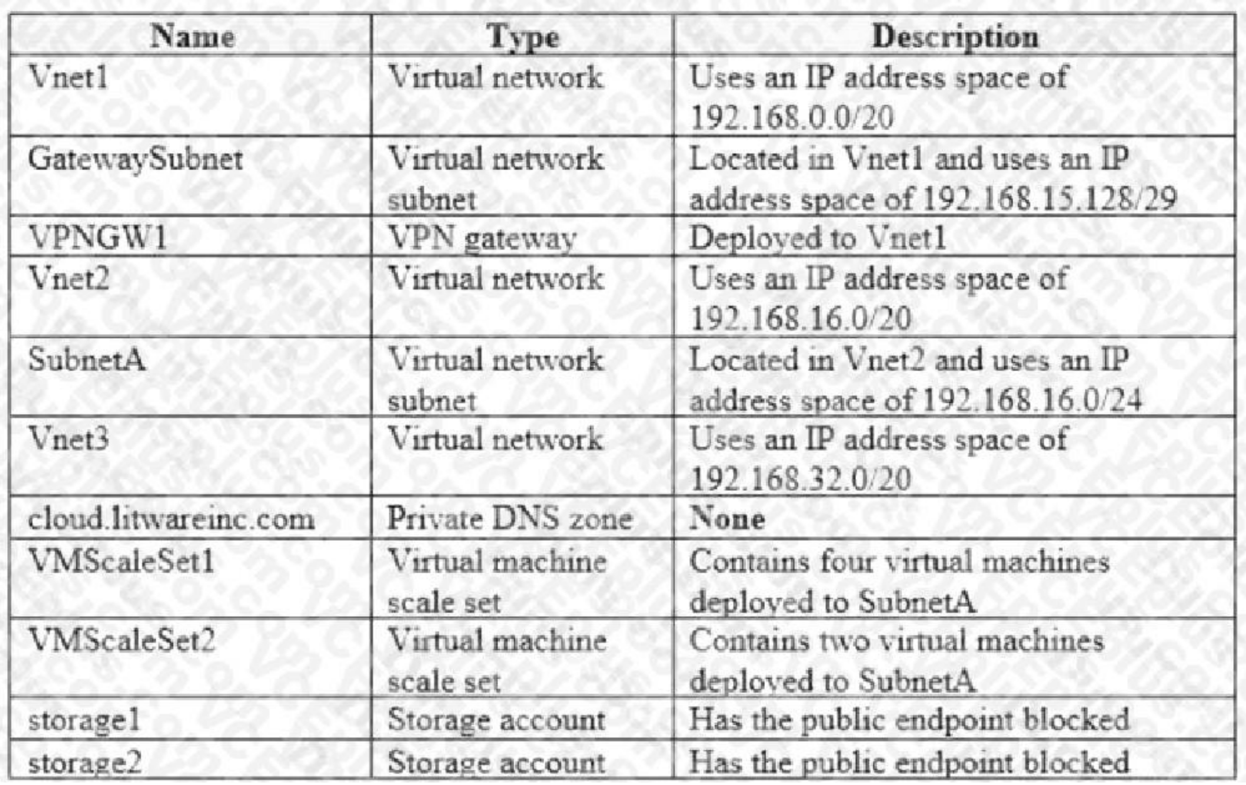
Existing Environment

Hybrid Environment

The on-premises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by using Azure AD Connect. All offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment

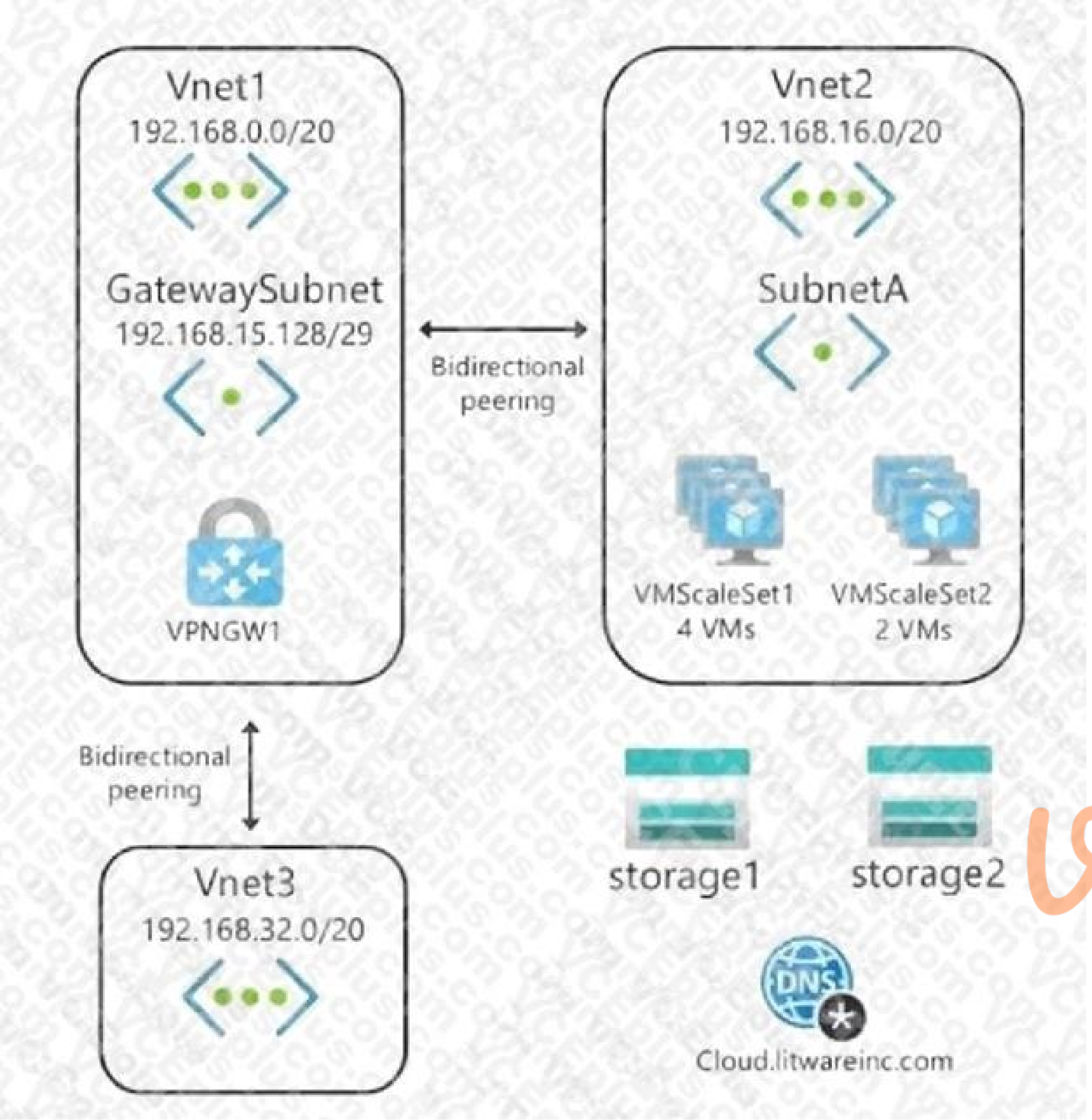
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.



Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	None
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Network Diagram exhibit.

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly. Azure Environment Diagram



Requirements

Business Requirements

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements

Litware identifies the following virtual networking requirements:

Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit. Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.

Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.

Minimize the size of the subnets allocated to platform-managed services.

Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements

Litware identifies the following hybrid networking requirements:

Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely. Connections must be authenticated by Azure AD. Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection. Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements

Litware identifies the following networking requirements for platform as a service (PaaS):

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1. The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

QUESTION 1

You need to provide access to storage2. The solution must meet the PaaS networking requirements and the business requirements. Which connectivity method should you use?

A. a private endpoint
B. Azure Firewall
C. Azure Front Door
D. a service endpoint

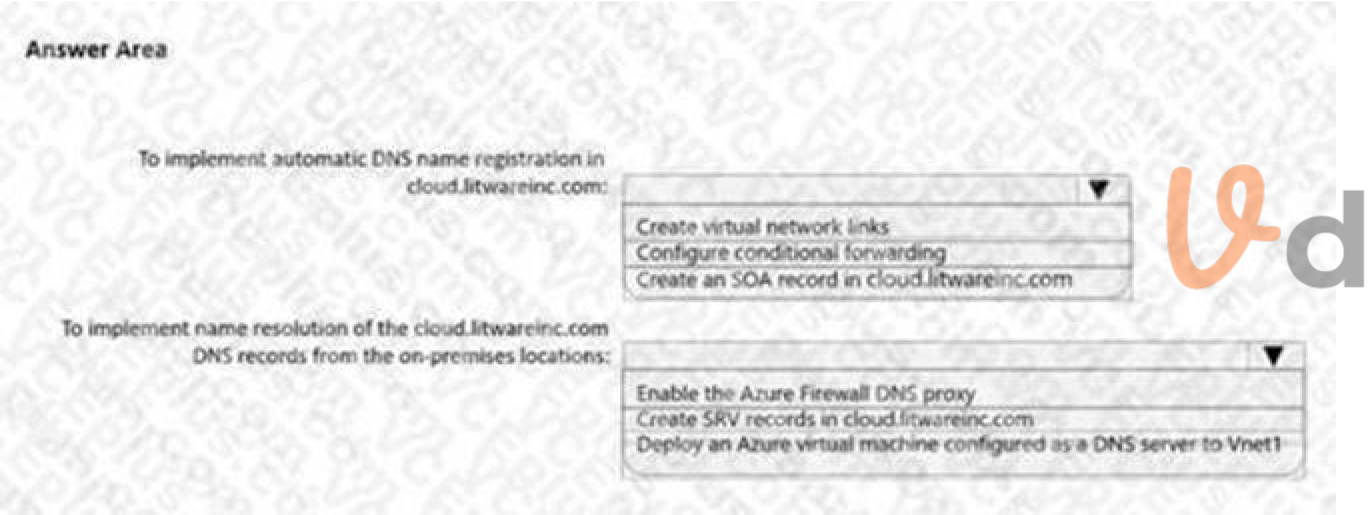
Correct Answer: D
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

QUESTION 2

HOTSPOT

You need to implement name resolution for the cloud.liwareinc.com. The solution must meet the networking requirements. What should you do? To answer, select the appropriate options in the answer area.

Hot Area:



Answer Area

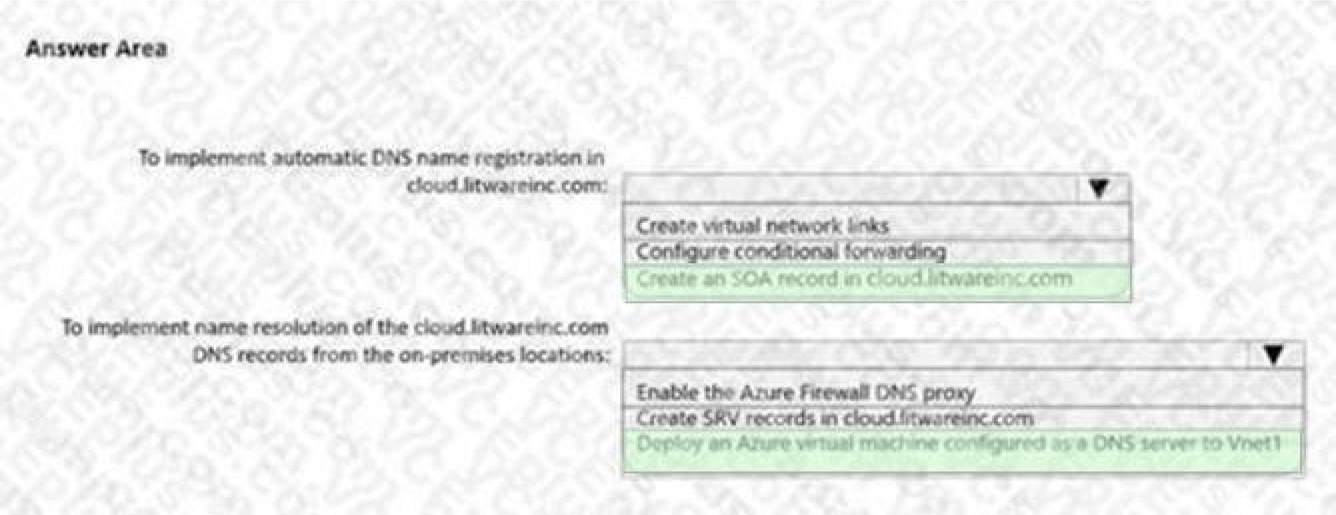
To implement automatic DNS name registration in cloud.litwareinc.com:

- Create virtual network links
- Configure conditional forwarding
- Create an SOA record in cloud.litwareinc.com

To implement name resolution of the cloud.litwareinc.com DNS records from the on-premises locations:

- Enable the Azure Firewall DNS proxy
- Create SRV records in cloud.litwareinc.com
- Deploy an Azure virtual machine configured as a DNS server to Vnet1

Answer Area:



Answer Area

To implement automatic DNS name registration in cloud.litwareinc.com:

- Create virtual network links
- Configure conditional forwarding
- [✓ Create an SOA record in cloud.litwareinc.com]

To implement name resolution of the cloud.litwareinc.com DNS records from the on-premises locations:

- Enable the Azure Firewall DNS proxy
- Create SRV records in cloud.litwareinc.com
- [✓ Deploy an Azure virtual machine configured as a DNS server to Vnet1]

Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/dns/private-dns-autoregistration https://docs.microsoft.com/enus/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances

Exam A

QUESTION 1

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN. You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit. Vnet2 can use the remote gateway. You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You enable BGP on the gateway of Vnet1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

Explanation:

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

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

QUESTION 2

You plan to deploy Azure virtual network.

You need to design the subnets.

Which three types of resources require a dedicated subnet? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Azure Bastion

B. Azure Active Directory Domain Services

C. Azure Private Link

D. Azure Application Gateway v2

E. VPN gateway

Correct Answer: A, D, E

Section:

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services

QUESTION 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit. Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You download and reinstall the VPN client configuration.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:
Explanation:
The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

QUESTION 4
You have an Azure virtual network named Vnet1 that hosts an Azure firewall named FW1 and 150 virtual machines. Vnet1 is linked to a private DNS zone named contoso.com. All the virtual machines have their name registered in the contoso.com zone.
Vnet1 connects to an on-premises datacenter by using ExpressRoute.
You need to ensure that on-premises DNS servers can resolve the names in the contoso.com zone.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Modify the DNS server settings of Vnet1.
B. For FW1, configure custom DNS server.
C. For FW1, enable DNS proxy.
D. On the on-premises DNS servers, configure forwarders that point to the frontend IP address of FW1.
E. On the on-premises DNS servers, configure forwarders that point to the Azure provided DNS service at 168.63.129.16.

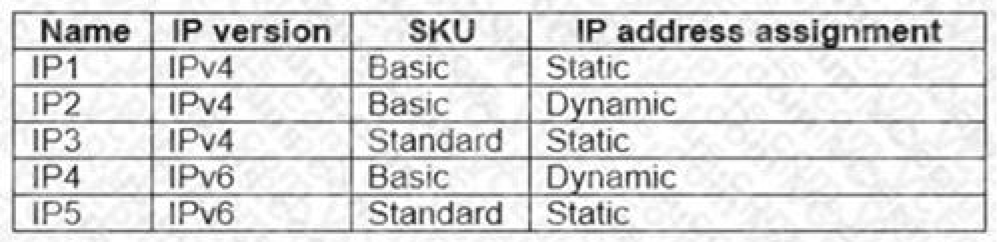
Correct Answer: C, D
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns#on-premises-workloads-using-a-dns-forwarder https://azure.microsoft.com/en-gb/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/

QUESTION 5
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
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

QUESTION 6
You have an Azure subscription that contains the public IP addresses shown in the following table.



Name	IP version	SKU	IP address assignment
IP1	IPv4	Basic	Static
IP2	IPv4	Basic	Dynamic
IP3	IPv4	Standard	Static
IP4	IPv6	Basic	Dynamic
IP5	IPv6	Standard	Static

You plan to deploy a NAT gateway named NAT1.
Which public IP addresses can be used as the public IP address for NAT1?

A. IP3 only
B. IP5 only
C. IP2 and IP4 only
D. IP1, IP3 and IP5 only
E. IP3 and IP5 only

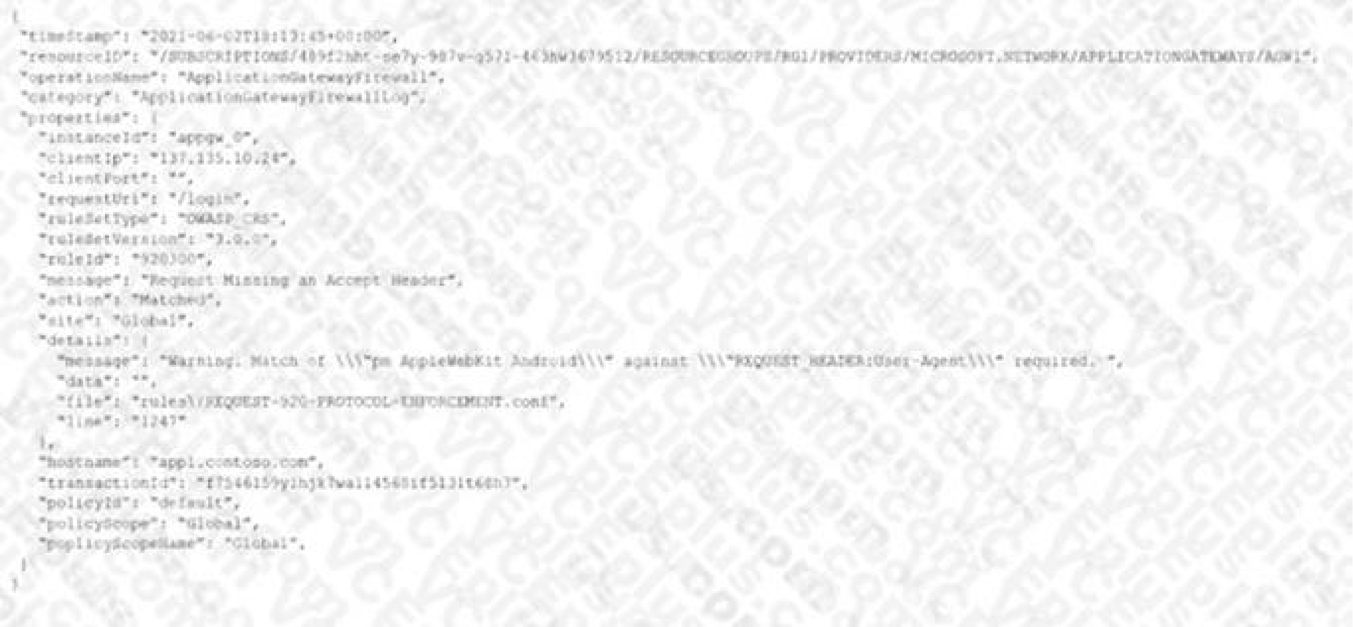
Correct Answer: A
Section:
Explanation:
Only static IPv4 addresses in the Standard SKU are supported. IPv6 doesn’t support NAT.
Reference: https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview

QUESTION 7
You have an Azure application gateway named AGW1 that has a routing rule named Rule1. Rule 1 directs traffic for http://www.contoso.com to a backend pool named Pool1. Pool1 targets an Azure virtual machine scale set named VMSS1. You deploy another virtual machine scale set named VMSS2.
You need to configure AGW1 to direct all traffic for http://www.adatum.com to VMSS2.
The solution must ensure that requests to http://www.contoso.com continue to be directed to Pool1.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add a backend pool.
B. Modify an HTTP setting.
C. Add an HTTP setting.
D. Add a listener.
E. Add a rule.

Correct Answer: A, D, E
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/application-gateway/configuration-overview

QUESTION 8
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 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": "appl.contoso.com",
    "transactionId": "f7546159y1hjk7wa114568if5131t68h7",
    "policyId": "default",
    "policyScope": "Global",
    "poplicyScopeName": "Global",
  }
}
```

You need to ensure that the URL is accessible through the application gateway.
Solution: You add a rewrite rule for the host header.
Does this meet the goal?

A. Yes

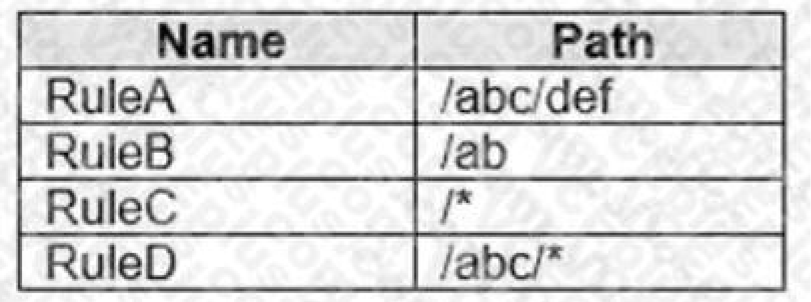
B. No

Correct Answer: B
Section:

QUESTION 9

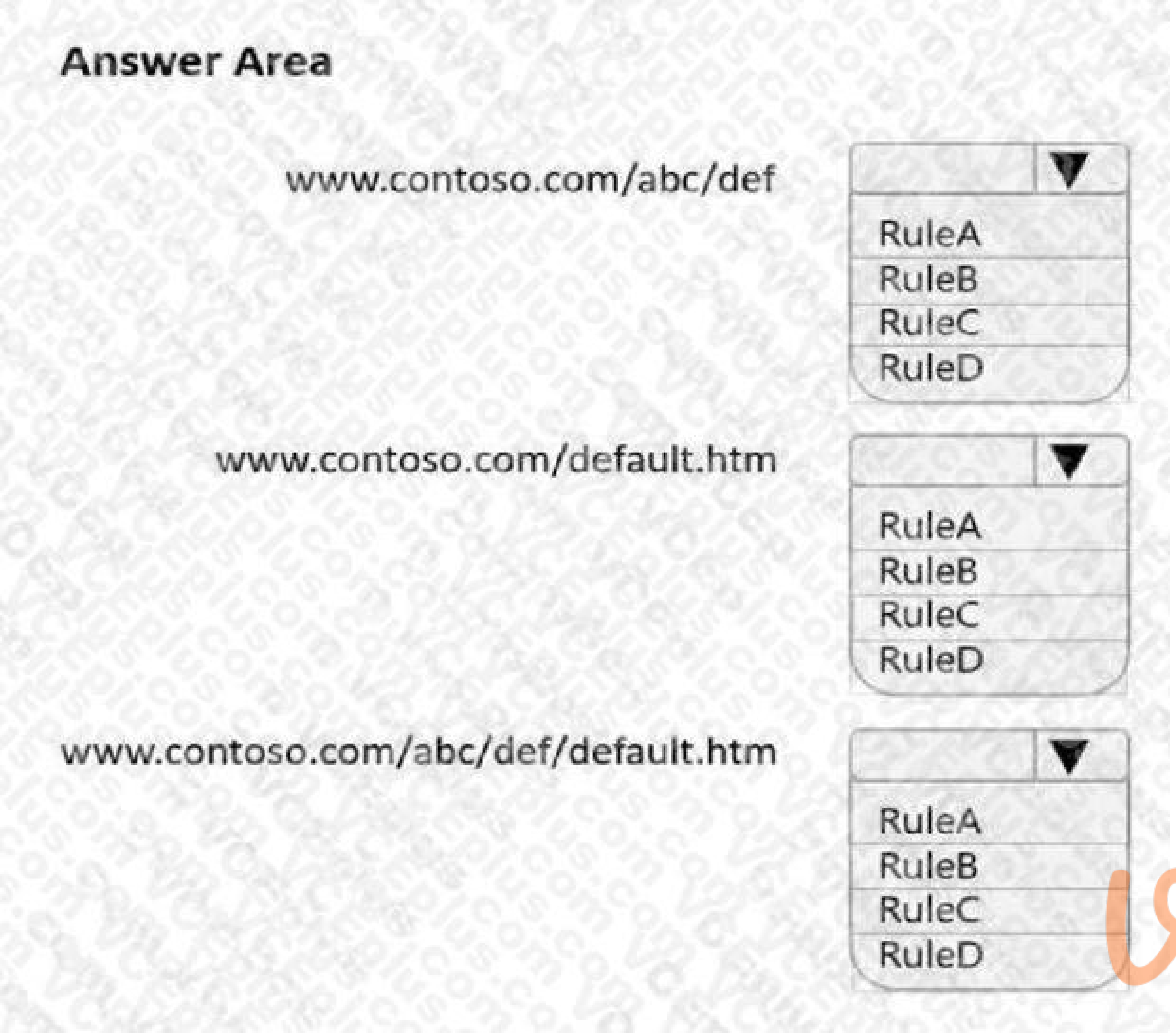
HOTSPOT

You have an Azure Front Door instance that provides access to a web app. The web app uses a hostname of www.contoso.com. 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 each incoming request? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point Hot Area:



Answer Area

www.contoso.com/abc/def

- RuleA
- RuleB
- RuleC
- RuleD

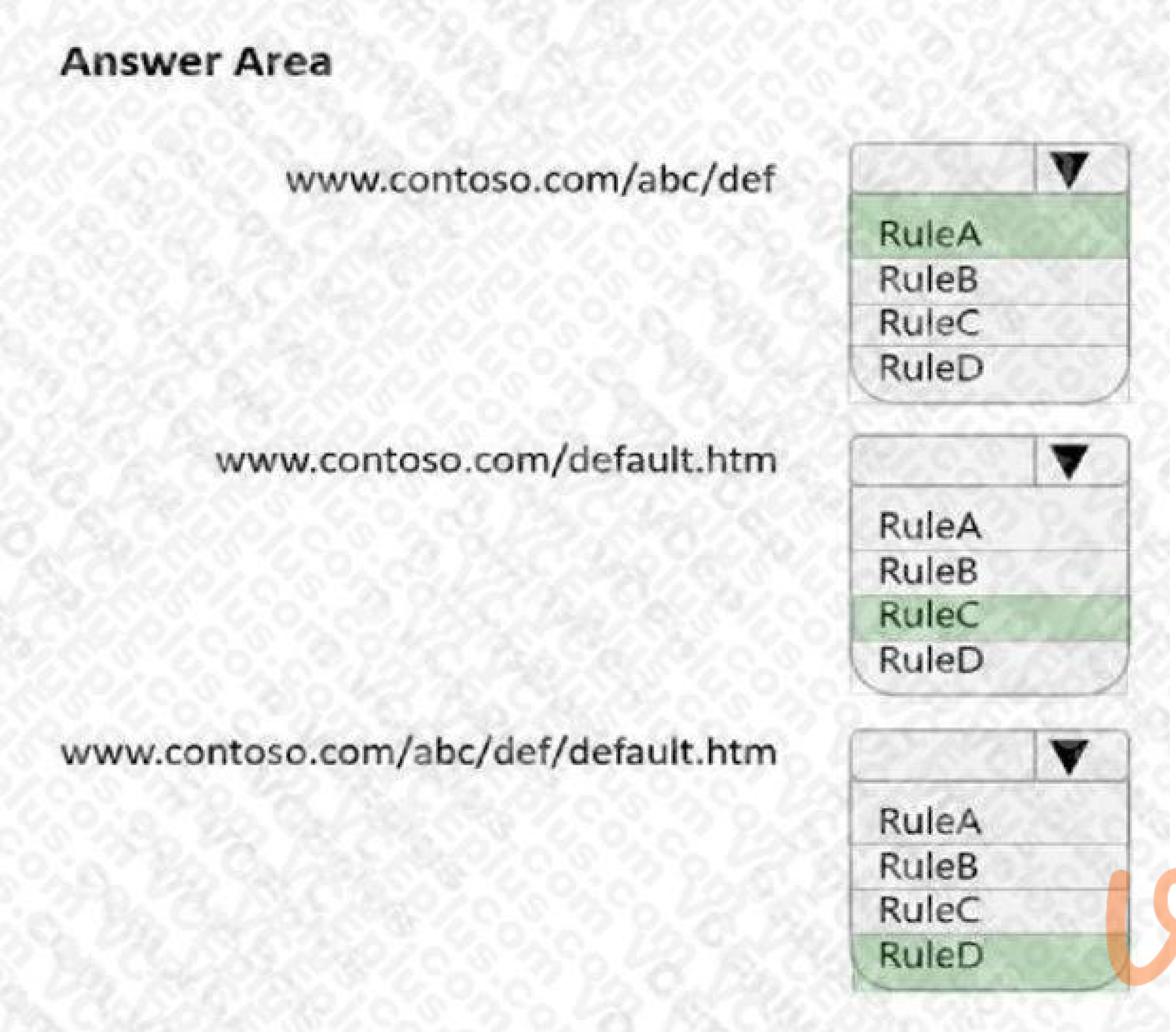
www.contoso.com/default.htm

- RuleA
- RuleB
- RuleC
- RuleD

www.contoso.com/abc/def/default.htm

- RuleA
- RuleB
- RuleC
- RuleD

A.
B.
C.
D.
Answer:



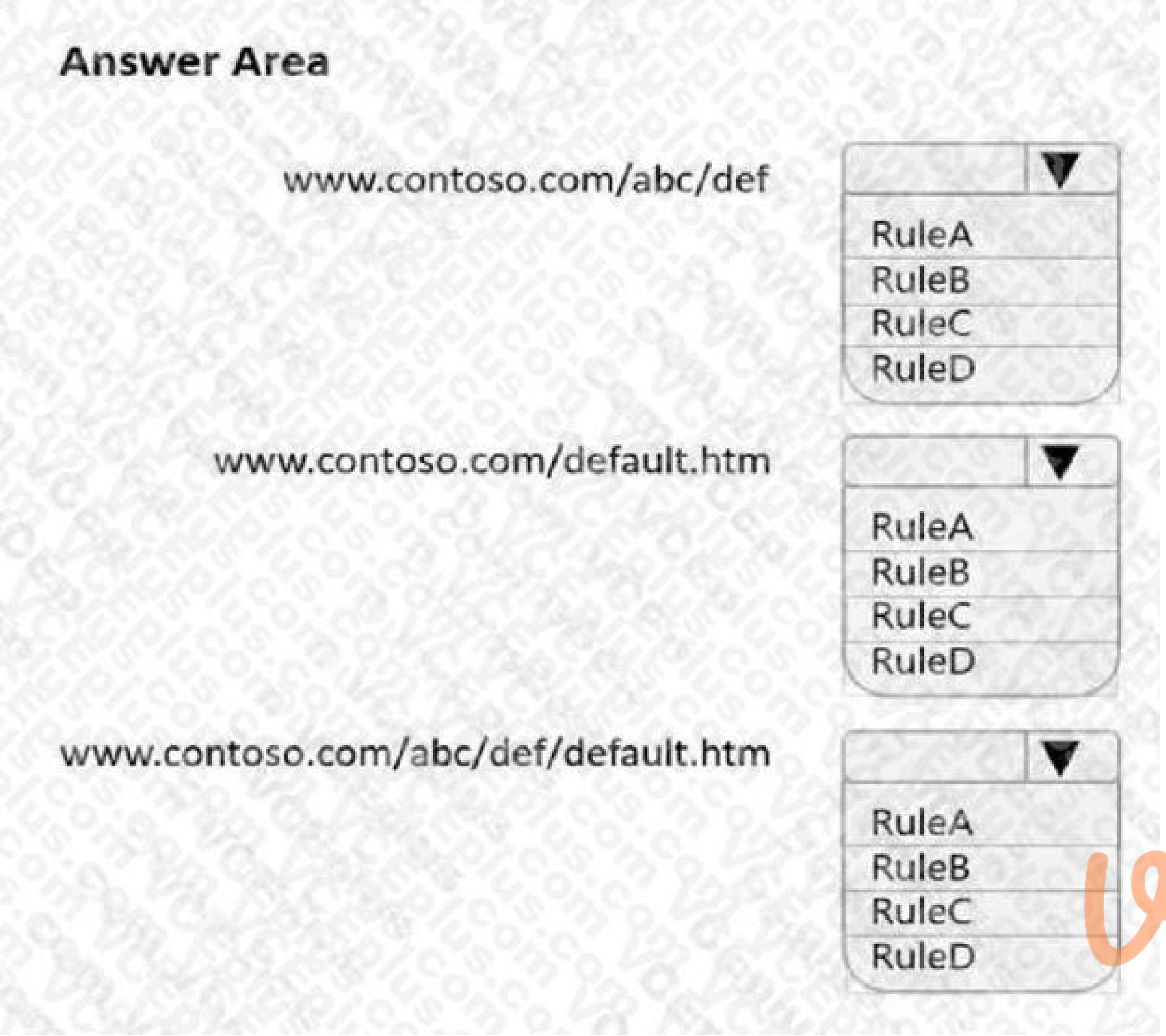
Answer Area

www.contoso.com/abc/def
[✓ RuleA]
RuleB
RuleC
RuleD

www.contoso.com/default.htm
RuleA
RuleB
[✓ RuleC]
RuleD

www.contoso.com/abc/def/default.htm
RuleA
RuleB
RuleC
[✓ RuleD]

Hot Area:



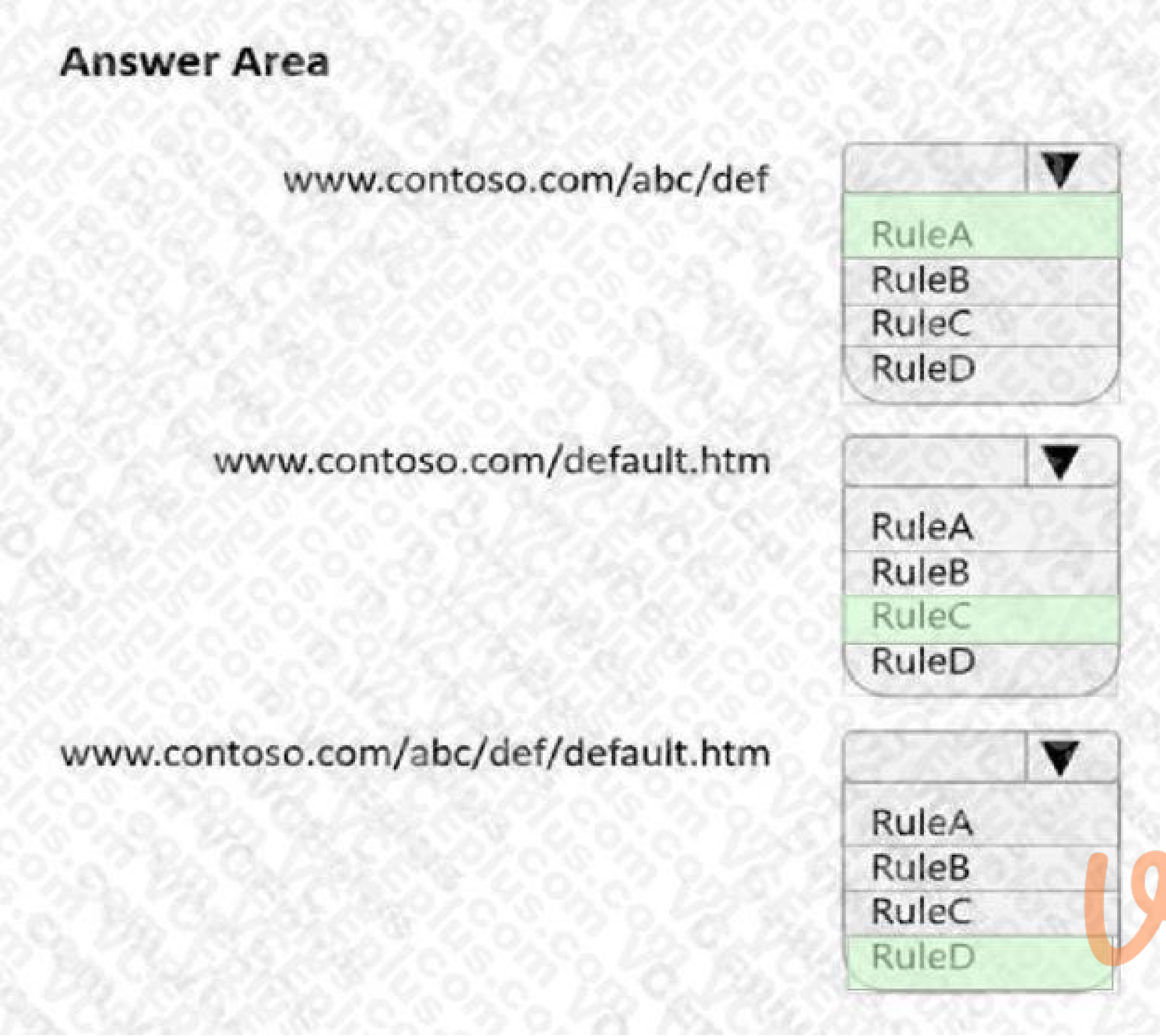
Answer Area

www.contoso.com/abc/def

www.contoso.com/default.htm

www.contoso.com/abc/def/default.htm

Answer Area:



Answer Area

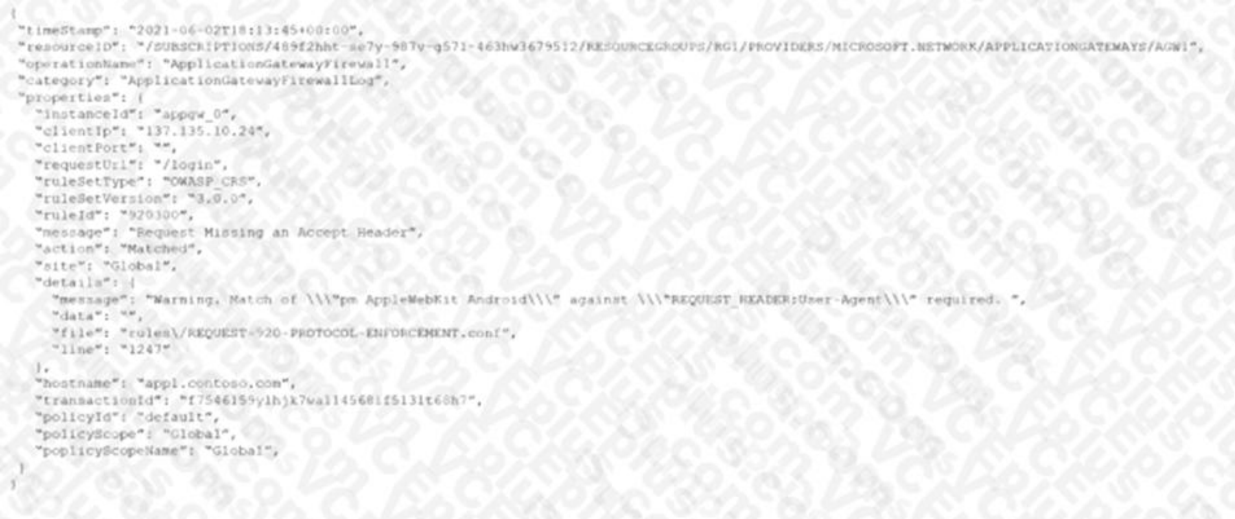
www.contoso.com/abc/def
[✓ RuleA]
RuleB
RuleC
RuleD

www.contoso.com/default.htm
RuleA
RuleB
[✓ RuleC]
RuleD

www.contoso.com/abc/def/default.htm
RuleA
RuleB
RuleC
[✓ RuleD]

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

QUESTION 10
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 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": "appl.contoso.com",
   "transactionId": "f7546159ylhjk7wal145681f5131t68h7",
   "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
Section:

QUESTION 11
You have an Azure application gateway for a web app named App1. The application gateway allows end-to-end encryption. You configure the listener for HTTPS by uploading an enterprise-signed certificate.
You need to ensure that the application gateway can provide end-to-end encryption for App1.
What should you do?

A. Increase the Unhealthy threshold setting in the custom probe.
B. Enable the SSL profile to the listener.
C. Set Listener type to Multi site.
D. Upload the public key certificate to the HTTP settings.

Correct Answer: D
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/application-gateway/end-to-end-ssl-portal

QUESTION 12
You have an Azure application gateway named AppGW1 that balances requests to a web app named App1.
You need to modify the server variables in the response header of App1.
What should you configure on AppGW1?

A. HTTP settings
B. rewrites
C. rules
D. listeners

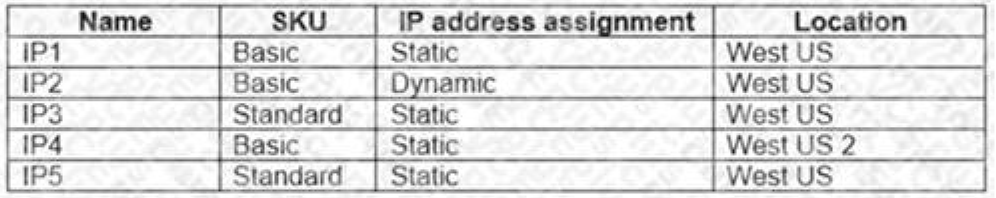
Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-url

QUESTION 13
You have an Azure Virtual Desktop deployment that has 500 session hosts.
All outbound traffic to the internet uses a NAT gateway.
During peak business hours. some users report that they cannot access internet resources. In Azure Monitor, you discover many failed SNAT connections. You need to increase the available SNAT connections.
What should you do?

A. Bind the NAT gateway to another subnet.
B. Add a public IP address.
C. Deploy Azure Standard Load Balancer that has outbound rules.

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource

QUESTION 14
You have an Azure subscription that contains the public IPv4 addresses shown in the following table.



Name	SKU	IP address assignment	Location
IP1	Basic	Static	West US
IP2	Basic	Dynamic	West US
IP3	Standard	Static	West US
IP4	Basic	Static	West US 2
IP5	Standard	Static	West US

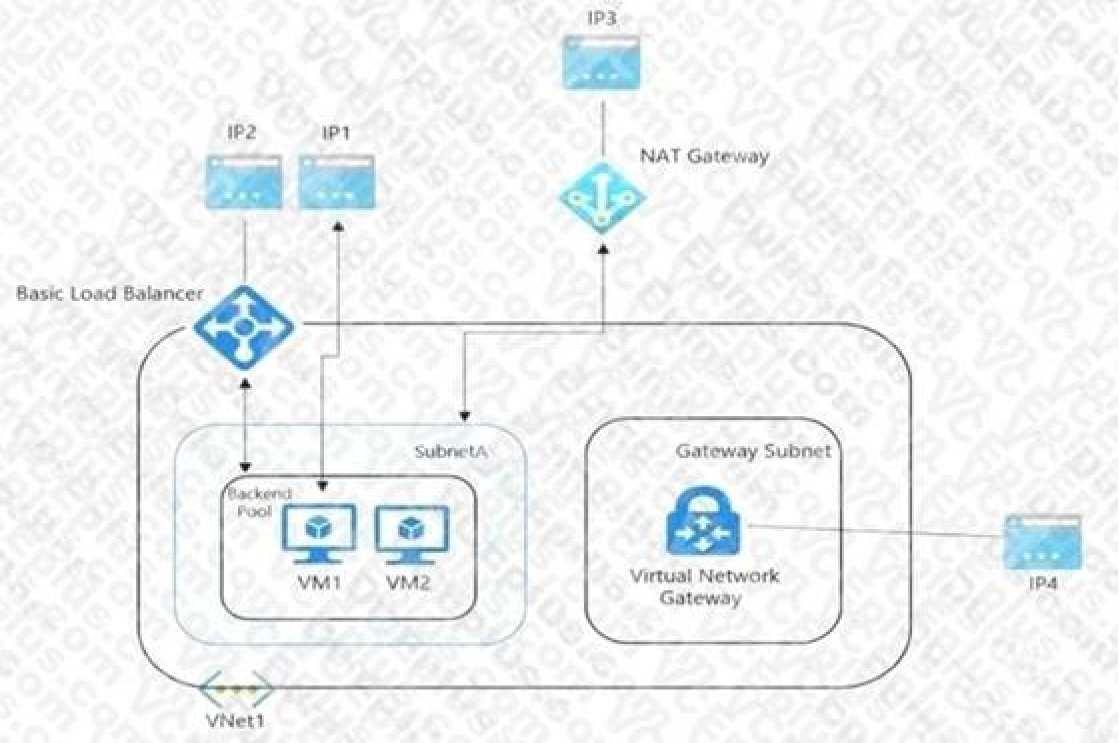
You plan to create a load balancer named LB1 that will have the following settings:
Name: LB1
Location: West US
Type: Public
SKU: Standard
Which public IPv4 addresses can be used by LB1?

A. IP1, IP3, IP4, and IP5 only
B. IP3 only
C. IP1 and IP3 only
D. IP2 only
E. IP1, IP2, IP3, IP4, and IP5
F. IP3 and IP5 only

Correct Answer: F
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address

QUESTION 15

You have the Azure environment shown in the exhibit.



VM1 is a virtual machine that has an instance-level public IP address (ILPIP).
Basic Load Balancer uses a public IP address. VM1 and VM2 are in the backend pool.
NAT Gateway uses a public IP address named IP3 that is associated to SubnetA.
VNet1 has a virtual network gateway that has a public IP address named IP4.
When initiating outbound traffic to the internet from VM1, which public address is used?

A. IP1
B. IP2
C. IP3
D. IP4

Correct Answer: A
Section:

QUESTION 16
You are configuring two network virtual appliances (NVAs) in an Azure virtual network. The NVAs will be used to inspect all the traffic within the virtual network. You need to provide high availability for the NVAs. The solution must minimize administrative effort. What should you include in the solution?

A. Azure Standard Load Balancer
B. Azure Application Gateway
C. Azure Traffic Manager
D. Azure Front Door

Correct Answer: C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha?tabs=cli

QUESTION 17

You have five virtual machines that run Windows Server. Each virtual machine hosts a different web app. You plan to use an Azure application gateway to provide access to each web app by using a hostname of www.contoso.com and a different URL path for each web app, for example: https:// www.contoso.com/app1. You need to control the flow of traffic based on the URL path.

What should you configure?

A. HTTP settings

B. listeners

C. rules

D. rewrites

Correct Answer: C

Section:

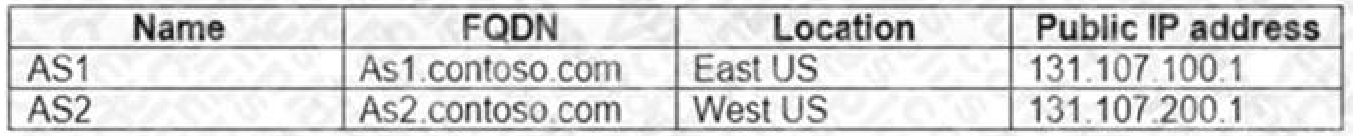
Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/application-gateway/url-route-overview

QUESTION 18

You plan to publish a website that will use an FQDN of www.contoso.com. The website will be hosted by using the Azure App Service apps shown in the following table.



Name	FQDN	Location	Public IP address
AS1	As1.contoso.com	East US	131.107.100.1
AS2	As2.contoso.com	West US	131.107.200.1

You plan to use Azure Traffic Manager to manage the routing of traffic for www.contoso.com between AS1 and AS2. You need to ensure that Traffic Manager routes traffic for www.contoso.com.

Which DNS record should you create?

A. two A records that map www.contoso.com to 131.107.100.1 and 131.107.200.1

B. a CNAME record that maps www.contoso.com to TMprofile1.azurefd.net

C. a CNAME record that maps www.contoso.com to TMprofile1.trafficmanager.net

D. a TXT record that contains a string of as1.contoso.com and as2.contoso.com in the details

Correct Answer: C

Section:

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/traffic-manager/quickstart-create-traffic-manager-profile

https://docs.microsoft.com/en-us/azure/app-service/configure-domain-traffic-manager

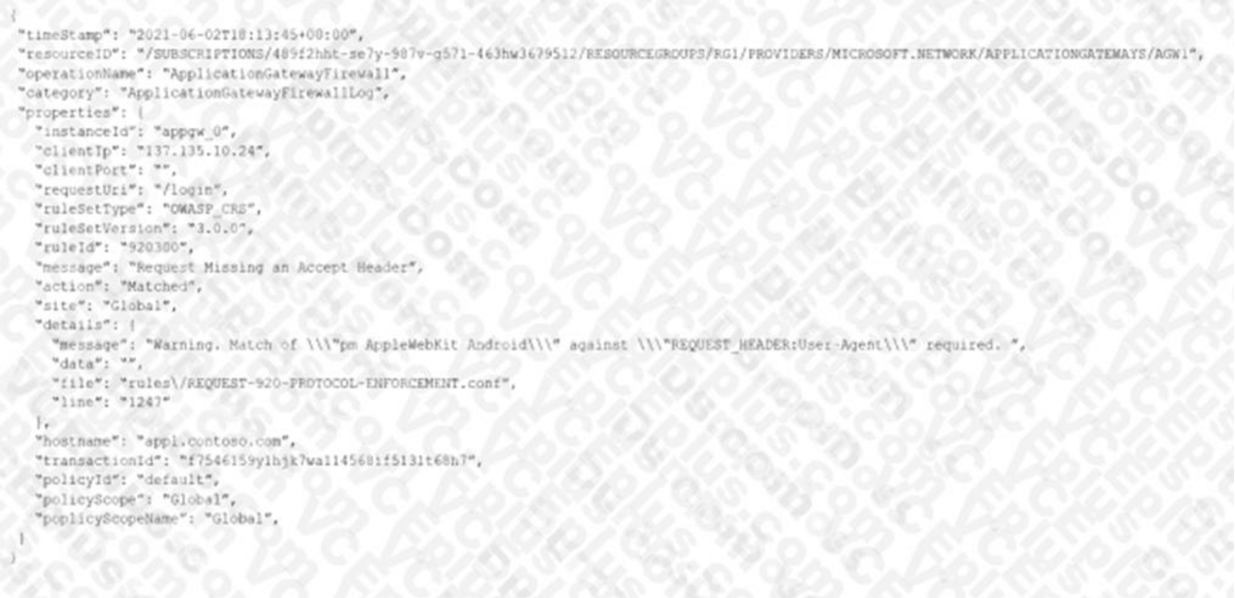
QUESTION 19

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 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.



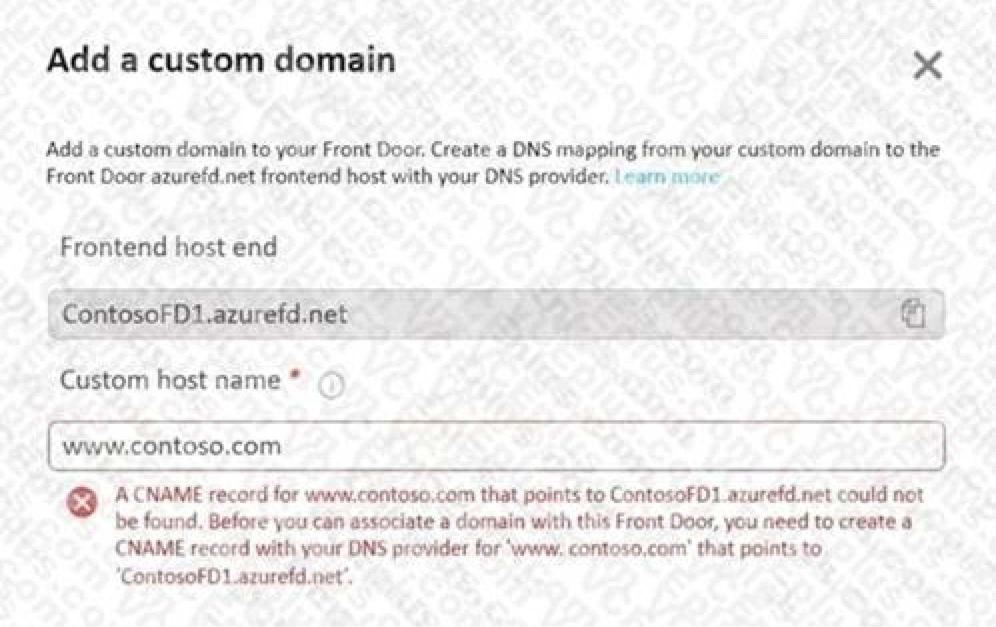
```
{
 "timeStamp": "2021-06-02T18:13:45+00:00",
 "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
 "operationName": "ApplicationGatewayFirewall",
 "category": "ApplicationGatewayFirewallLog",
 "properties": {
   "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": "appl.contoso.com",
   "transactionId": "f7546159y1hjk7wa114568if5131t68h7",
   "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 for request headers that contain 137.135.10.24.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 20



Add a custom domain ✕

Add a custom domain to your Front Door. Create a DNS mapping from your custom domain to the Front Door azurefd.net frontend host with your DNS provider. Learn more

Frontend host end

ContosoFD1.azurefd.net

Custom host name *

www.contoso.com

A CNAME record for www.contoso.com that points to ContosoFD1.azurefd.net could not be found. Before you can associate a domain with this Front Door, you need to create a CNAME record with your DNS provider for 'www. contoso.com' that points to 'ContosoFD1.azurefd.net'.

You have a website that uses an FQDN of www.contoso.com. The DNS record for www. contoso.com resolves to an onpremises 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?

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

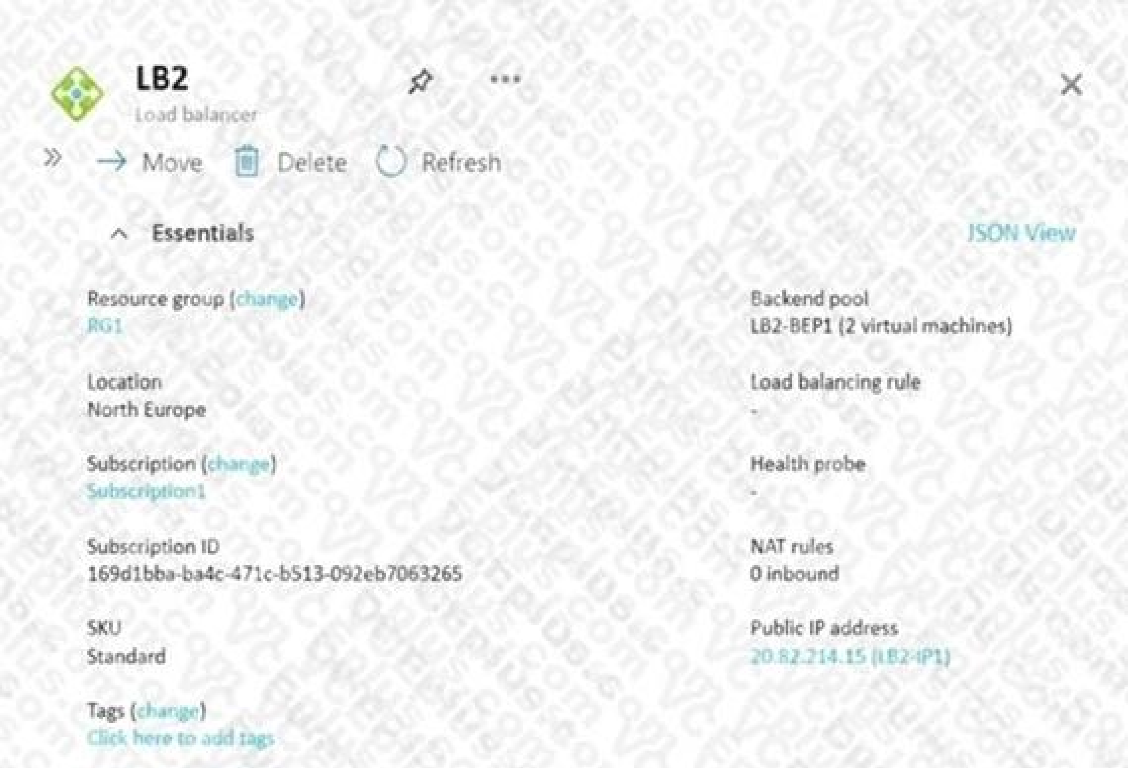
B. a CNAME record that maps www.contoso.com to ContosoFD1.azurefd.net

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

QUESTION 21
You have the Azure load balancer shown in the Load Balancer exhibit.



LB2
Load balancer

Essentials

Resource group (change)
RG1

Location
North Europe

Subscription (change)
Subscription1

Subscription ID
169d1bba-ba4c-471c-b513-092eb7063265

SKU
Standard

Tags (change)
Click here to add tags

Backend pool
LB2-BEP1 (2 virtual machines)

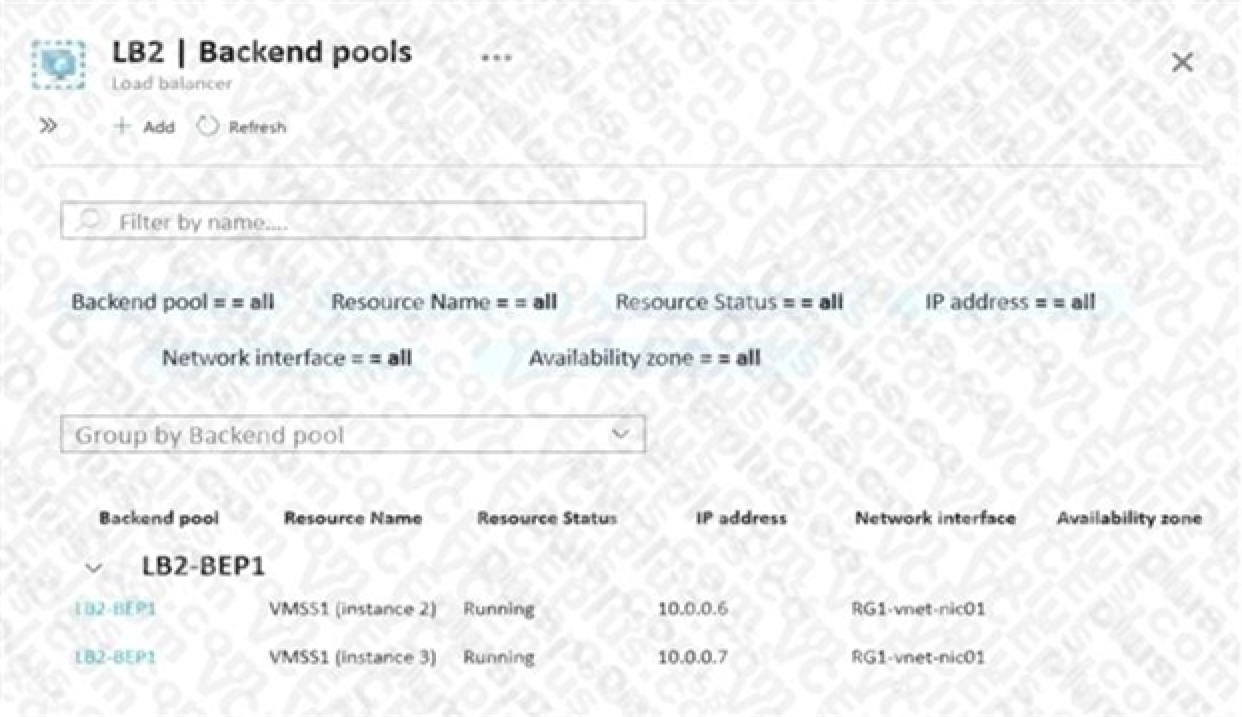
Load balancing rule
-

Health probe
-

NAT rules
0 inbound

Public IP address
20.82.214.15 (LB2-IP1)

LB2 has the backend pools shown in the Backend Pools exhibit.



Backend pool = = all   Resource Name = = all   Resource Status = = all   IP address = = all   Network interface = = all   Availability zone = = all

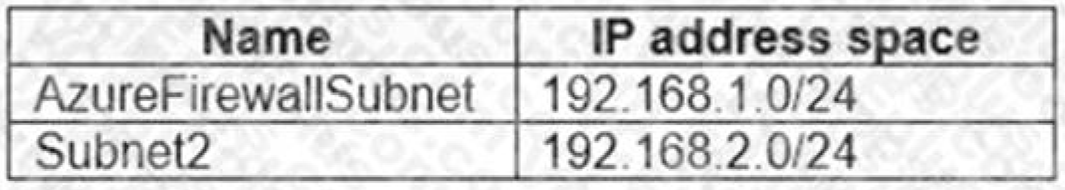
Backend pool	Resource Name	Resource Status	IP address	Network interface	Availability zone
LB2-BEP1					
LB2-BEP1	VMSS1 (instance 2)	Running	10.0.0.6	RG1-vnet-nic01	
LB2-BEP1	VMSS1 (instance 3)	Running	10.0.0.7	RG1-vnet-nic01	

You need to ensure that LB2 distributes traffic to all the members of VMSS1.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add a network interface to VMSS1.
B. Add a load balancing rule.
C. Configure a health probe.
D. Add a public IP address to each member of VMSS1.

Correct Answer: B, C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal?tabs=option-1-createload-balancer-standard

QUESTION 22
You have an Azure virtual network that contains the subnets shown in the following table.



Name	IP address space
AzureFirewallSubnet	192.168.1.0/24
Subnet2	192.168.2.0/24

You deploy an Azure firewall to AzureFirewallSubnet. You route all traffic from Subnet2 through the firewall. You need to ensure that all the hosts on Subnet2 can access an external site located at https://*.contoso.com. What should you do?

A. In a firewall policy, create a DNAT rule.
B. Create a network security group (NSG) and associate the NSG to Subnet2.
C. In a firewall policy, create a network rule.
D. In a firewall policy, create an application rule.

Correct Answer: D
Section:

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

QUESTION 23
You have an Azure Web Application Firewall (WAF) policy in prevention mode that is associated to an Azure Front Door instance. You need to configure the policy to meet the following requirements:
Log all connections from Australia.
Deny all connections from New Zealand.
Deny all further connections from a network of 131.107.100.0/24 if there are more than 100 connections during one minute. What is the minimum number of objects you should create?

A. three custom rules that each has one condition
B. one custom rule that has three conditions
C. one custom rule that has one condition
D. one rule that has two conditions and another rule that has one condition

Correct Answer: A
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

QUESTION 24
You have an Azure subscription that contains multiple virtual machines in the West US Azure region. You need to use Traffic Analytics.
Which two resources should you create? Each correct answer presents part of the solution. (Choose two.) NOTE: Each correct answer selection is worth one point.

A. an Azure Monitor workbook
B. a Log Analytics workspace
C. a storage account
D. an Azure Sentinel workspace
E. an Azure Monitor data collection rule

Correct Answer: B, C
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

QUESTION 25
You have a hybrid environment that uses ExpressRoute to connect an on-premises network and Azure.
You need to log the uptime and the latency of the connection periodically by using an Azure virtual machine and an onpremises virtual machine. What should you use?

A. Azure Monitor
B. IP flow verify
C. Connection Monitor
D. Azure Internet Analyzer

Correct Answer: C
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor

QUESTION 26
You have an Azure subscription that contains the following resources:
A virtual network named Vnet1
Two subnets named subnet1 and AzureFirewallSubnet A public Azure Firewall named FW1 A route table named RT1 that is associated to Subnet1 A rule routing of 0.0.0.0/0 to FW1 in RT1 After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.
You need to ensure that the virtual machines can be activated.
What should you do?

A. Deploy an application security croup mat allows outbound traffic to 1688
B. Deploy an Azure Standard Load Balancer that has an outbound NAT rule
C. On fW1.configure a DNAT rule for port 1688.
D. Add an internet route to RI1 for the Azure Key Management Service (KMS).

Correct Answer: D
Section:
Explanation:
Reference: https://ryanmangansitblog.com/2020/05/11/firewall-considerations-windows-virtual-desktop-wvd/

QUESTION 27
You have an Azure virtual network that contains a subnet named Subnet1. Subnet1 is associated to a network security group (NSG) named NSG1. NSG1 blocks all outbound traffic that is not allowed explicitly. Subnet1 contains virtual machines that must communicate with the Azure Cosmos DB service.
You need to create an outbound security rule in NSG1 to enable the virtual machines to connect to Azure Cosmos DB. What should you include in the solution?

A. a service tag
B. a service endpoint policy
C. a subnet delegation
D. an application security group

Correct Answer: A
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview https://docs.microsoft.com/enus/azure/virtual-network/virtual-network-service-endpoint-policies-portal

QUESTION 28
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: A
Section:
Explanation:

QUESTION 29
You have an Azure virtual network named Vnet1.
You need to ensure that the virtual machines in Vnet1 can access only the Azure SQL resources in the East US Azure region. The virtual machines must be prevented from accessing any Azure Storage resources. Which two outbound network security group (NSG) rules should you create? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. a deny rule that has a source of VirtualNetwork and a destination of Sql
B. an allow rule that has the IP address range of Vnet1 as the source and destination of Sql.EastUS
C. a deny rule that has a source of VirtualNetwork and a destination of 168.63.129.0/24
D. a deny rule that has the IP address range of Vnet1 as the source and destination of Storage

Correct Answer: C, D
Section:
Explanation:

QUESTION 30
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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:
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. Solution: You configure the firewall on storage1 to only accept connections from Vnet1.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 31
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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:
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. Solution: You create a network security group (NSG) and associate the NSG to Subnet1.
Does this meet the goal?

A. Yes
B. No

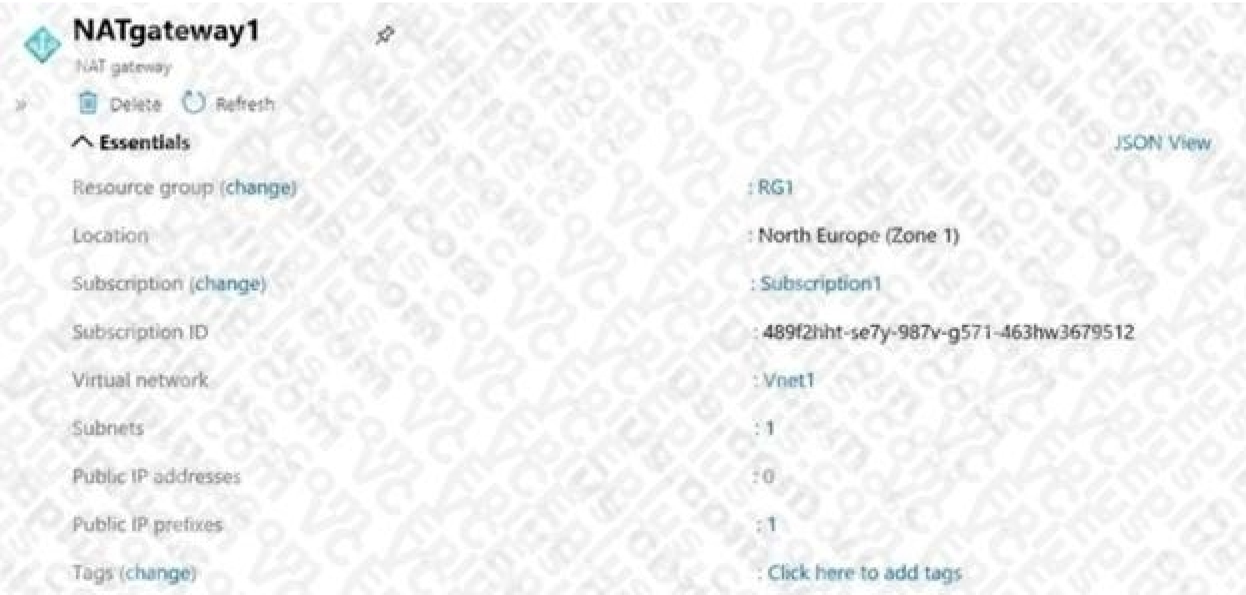
Correct Answer: B
Section:

QUESTION 32

HOTSPOT

You have an Azure virtual network named Vnet1 that contains two subnets named Subnet1 and Subnet2.

You have the NAT gateway shown in the NATgateway1 exhibit.



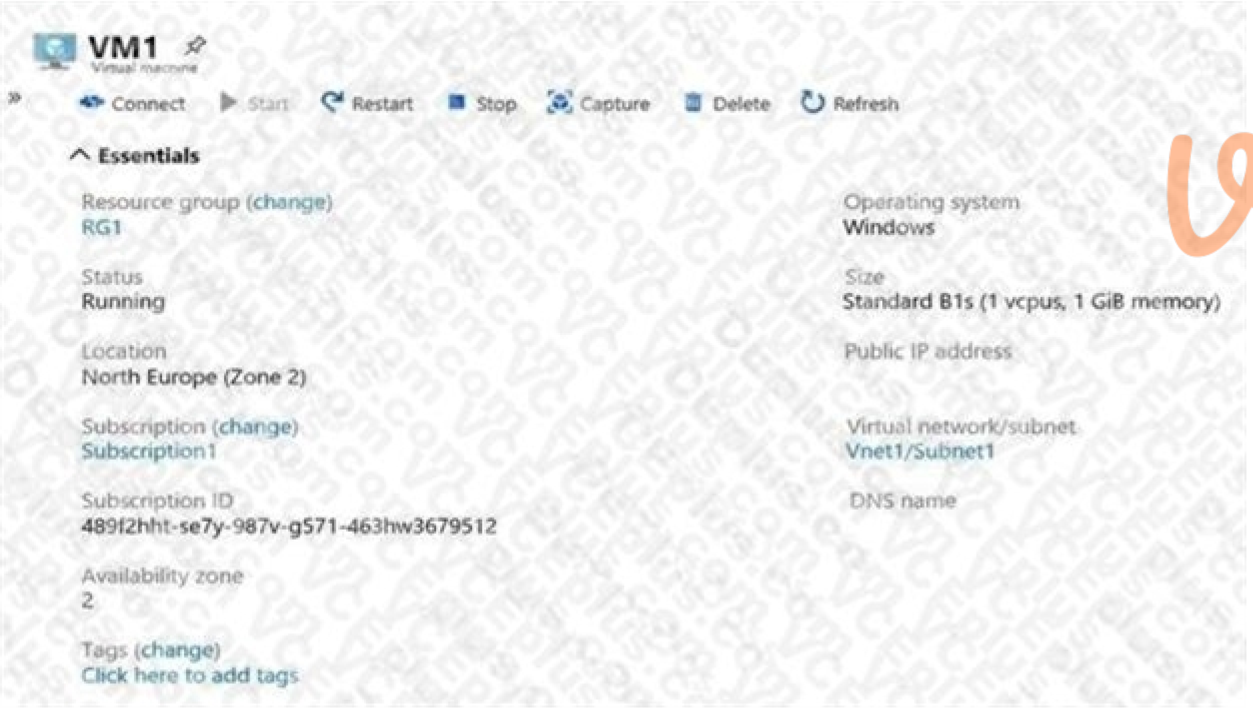
NATgateway1

NAT gateway

Essentials

Resource group (change)	: RG1
Location	: North Europe (Zone 1)
Subscription (change)	: Subscription1
Subscription ID	: 489f2hht-se7y-987v-g571-463hw3679512
Virtual network	: Vnet1
Subnets	: 1
Public IP addresses	: 0
Public IP prefixes	: 1
Tags (change)	: Click here to add tags

You have the virtual machine shown in the VM1 exhibit.



VM1

Virtual machine

Essentials

Resource group (change)
RG1

Status
Running

Location
North Europe (Zone 2)

Subscription (change)
Subscription1

Subscription ID
489f2hht-se7y-987v-g571-463hw3679512

Availability zone
2

Tags (change)
Click here to add tags

Operating system
Windows

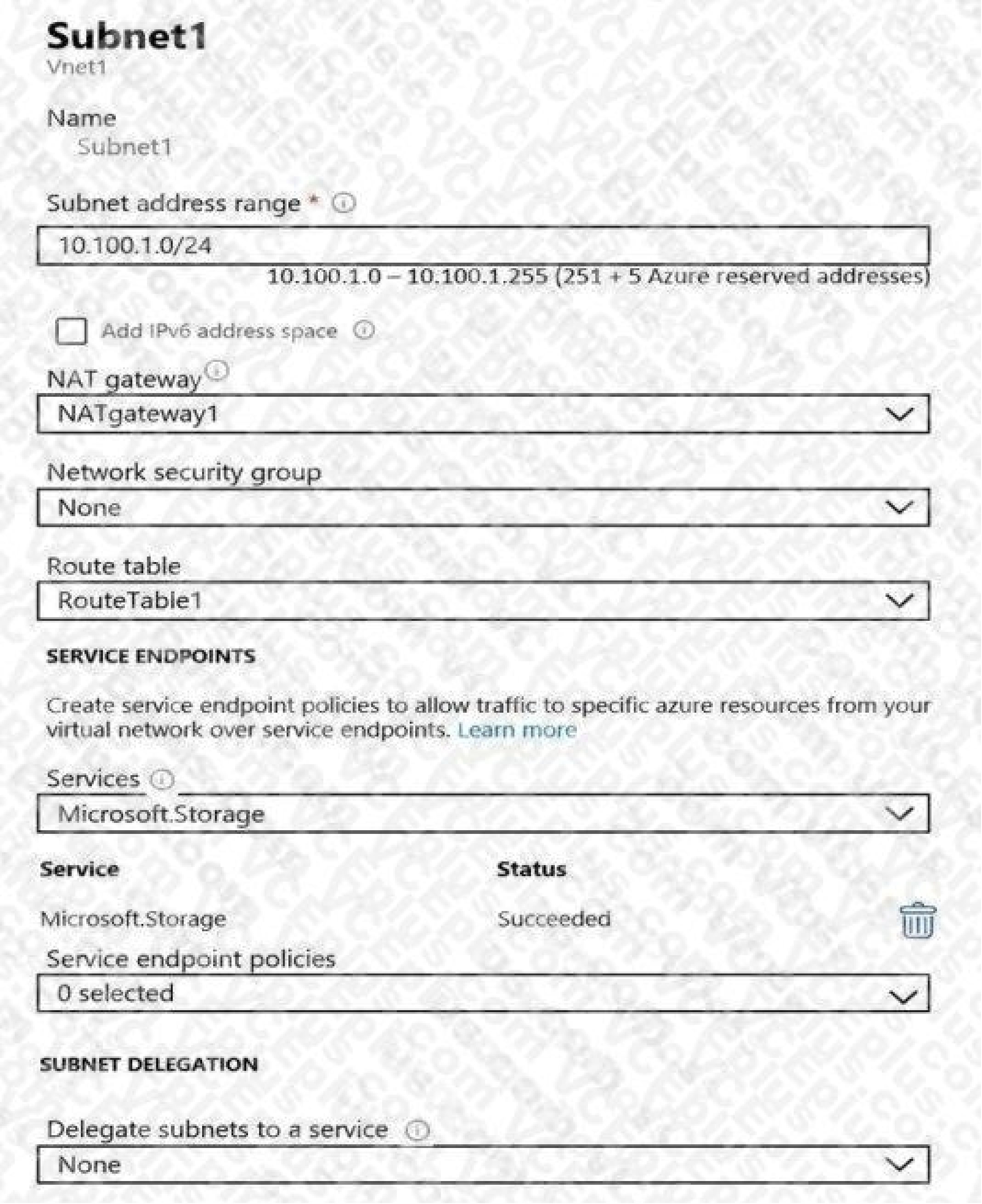
Size
Standard B1s (1 vcpus, 1 GiB memory)

Public IP address

Virtual network/subnet
Vnet1/Subnet1

DNS name

Subnet1 is configured as shown in the Subnet1 exhibit.



Subnet1
Vnet1

Name
Subnet1

Subnet address range * ⓘ
10.100.1.0/24
10.100.1.0 – 10.100.1.255 (251 + 5 Azure reserved addresses)

□ Add IPv6 address space ⓘ

NAT gateway ⓘ
NATgateway1

Network security group
None

Route table
RouteTable1

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services ⓘ
Microsoft.Storage

Service	Status
Microsoft.Storage	Succeeded

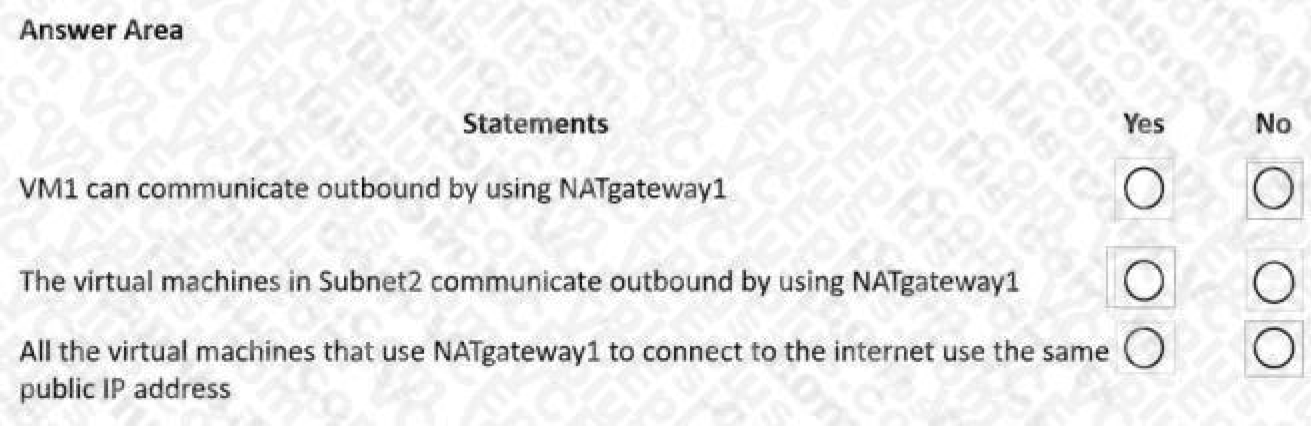
Service endpoint policies
0 selected

SUBNET DELEGATION

Delegate subnets to a service ⓘ
None

For each of the following statements, select Yes of the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

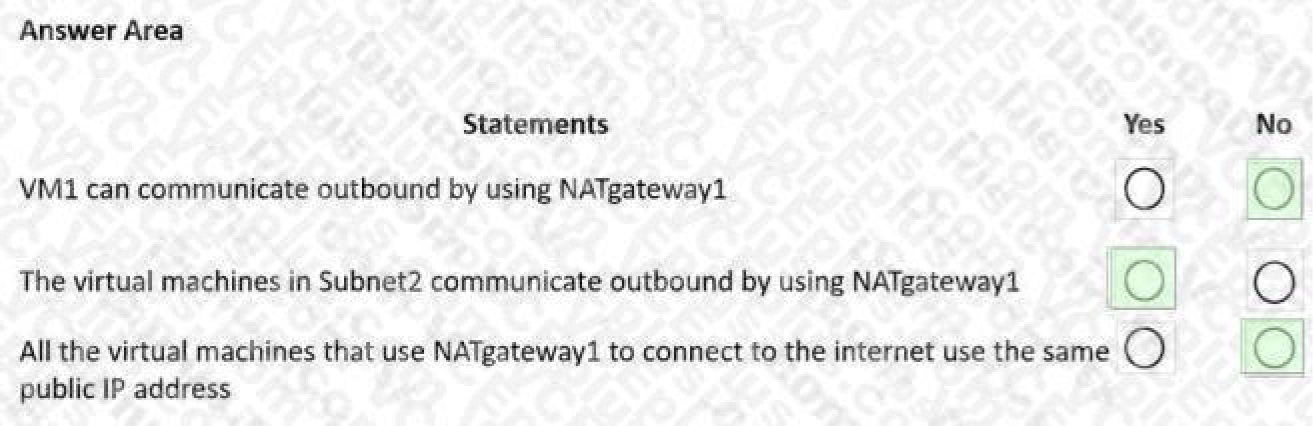
Hot Area:



Answer Area

Statements	Yes	No
VM1 can communicate outbound by using NATgateway1	○	○
The virtual machines in Subnet2 communicate outbound by using NATgateway1	○	○
All the virtual machines that use NATgateway1 to connect to the internet use the same public IP address	○	○

Answer Area:



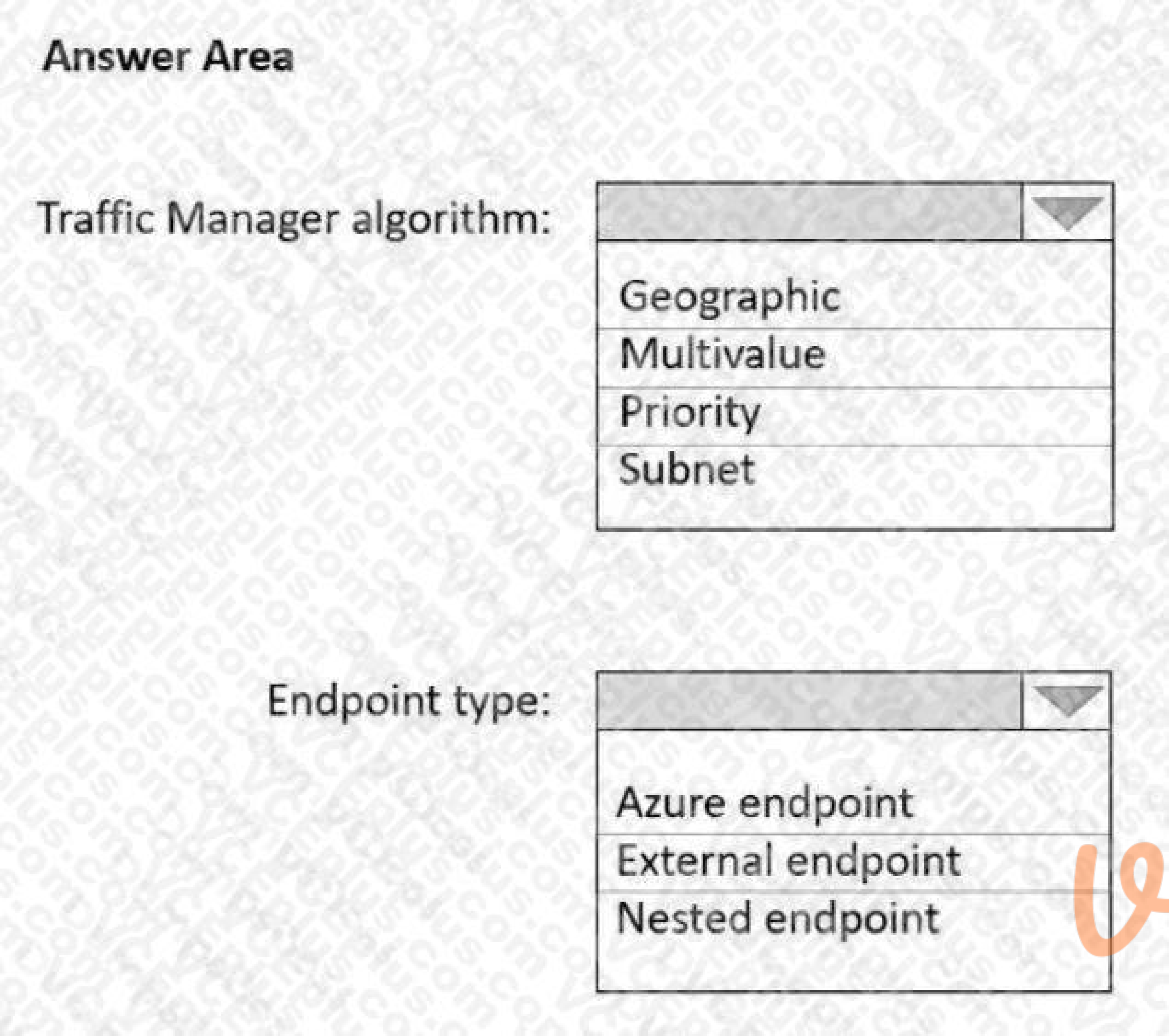
Answer Area

Statements	Yes	No
VM1 can communicate outbound by using NATgateway1	○	[✓ ○]
The virtual machines in Subnet2 communicate outbound by using NATgateway1	[✓ ○]	○
All the virtual machines that use NATgateway1 to connect to the internet use the same public IP address	○	[✓ ○]

Section:
Explanation:
Box 1: No
VM1 is in Zone2 whereas the NAT Gateway is in Zone1. The VM would need to be in the same zone as the NAT Gateway to be able to use it. Therefore, VM1 cannot use the NAT gateway.
Box 2: Yes
NATgateway1 is configured in the settings for Subnet2.
Box 3: No
The NAT gateway does not have a single public IP address, it has an IP prefix which means more than one IP address. The VMs the use the NAT Gateway can use different public IP addresses contained within the IP prefix.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource

QUESTION 33
HOTSPOT
Your company has 10 instances of a web service. Each instance is hosted in a different Azure region and is accessible through a public endpoint. The development department at the company is creating an application named App1. Every 10 minutes, App1 will use a list of endpoints and connect to the first available endpoint. You plan to use Azure Traffic Manager to maintain the list of endpoints.
You need to configure a Traffic Manager profile that will minimize the impact of DNS caching. What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

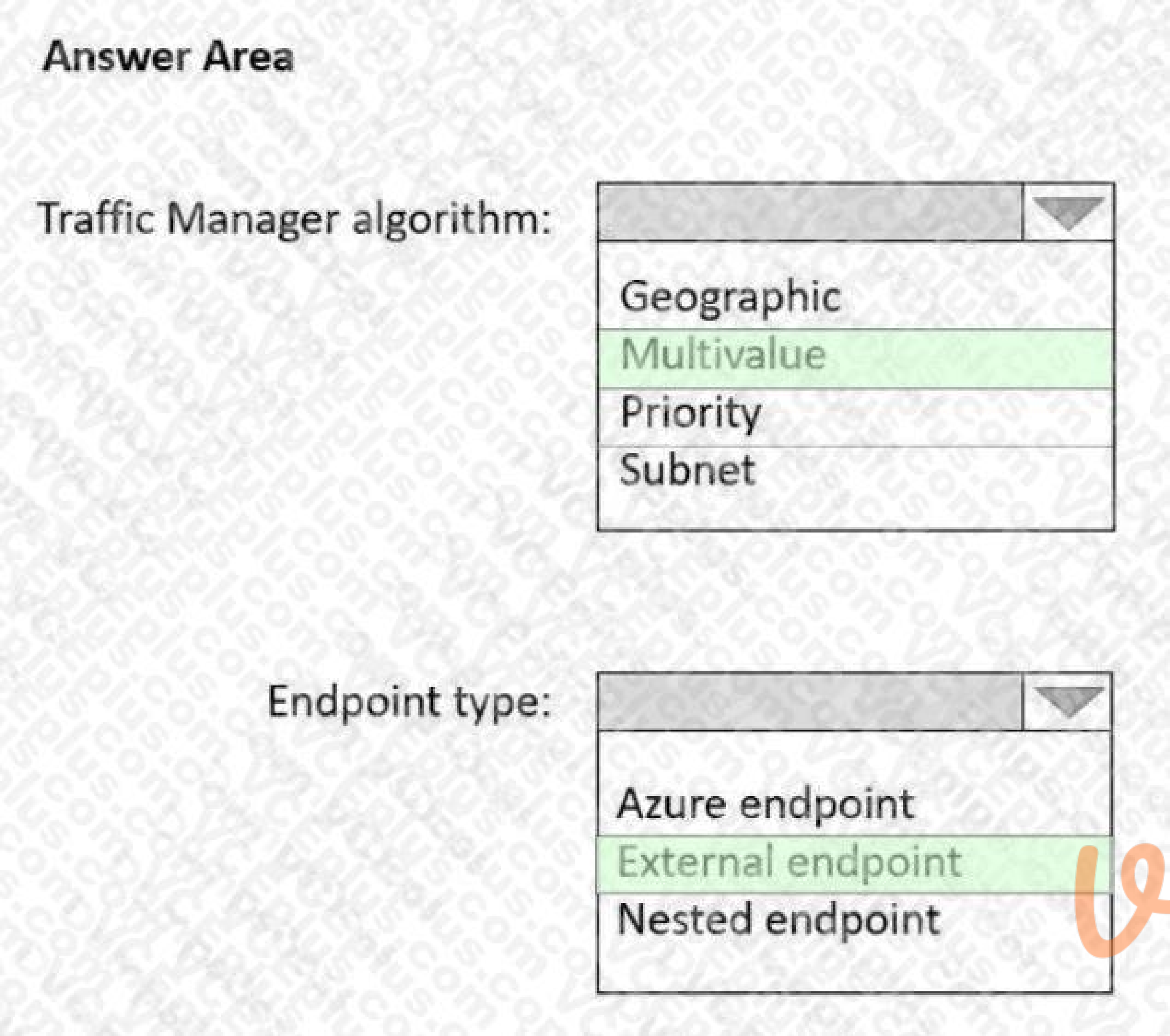
Traffic Manager algorithm:

- Geographic
- Multivalue
- Priority
- Subnet

Endpoint type:

- Azure endpoint
- External endpoint
- Nested endpoint

Answer Area:



Answer Area

Traffic Manager algorithm:

- Geographic
- [✓ Multivalue]
- Priority
- Subnet

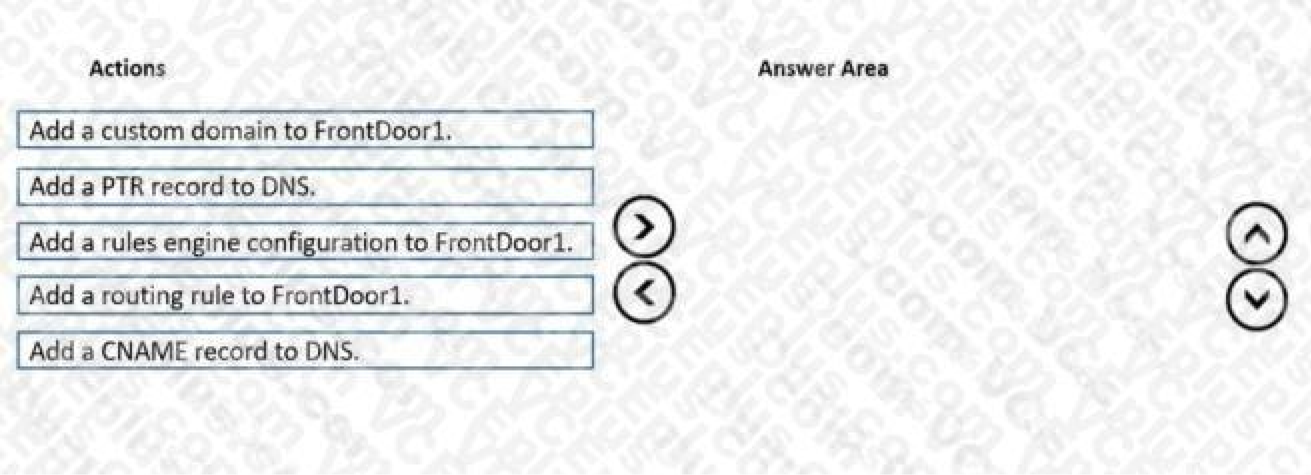
Endpoint type:

- Azure endpoint
- [✓ External endpoint]
- Nested endpoint

Section:
Explanation:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods https://docs.microsoft.com/enus/azure/traffic-manager/traffic-manager-endpoint-types

QUESTION 34
DRAG DROP
You have an Azure Front Door instance named FrontDoor1.
You deploy two instances of an Azure web app to different Azure regions.
You plan to provide access to the web app through FrontDoor1 by using the name app1.contoso.com.
You need to ensure that FrontDoor1 is the entry point for requests that use app1.contoso.com.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

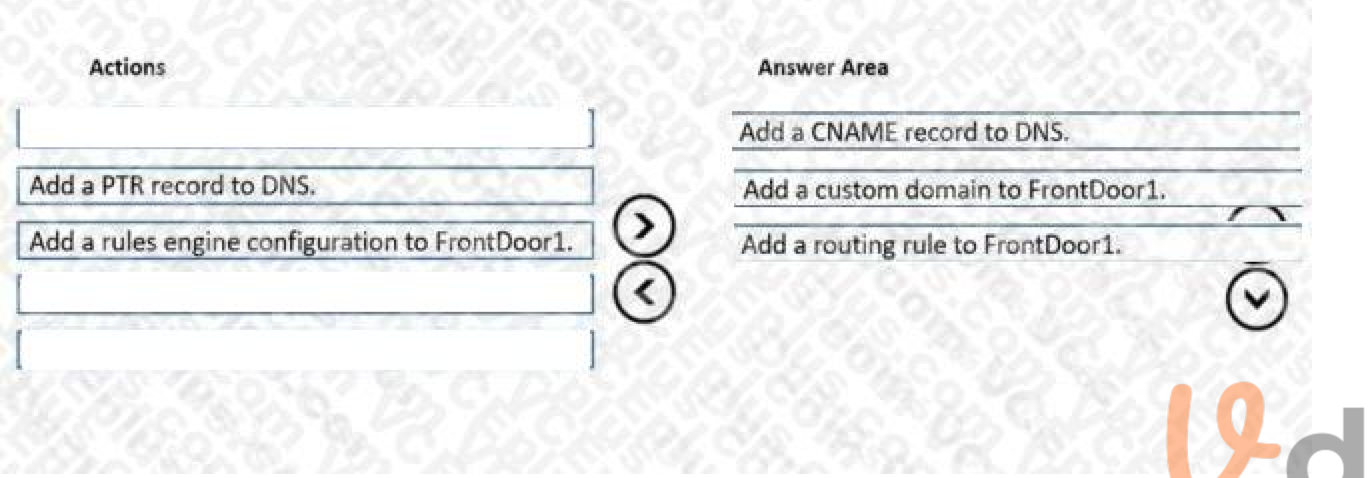


Actions

- Add a custom domain to FrontDoor1.
- Add a PTR record to DNS.
- Add a rules engine configuration to FrontDoor1.
- Add a routing rule to FrontDoor1.
- Add a CNAME record to DNS.

Answer Area

Correct Answer:



Actions

- Add a PTR record to DNS.
- Add a rules engine configuration to FrontDoor1.

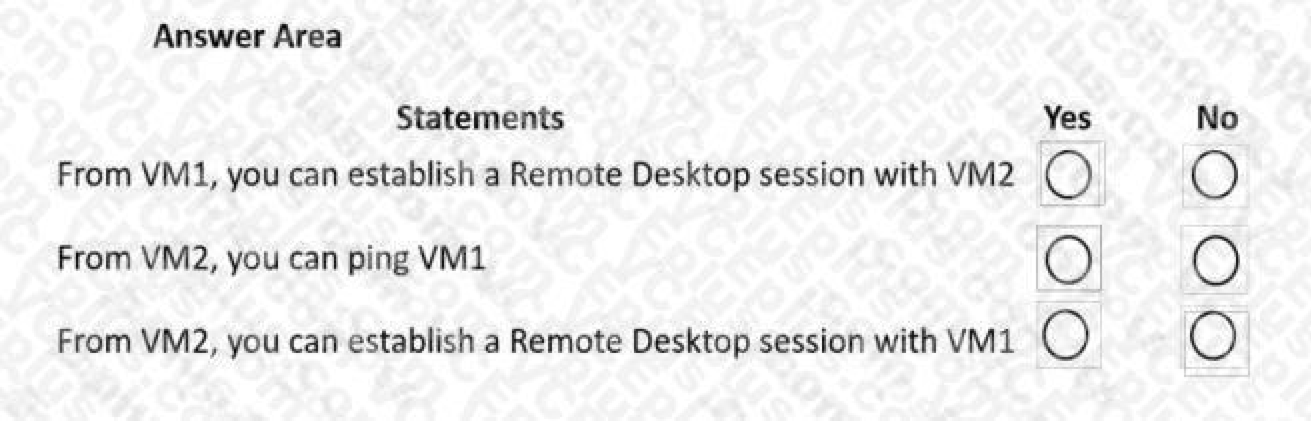
Answer Area

- Add a CNAME record to DNS.
- Add a custom domain to FrontDoor1.
- Add a routing rule to FrontDoor1.

Section:
Explanation:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#associate-the-custom-domain-with-your-frontdoor https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door

QUESTION 35
HOTSPOT
You create NSG10 and NSG11 to meet the network security requirements.
For each of the following statements, select Yes of the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

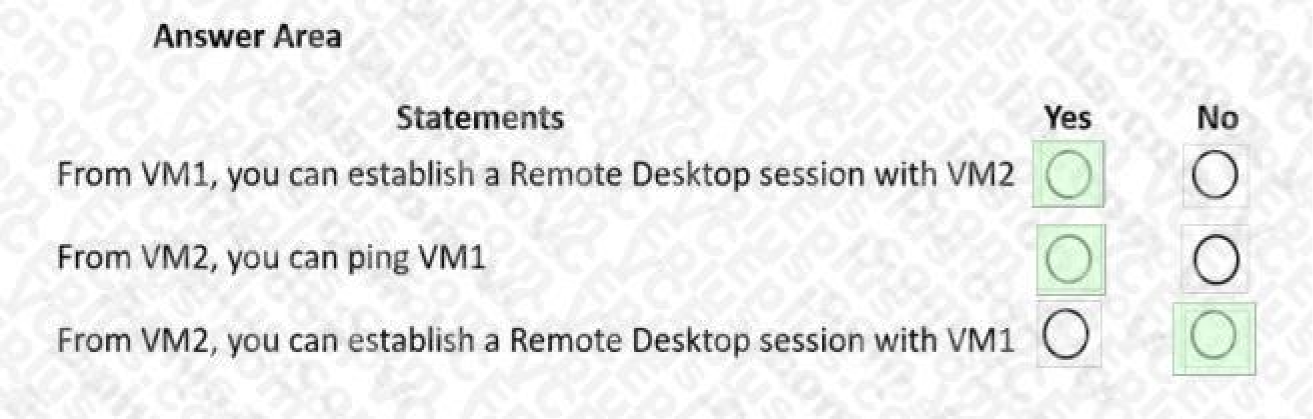
Hot Area:



Answer Area

Statements	Yes	No
From VM1, you can establish a Remote Desktop session with VM2	○	○
From VM2, you can ping VM1	○	○
From VM2, you can establish a Remote Desktop session with VM1	○	○

Answer Area:



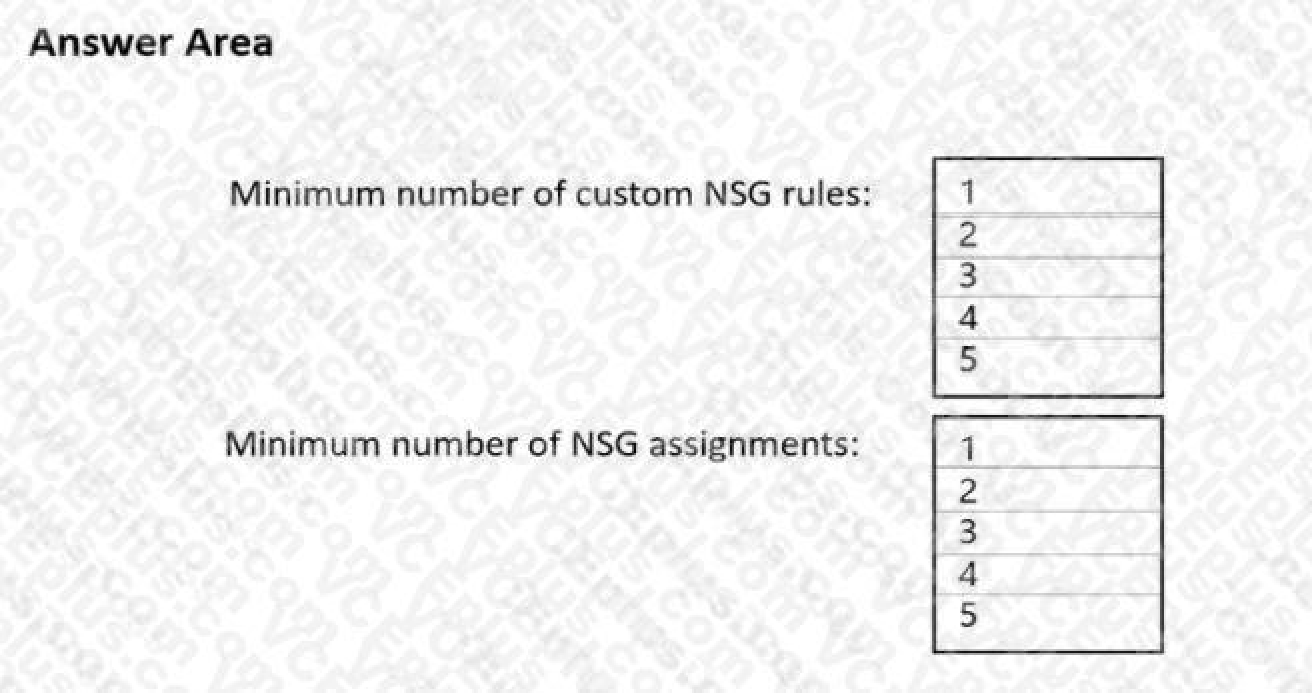
Answer Area

Statements	Yes	No
From VM1, you can establish a Remote Desktop session with VM2	[✓ ○]	○
From VM2, you can ping VM1	[✓ ○]	○
From VM2, you can establish a Remote Desktop session with VM1	○	[✓ ○]

Section:
Explanation:
Yes
subnet1(WM1->NSG1 outbound->NSG10 outbound)->subnet2(NSG1 inbound->NSG11 inbound>VM2) Yes
NSG10 blocks ICMP from VNet4 (source 10.10.0.0/16) but it is not blocked from VM2's subnet (VNet1/Subnet2).
No
NSG11 blocks RDP (port TCP 3389) destined for VirtualNetwork. VirtualNetwork is a service tag and means the address space of the virtual network (VNet1) which in this case is 10.1.0.0/16. Therefore, RDP traffic from subnet2 to anywhere else in VNet1 is blocked.

QUESTION 36
HOTSPOT
You need to restrict traffic from VMScaleSet1 to VMScaleSet2. The solution must meet the virtual networking requirements. What is the minimum number of custom NSG rules and NSG assignments required? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

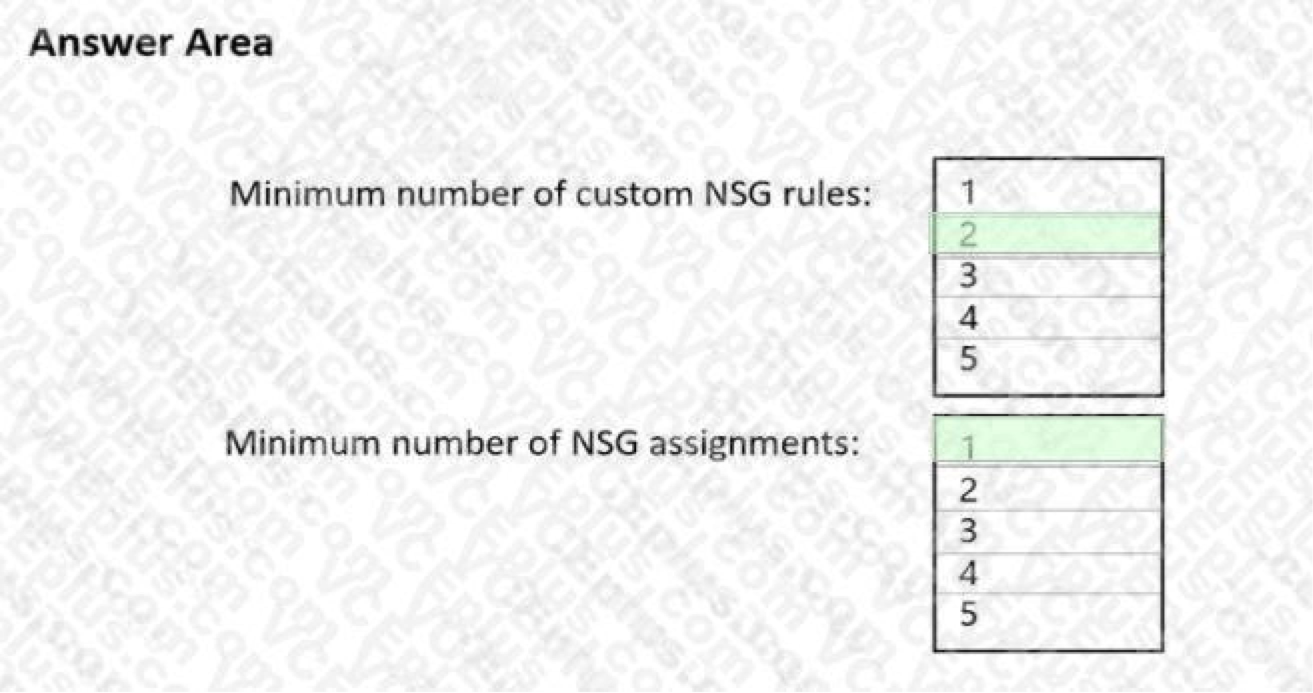


Answer Area

Minimum number of custom NSG rules:
1
2
3
4
5

Minimum number of NSG assignments:
1
2
3
4
5

Answer Area:



Answer Area

Minimum number of custom NSG rules:

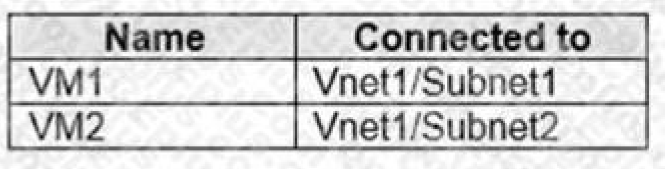
- 1
- [✓ 2]
- 3
- 4
- 5

Minimum number of NSG assignments:

- [✓ 1]
- 2
- 3
- 4
- 5

Section:
Explanation:
Box 2: One NSG
The minimum requirement is one NSG. You could attach the NSG to VMScaleSet1 and restrict outbound traffic, or you could attach the NSG to VMScaleSet2 and restrict inbound traffic. Either way you would need two custom NSG rules. Box 1: Two custom rules
With the NSG attached to VMScaleSet2, you would need to create a custom rule blocking all traffic from VMScaleSet1. Then you would need to create another custom rule with a higher priority than the first rule that allows traffic on port 443.
The default rules in the NSG will allow all other traffic to VMScaleSet2.

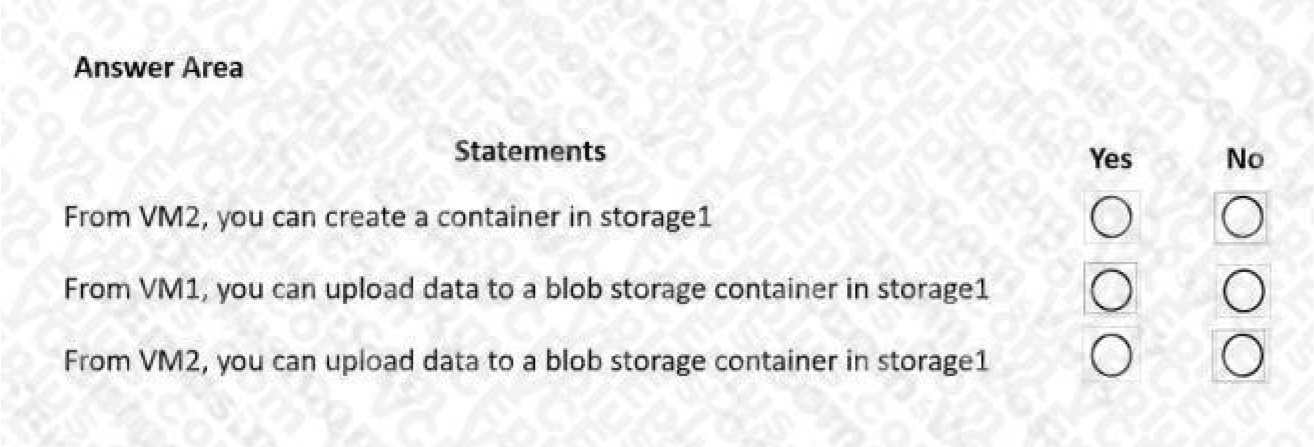
QUESTION 37
HOTSPOT
You have an Azure subscription that contains the virtual machines shown in the following table.



Name	Connected to
VM1	Vnet1/Subnet1
VM2	Vnet1/Subnet2

Subnet1 and Subnet2 are associated to a network security group (NSG) named NSG1 that has the following outbound rule:
Priority: 100
Port: Any
Protocol: Any
Source: Any
Destination: Storage Action: Deny
You create a private endpoint that has the following settings:
Name: Private1
Resource type: Microsoft.Storage/storageAccounts
Resource: storage1
Target sub-resource: blob
Virtual network: Vnet1 Subnet: Subnet1
For each of the following statements, select Yes of the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

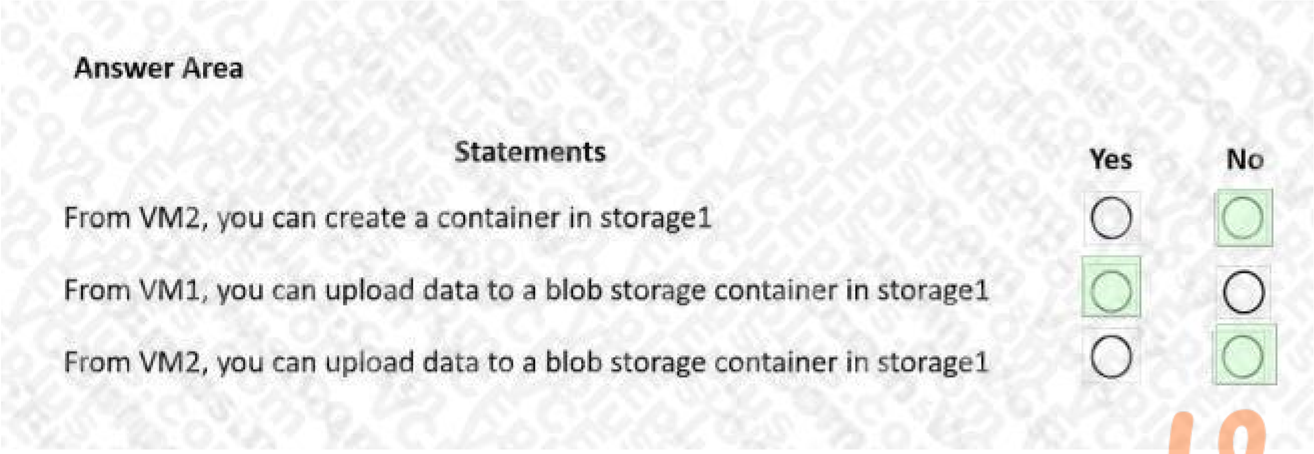
Hot Area:



Answer Area

Statements	Yes	No
From 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	○	○

Answer Area:

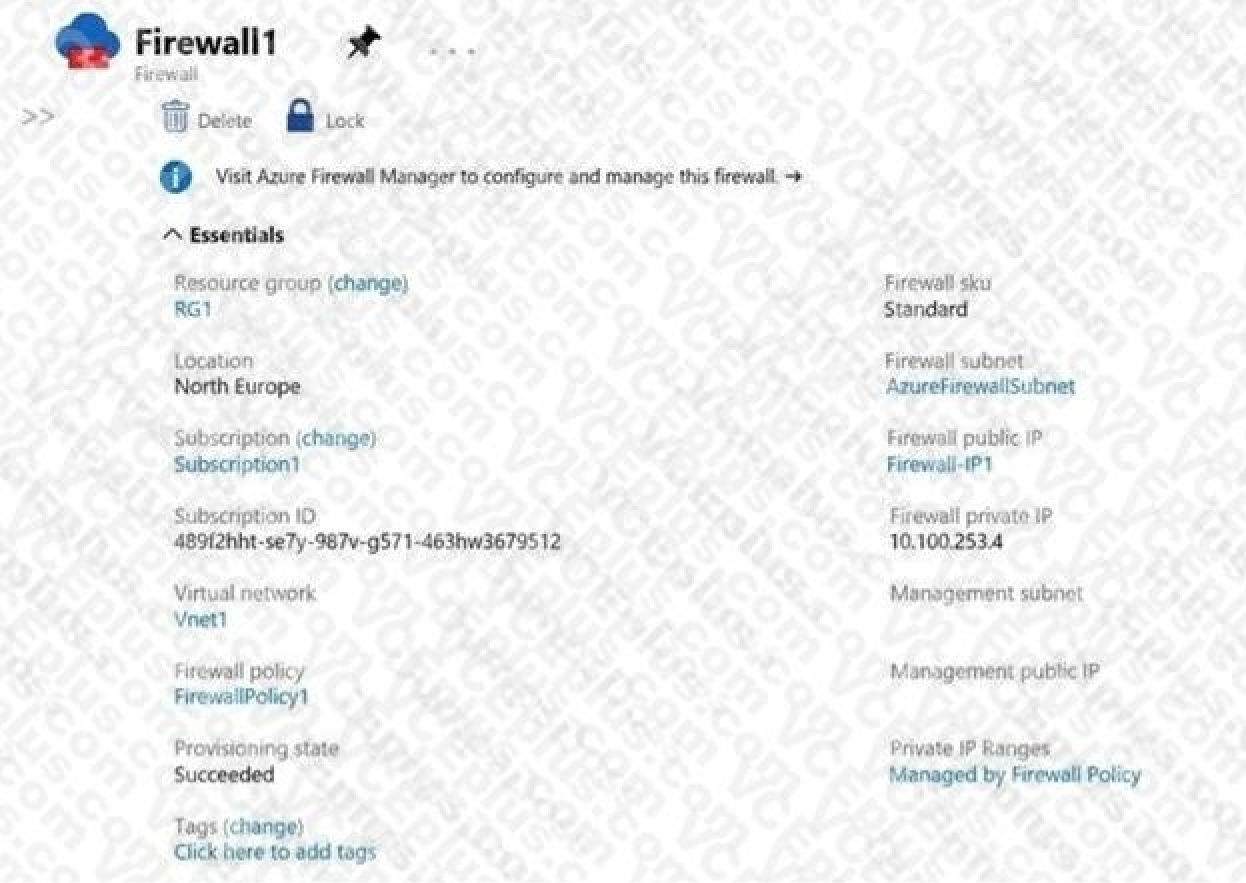


Answer Area

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	○	[✓ ○]

Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/private-link/disable-private-endpoint-network-policy

QUESTION 38
HOTSPOT
You have an Azure firewall shown in the following exhibit.



Firewall1

Firewall

Visit Azure Firewall Manager to configure and manage this firewall. →

Essentials

Resource group (change)
RG1

Location
North Europe

Subscription (change)
Subscription1

Subscription ID
489f2hht-se7y-987v-g571-463hw3679512

Virtual network
Vnet1

Firewall policy
FirewallPolicy1

Provisioning state
Succeeded

Tags (change)
Click here to add tags

Firewall sku
Standard

Firewall subnet
AzureFirewallSubnet

Firewall public IP
Firewall-IP1

Firewall private IP
10.100.253.4

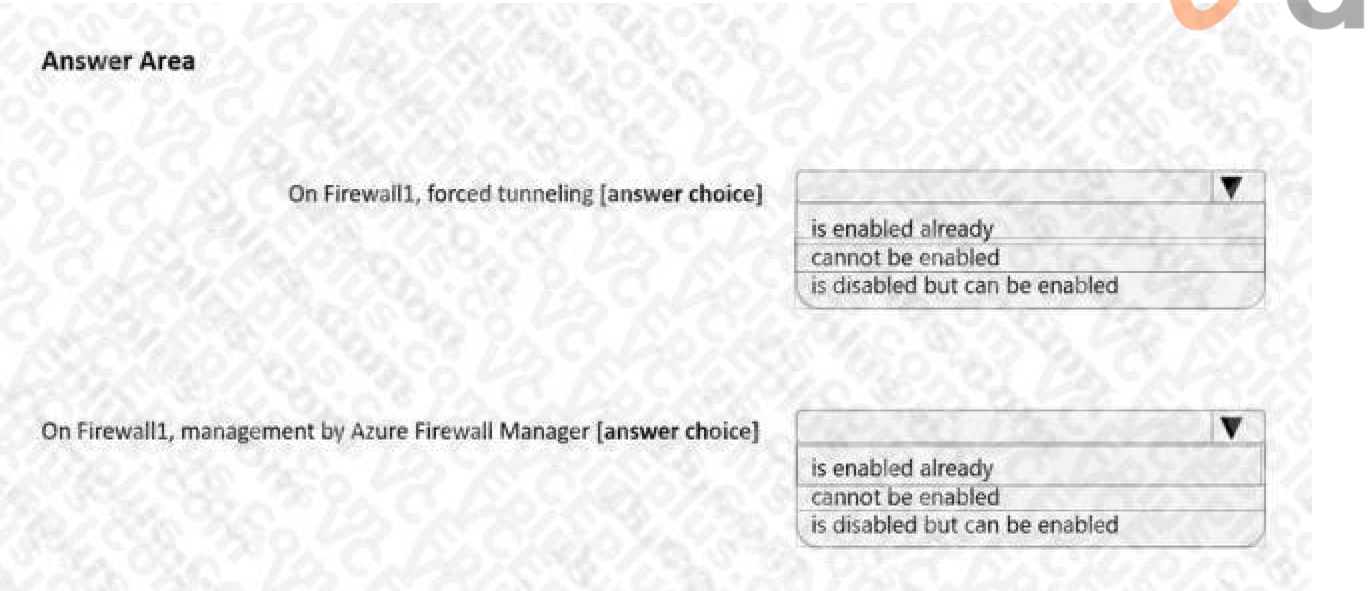
Management subnet

Management public IP

Private IP Ranges
Managed by Firewall Policy

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

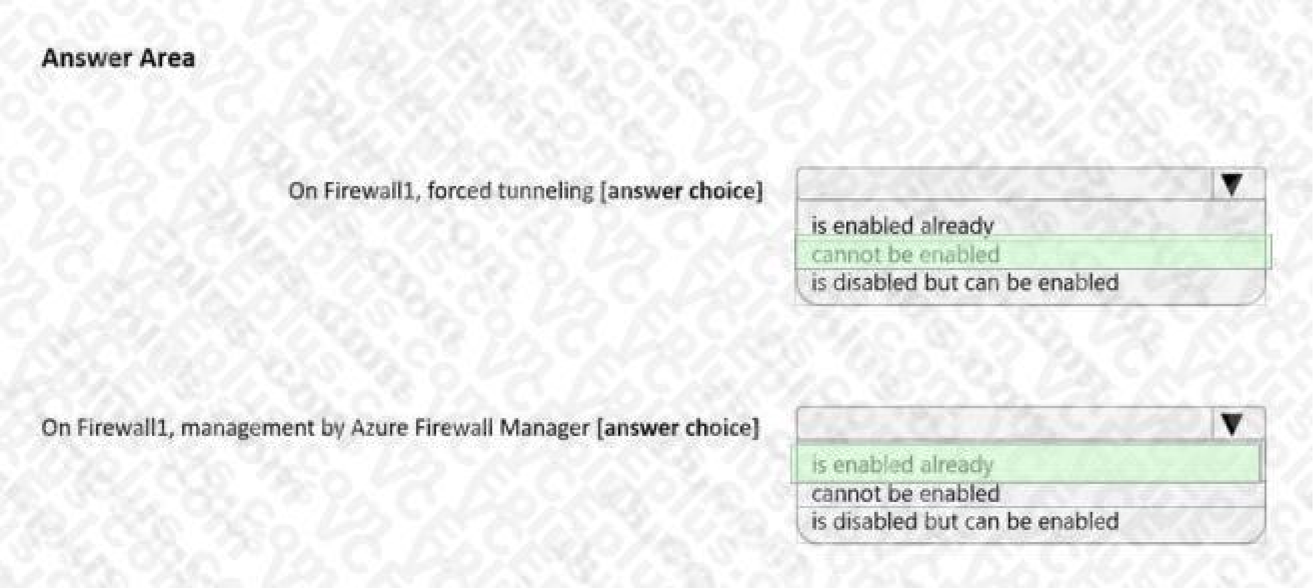
On Firewall1, forced tunneling [answer choice]

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

On Firewall1, management by Azure Firewall Manager [answer choice]

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

Answer Area:



Answer Area

On Firewall1, forced tunneling [answer choice]

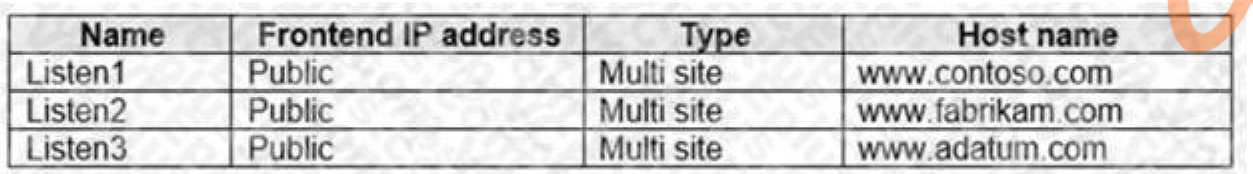
- is enabled already
- [✓ cannot be enabled]
- is disabled but can be enabled

On Firewall1, management by Azure Firewall Manager [answer choice]

- [✓ is enabled already]
- cannot be enabled
- is disabled but can be enabled

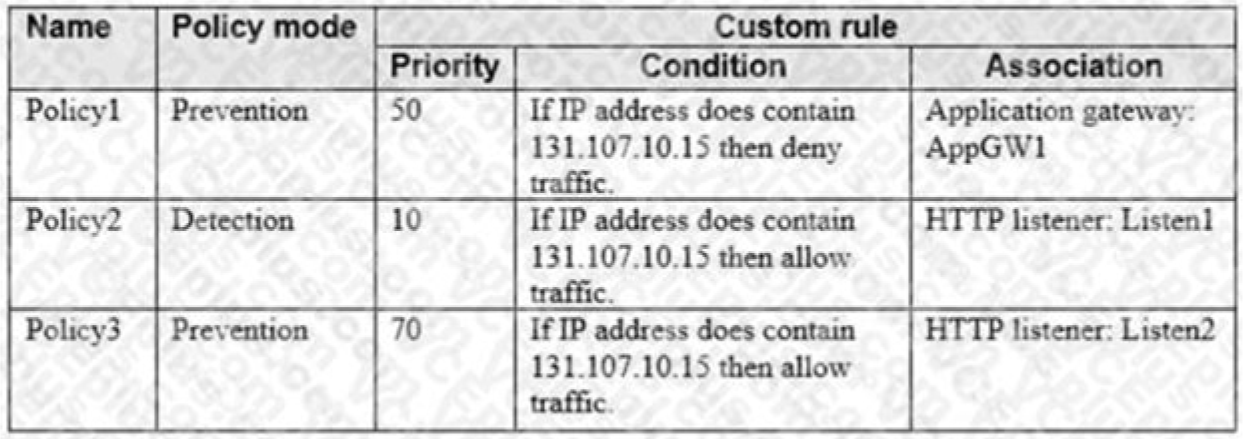
Section:
Explanation:
Box 1:
If forced tunneling was enabled, the Firewall Subnet would be named AzureFirewallManagementSubnet. Forced tunneling can only be enabled during the creation of the firewall. It cannot be enabled after the firewall has been deployed. Box 2:
The “Visit Azure Firewall Manager to configure and manage this firewall” link in the exhibit shows that the firewall is managed by Azure Firewall Manager.

QUESTION 39
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

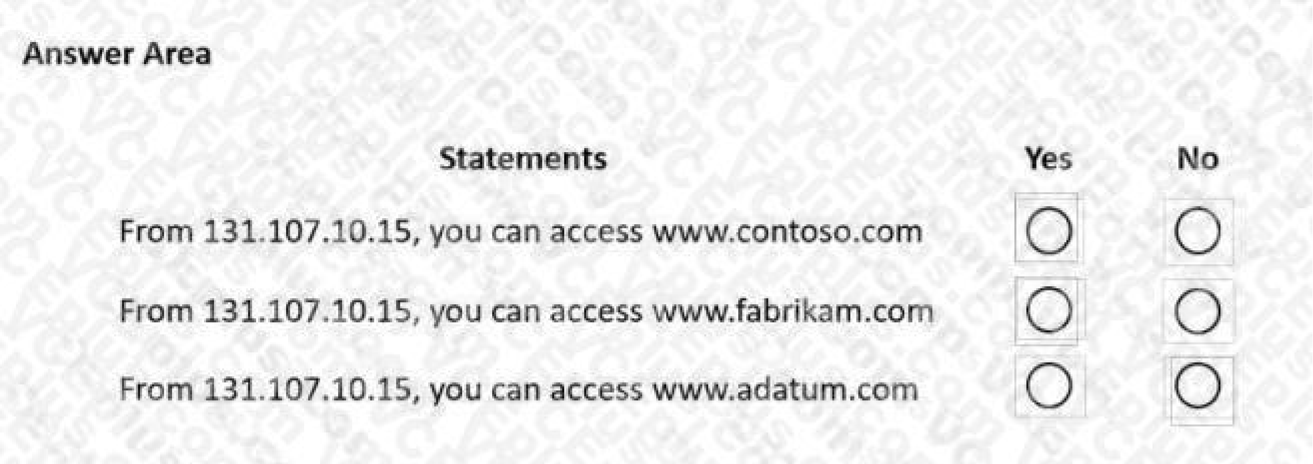
You create Azure Web Application Firewall (WAF) policies for AppGW1 as shown in the following table.



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.

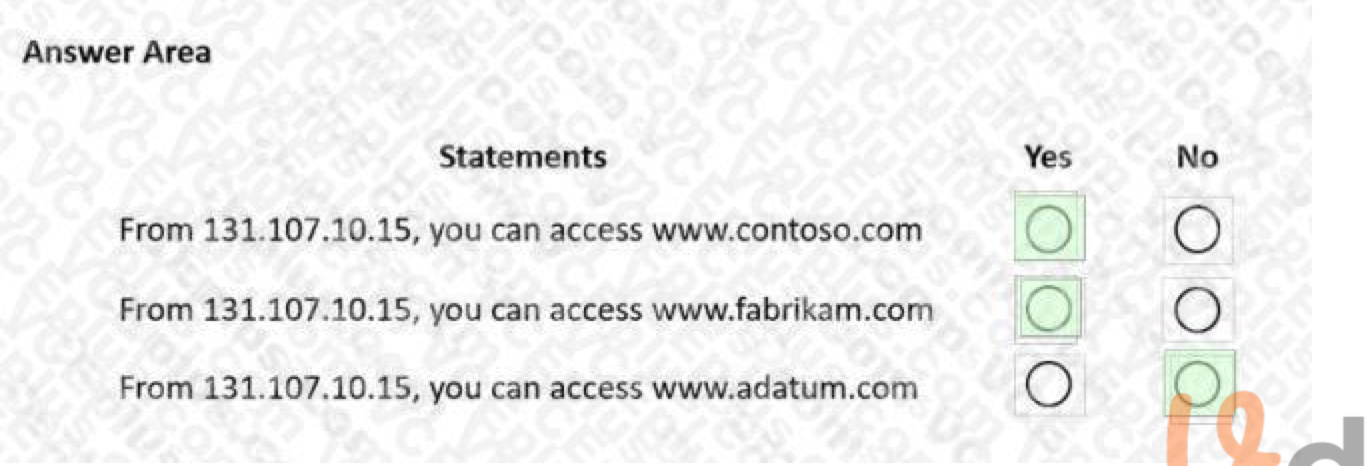
Hot Area:



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	○	○

Answer Area:

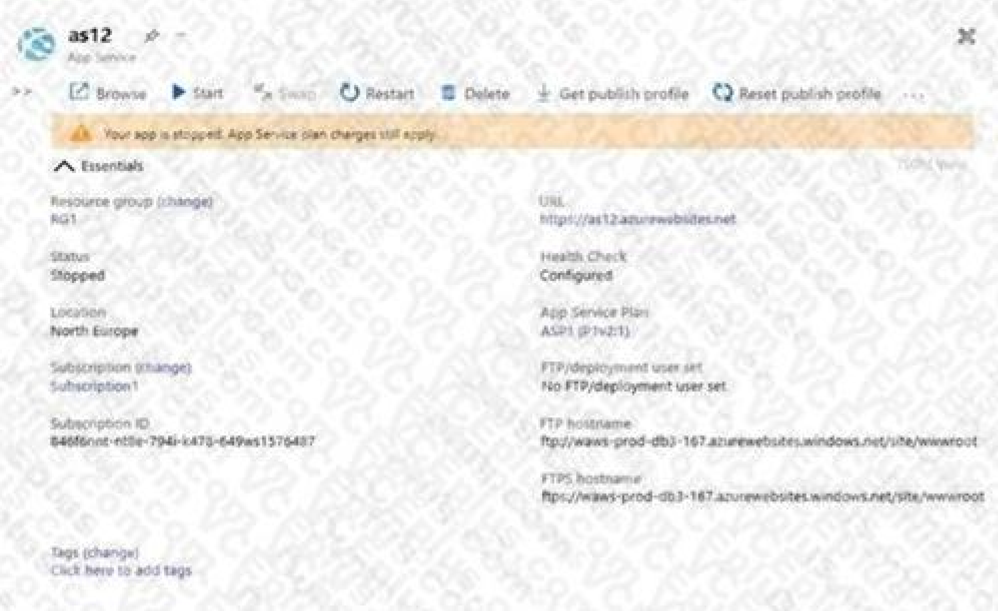


Answer Area

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	○	●

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

QUESTION 40
HOTSPOT
You have the Azure App Service app shown in the App Service exhibit.



Your app is stopped. App Service plan charges still apply.

Resource group (change)
RG1

Status
Stopped

Location
North Europe

Subscription (change)
Subscription1

Subscription ID
846f6nnt-n8le-794i-k478-649ws1576487

Tags (change)
Click here to add tags

URL
https://as12.azurewebsites.net

Health Check
Configured

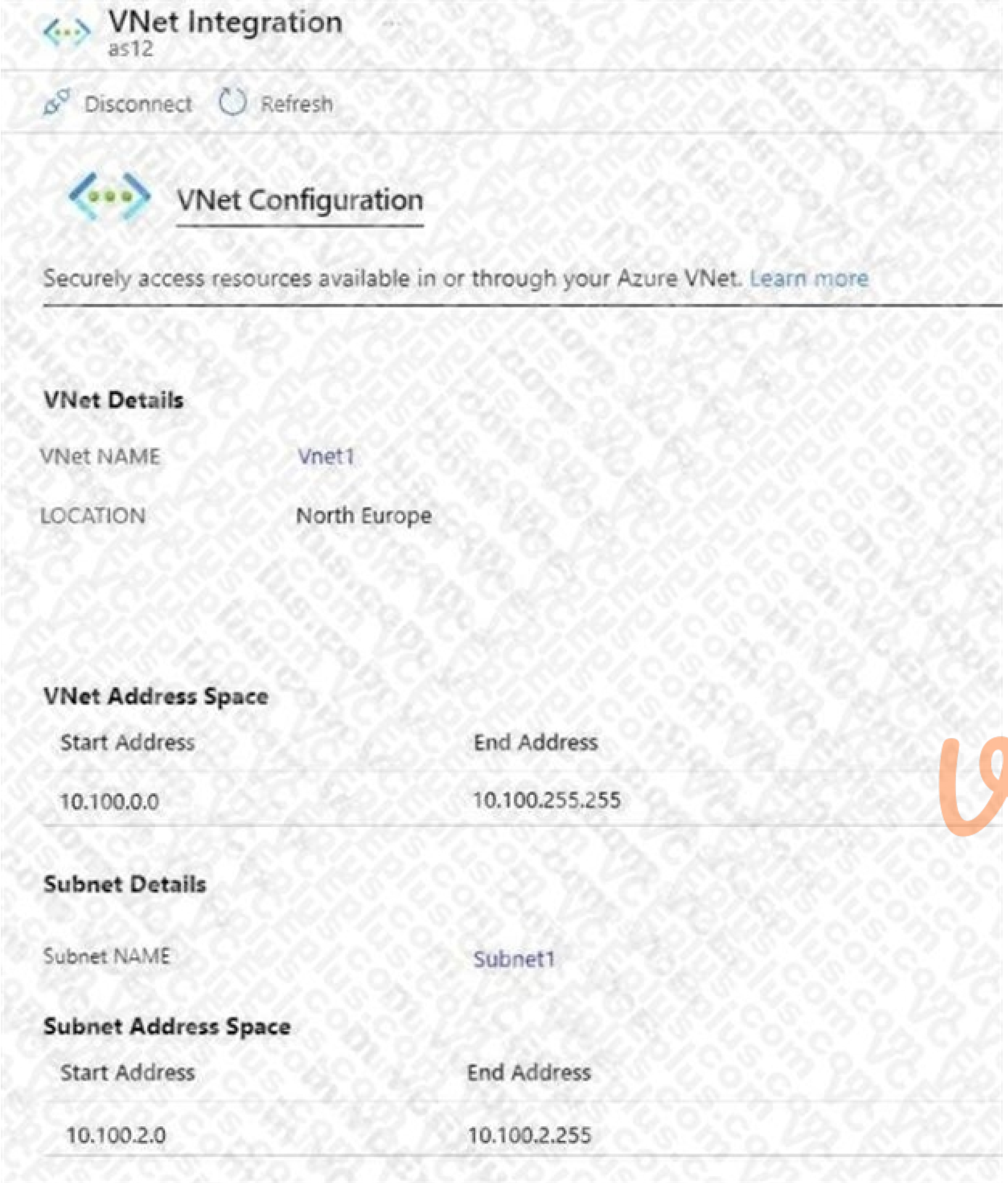
App Service Plan
ASP1 (P1v2:1)

FTP/deployment user set
No FTP/deployment user set

FTP hostname
ftp://waws-prod-db3-167.azurewebsites.windows.net/site/wwwroot

FTPS hostname
ftps://waws-prod-db3-167.azurewebsites.windows.net/site/wwwroot

The VNet Integration settings for as12 are configured as shown in the Vnet Integration exhibit.



VNet Integration
as12

Disconnect Refresh

VNet Configuration

Securely access resources available in or through your Azure VNet. Learn more

VNet Details

VNet NAME Vnet1

LOCATION North Europe

VNet Address Space

Start Address	End Address
10.100.0.0	10.100.255.255

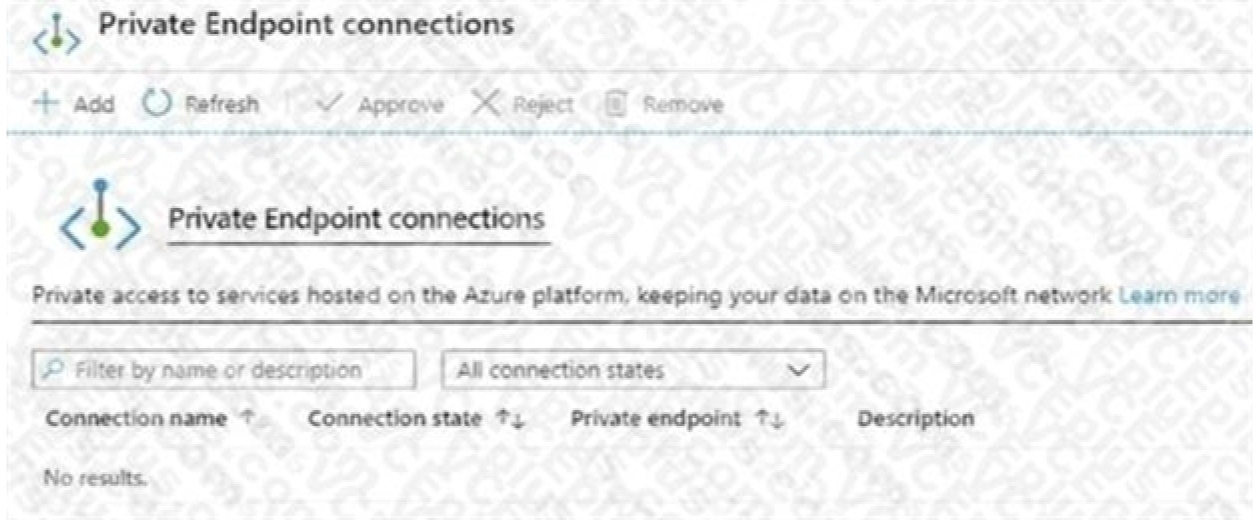
Subnet Details

Subnet NAME Subnet1

Subnet Address Space

Start Address	End Address
10.100.2.0	10.100.2.255

The Private Endpoint connections settings for as12 are configured as shown in the Private Endpoint connections exhibit.



Private Endpoint connections

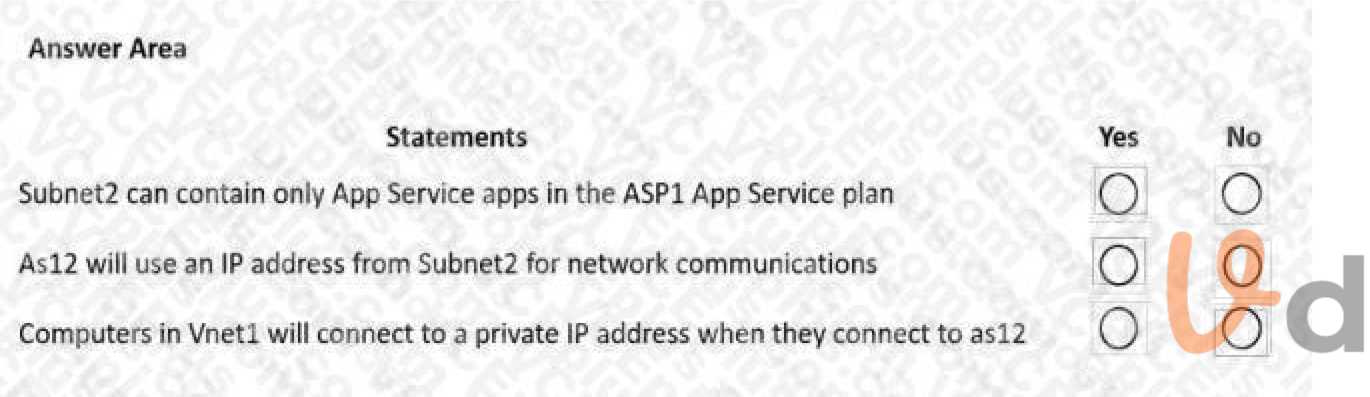
Private Endpoint connections

Private access to services hosted on the Azure platform, keeping your data on the Microsoft network Learn more

Connection name ↑	Connection state ↑↓	Private endpoint ↑↓	Description
No results.			

For each of the following statements, select Yes of the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

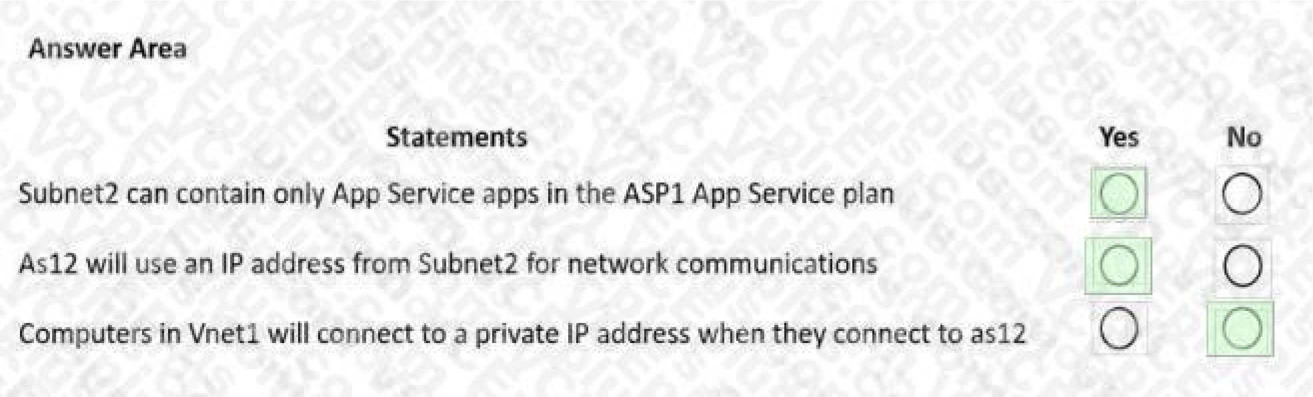
Hot Area:



Answer Area

Statements	Yes	No
Subnet2 can contain only App Service apps in the ASP1 App Service plan	○	○
As12 will use an IP address from Subnet2 for network communications	○	○
Computers in Vnet1 will connect to a private IP address when they connect to as12	○	○

Answer Area:



Answer Area

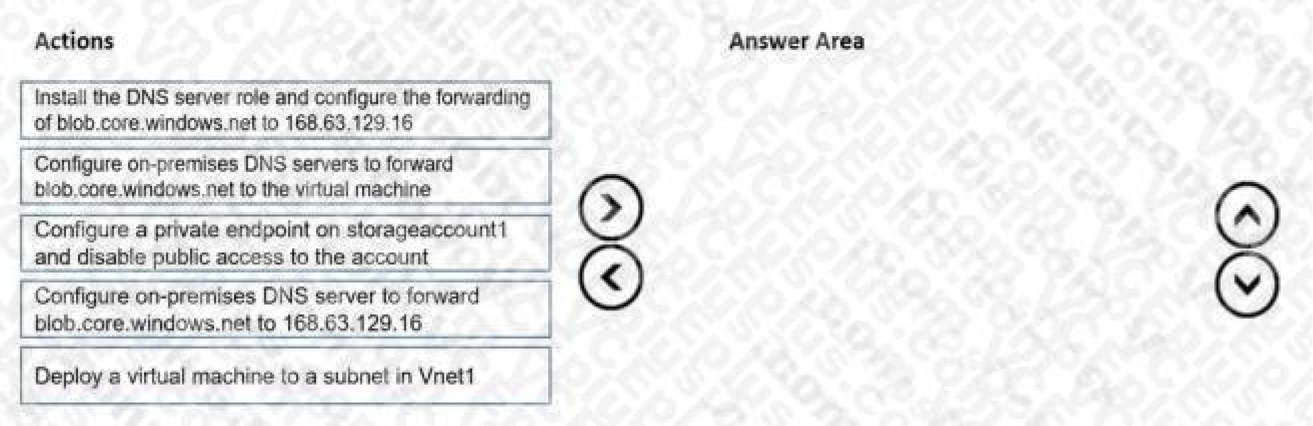
Statements	Yes	No
Subnet2 can contain only App Service apps in the ASP1 App Service plan	●	○
As12 will use an IP address from Subnet2 for network communications	●	○
Computers in Vnet1 will connect to a private IP address when they connect to as12	○	●

Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet

QUESTION 41
DRAG DROP
You have an Azure virtual network named Vnet1 that connects to an on-premises network.
You have an Azure Storage account named storageaccount1 that contains blob storage.
You need to configure a private endpoint for the blob storage. The solution must meet the following requirements:
Ensure that all on-premises users can access storageaccount1 through the private endpoint. Prevent access to storageaccount1 from being interrupted. Which four actions should you perform in sequence? To answer, move

the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

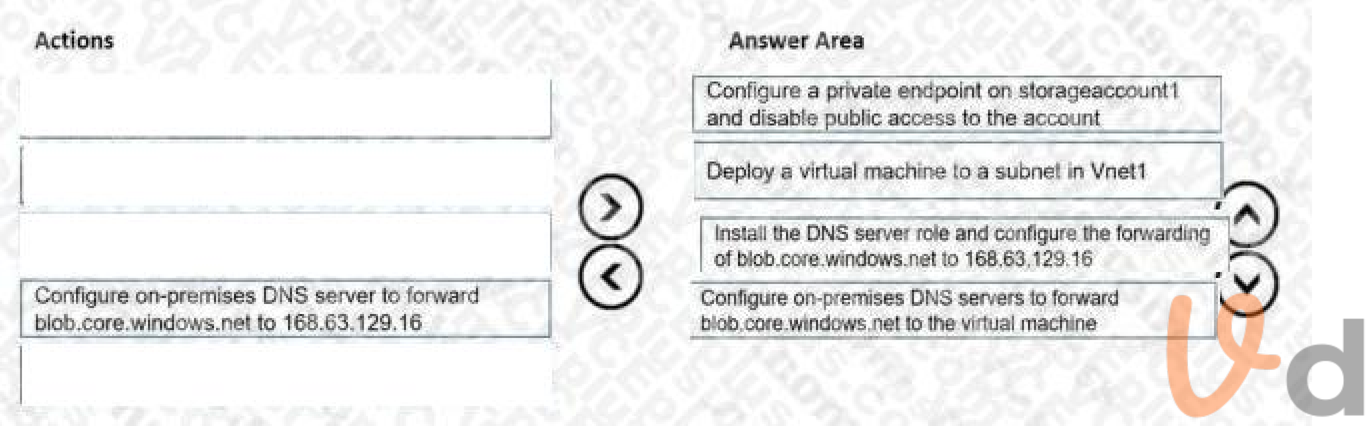


Actions

- Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
- Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine
- Configure a private endpoint on storageaccount1 and disable public access to the account
- Configure on-premises DNS server to forward blob.core.windows.net to 168.63.129.16
- Deploy a virtual machine to a subnet in Vnet1

Answer Area

Correct Answer:



Actions

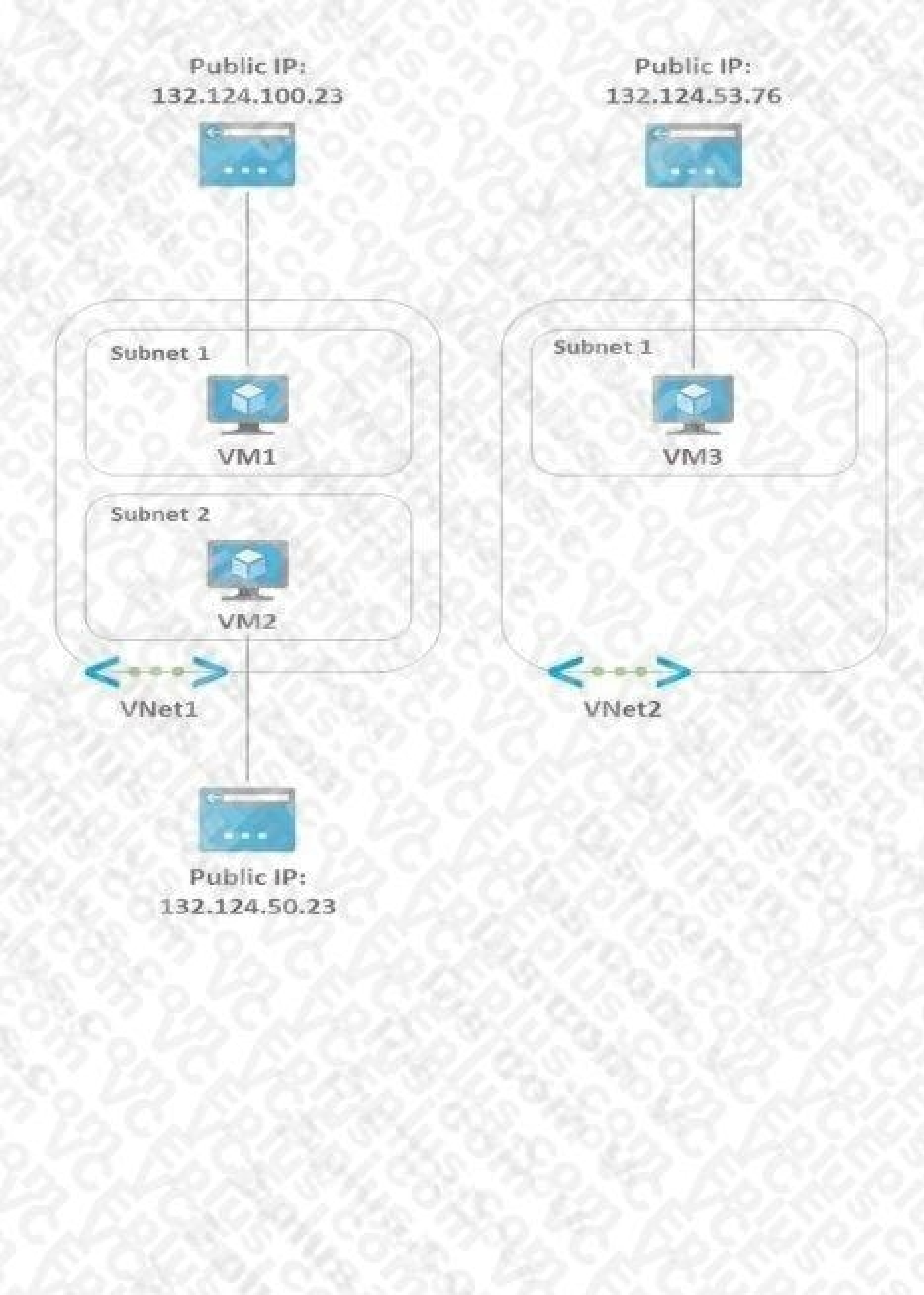
- Configure on-premises DNS server to forward blob.core.windows.net to 168.63.129.16

Answer Area

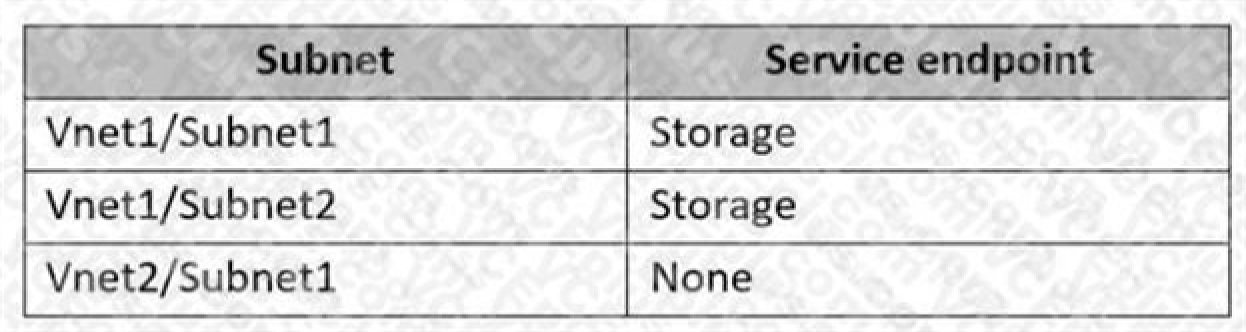
- Configure a private endpoint on storageaccount1 and disable public access to the account
- Deploy a virtual machine to a subnet in Vnet1
- Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
- Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine

Section:
Explanation:
168.63.129.16 is the IP address of Azure DNS which hosts Azure Private DNS zones. It is only accessible from within a VNet which is why we need to forward on-prem DNS requests to the VM running DNS in the VNet. The VM will then forward the request to Azure DNS for the IP of the storage account private endpoint.
Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints

QUESTION 42
HOTSPOT
You have the Azure environment shown in the Azure Environment exhibit.

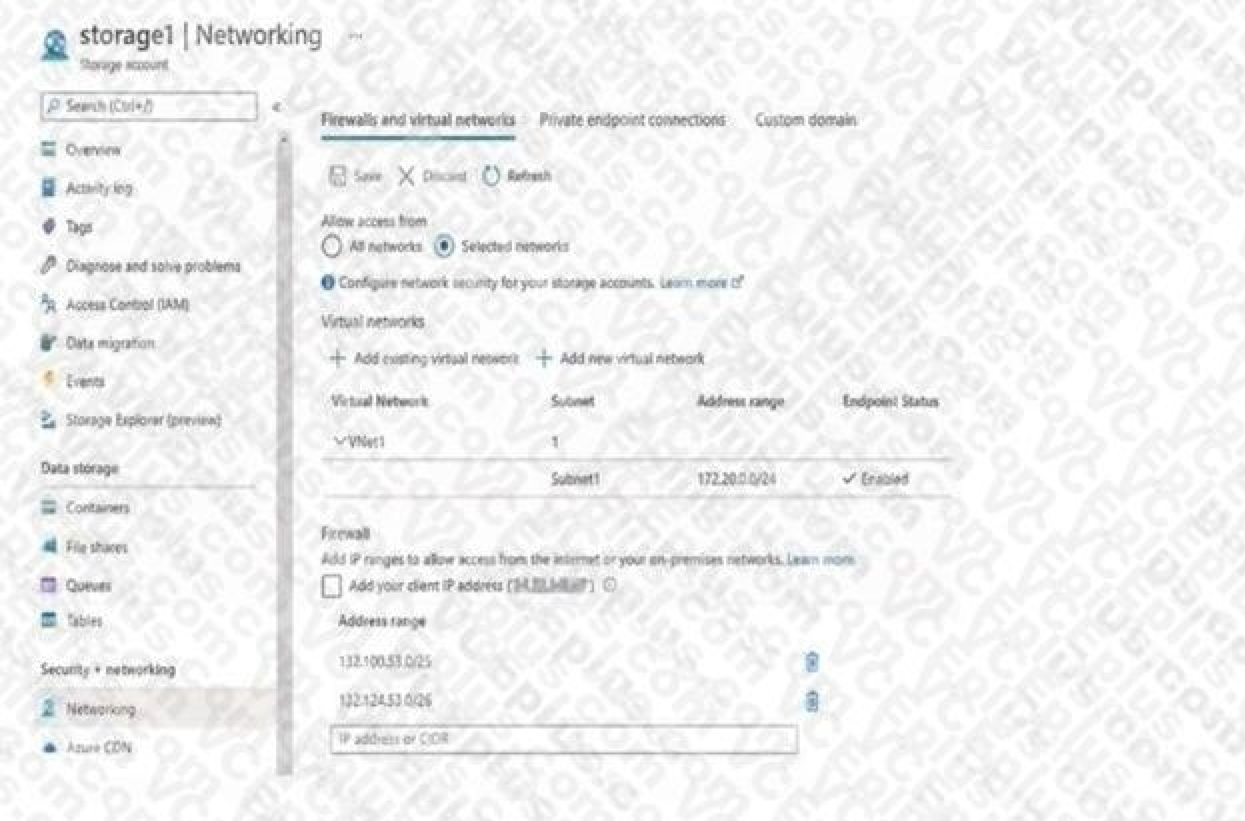


The settings for each subnet are shown in the following table.



Subnet	Service endpoint
Vnet1/Subnet1	Storage
Vnet1/Subnet2	Storage
Vnet2/Subnet1	None

The Firewalls and virtual networks settings for storage1 are configured as shown in the Storage1 exhibit.



Allow access from

○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more

Virtual networks

Virtual Network	Subnet	Address range	Endpoint Status
VNet1	1		
	Subnet1	172.20.0.0/24	✓ Enabled

Firewall

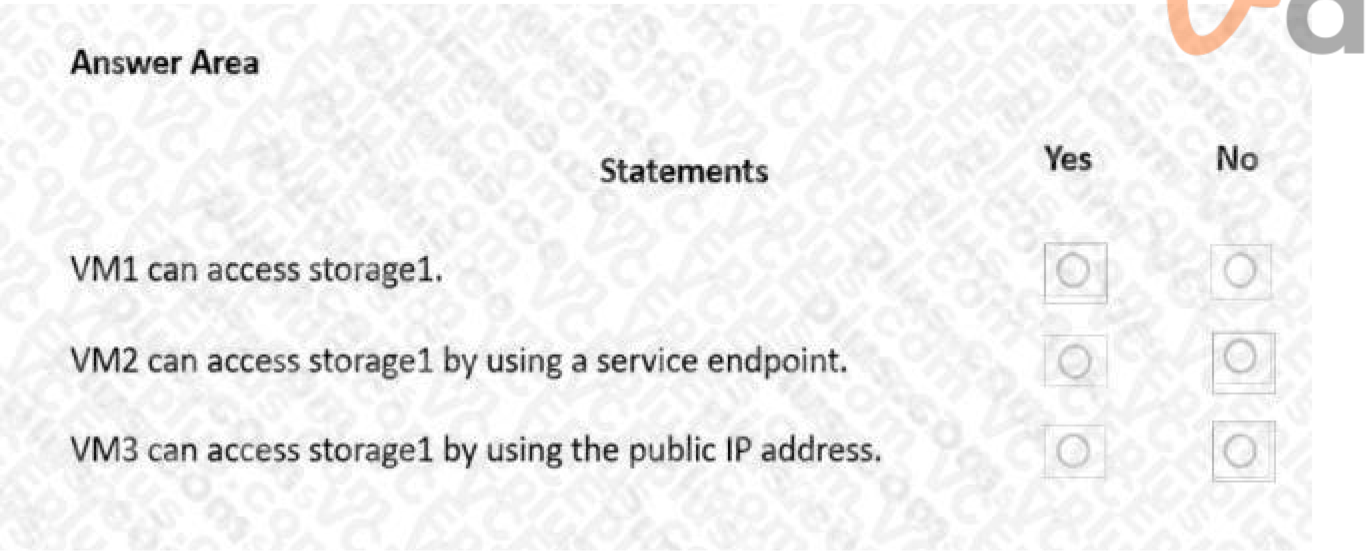
Add IP ranges to allow access from the internet or your on-premises networks. Learn more

□ Add your client IP address ('[illegible]')

Address range
132.100.53.0/25
132.124.53.0/26

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

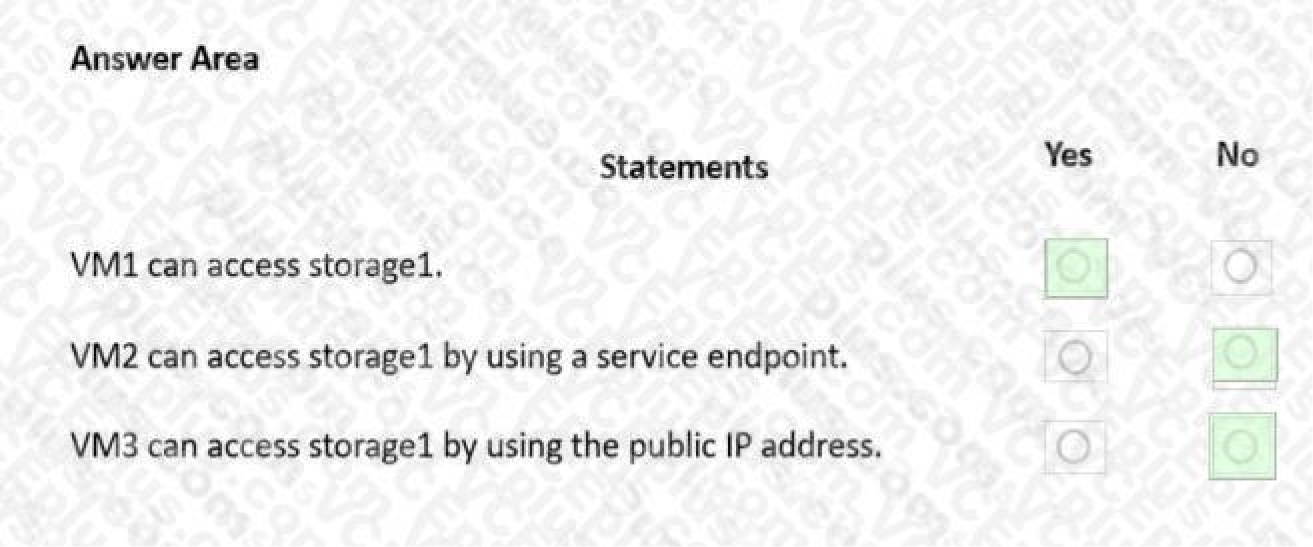
Hot Area:



Answer Area

Statements	Yes	No
VM1 can access storage1.	○	○
VM2 can access storage1 by using a service endpoint.	○	○
VM3 can access storage1 by using the public IP address.	○	○

Answer Area:

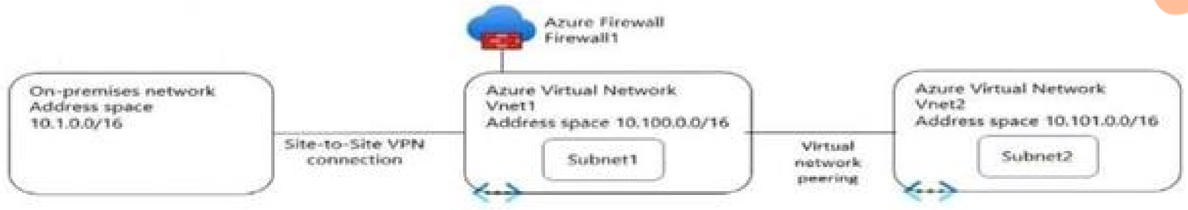


Answer Area

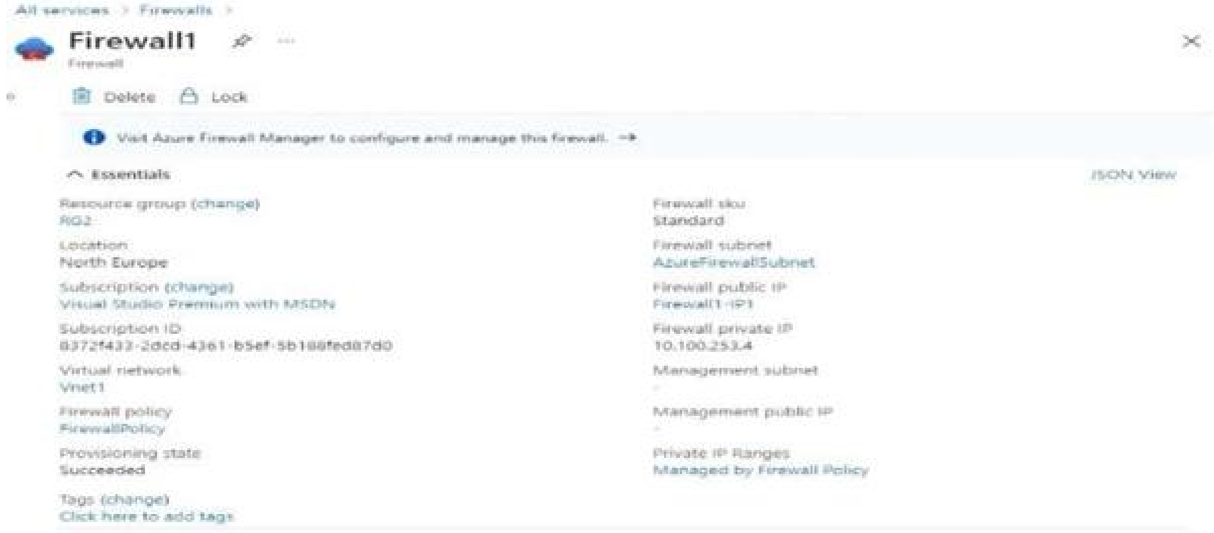
Statements	Yes	No
VM1 can access storage1.	●	○
VM2 can access storage1 by using a service endpoint.	○	●
VM3 can access storage1 by using the public IP address.	○	●

Section:
Explanation:
Box 1: Yes
The firewall allows VNet1\Subnet1 through the service endpoint.
Box 2: No
The firewall does not allow VNet1\Subnet2 through the service endpoint.
Box 3: No
The firewall allows 132.124.53.0/26 which means it allows all IP addresses between 132.124.53.0 and 132.124.53.63. The public IP of VM3 is 132.124.53.76 which is outside the allowed range.

QUESTION 43
HOTSPOT
You have the network topology shown in the Topology exhibit. (Click the Topology tab.)



You have the Azure firewall shown in the Firewall 1 exhibit. (Click the Firewall tab.)



Firewall1
Firewall

Visit Azure Firewall Manager to configure and manage this firewall. →

Essentials

Resource group (change)
RG2

Location
North Europe

Subscription (change)
Visual Studio Premium with MSDN

Subscription ID
8372f433-2dcd-4361-b5ef-5b188fed87d0

Virtual network
Vnet1

Firewall policy
FirewallPolicy

Provisioning state
Succeeded

Tags (change)
Click here to add tags

Firewall sku
Standard

Firewall subnet
AzureFirewallSubnet

Firewall public IP
Firewall1-IP1

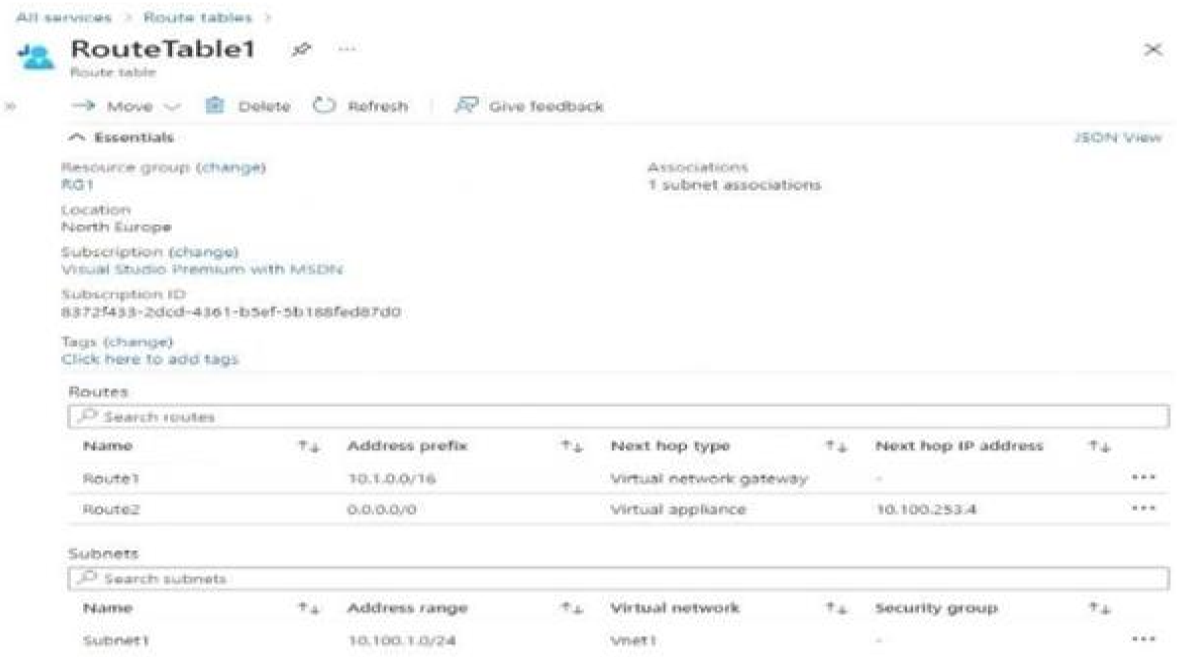
Firewall private IP
10.100.253.4

Management subnet
-

Management public IP
-

Private IP Ranges
Managed by Firewall Policy

You have the route table shown in the RouteTable1 exhibit. (Click the RouteTable1 tab.)



All services > Route tables >

RouteTable1

Route table

^ Essentials

Resource group (change)
RG1

Location
North Europe

Subscription (change)
Visual Studio Premium with MSDN

Subscription ID
8372f433-2dcd-4361-b5ef-5b188fed87d0

Tags (change)
Click here to add tags

Associations
1 subnet associations

Routes

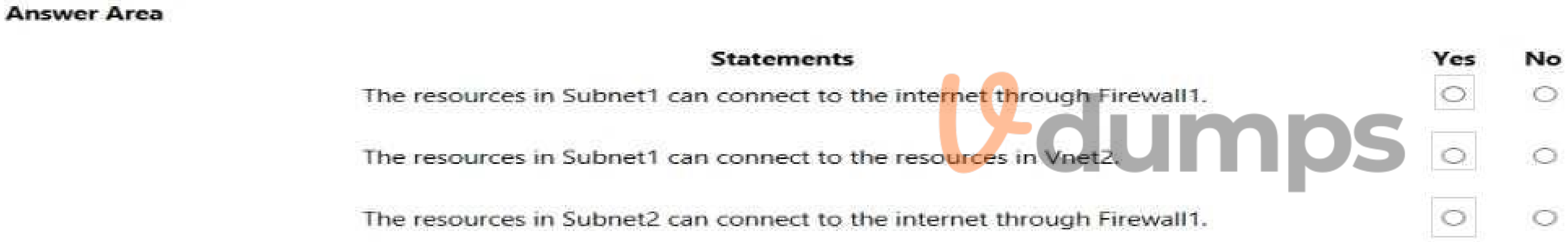
Name	Address prefix	Next hop type	Next hop IP address
Route1	10.1.0.0/16	Virtual network gateway	-
Route2	0.0.0.0/0	Virtual appliance	10.100.253.4

Subnets

Name	Address range	Virtual network	Security group
Subnet1	10.100.1.0/24	Vnet1	-

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

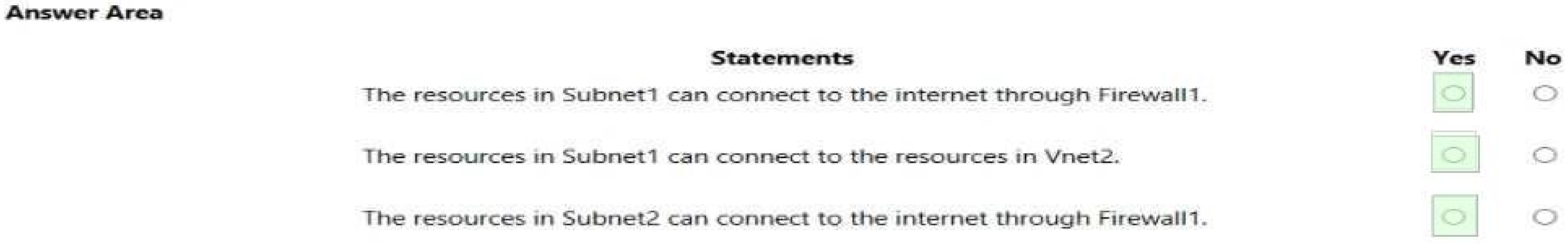
Hot Area:



Answer Area

Statements	Yes	No
The resources in Subnet1 can connect to the internet through Firewall1.	○	○
The resources in Subnet1 can connect to the resources in Vnet2.	○	○
The resources in Subnet2 can connect to the internet through Firewall1.	○	○

Answer Area:



Answer Area

Statements	Yes	No
The resources in Subnet1 can connect to the internet through Firewall1.	[✓ ○]	○
The resources in Subnet1 can connect to the resources in Vnet2.	[✓ ○]	○
The resources in Subnet2 can connect to the internet through Firewall1.	[✓ ○]	○

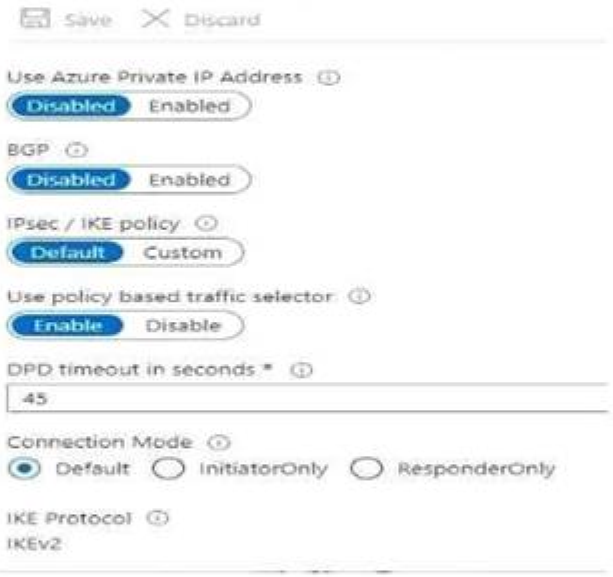
Section:
Explanation:

QUESTION 44

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.



Use Azure Private IP Address
[✓ Disabled] Enabled

BGP
[✓ Disabled] Enabled

IPsec / IKE policy
[✓ Default] Custom

Use policy based traffic selector
[✓ Enable] Disable

DPD timeout in seconds *
45

Connection Mode
● Default ○ InitiatorOnly ○ ResponderOnly

IKE Protocol
IKEv2

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 Use Azure Private IP Address to Enabled

B. Set IPsec / IKE policy to Custom.

C. Set Connection Mode to ResponderOnly

D. Set BGP to Enabled

Correct Answer: A
Section:

QUESTION 45

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
Section:

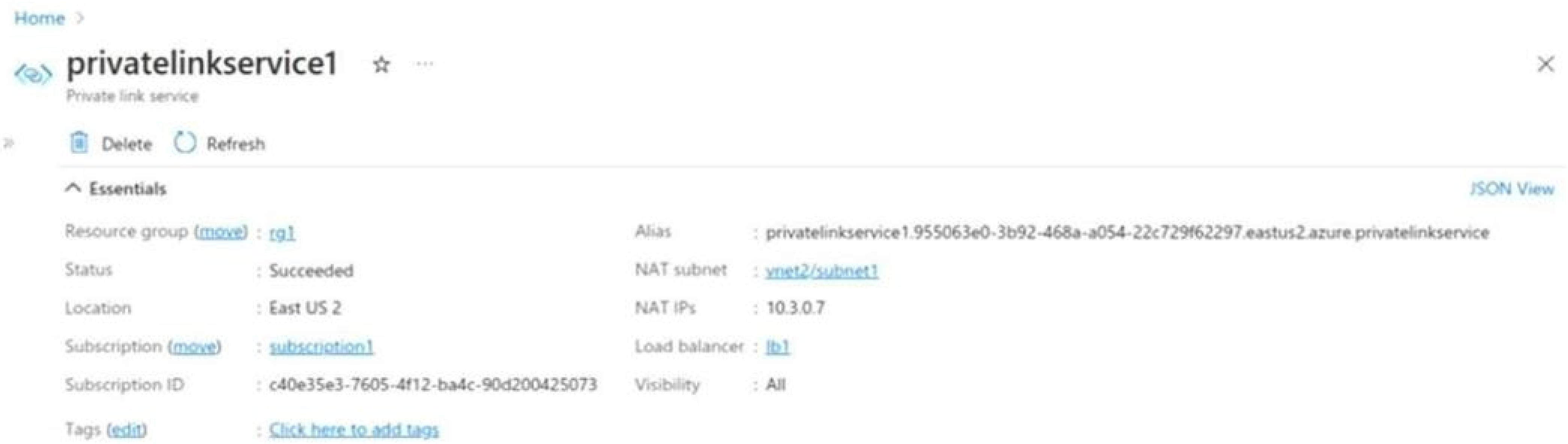
QUESTION 46

HOTSPOT

You have two Azure subscriptions named Subscription1 and Subscription2.

There are no connections between the virtual networks in two subscriptions.

You configure a private link service as shown in the privatelinkservice1 exhibit. (Click the privatelinkservice1 tab.)



Home >

privatelinkservice1

Private link service

Delete Refresh

Essentials

JSON View

Resource group (move) : rg1

Status : Succeeded

Location : East US 2

Subscription (move) : subscription1

Subscription ID : c40e35e3-7605-4f12-ba4c-90d200425073

Tags (edit) : Click here to add tags

Alias : privatelinkservice1.955063e0-3b92-468a-a054-22c729f62297.eastus2.azure.privatelinkservice

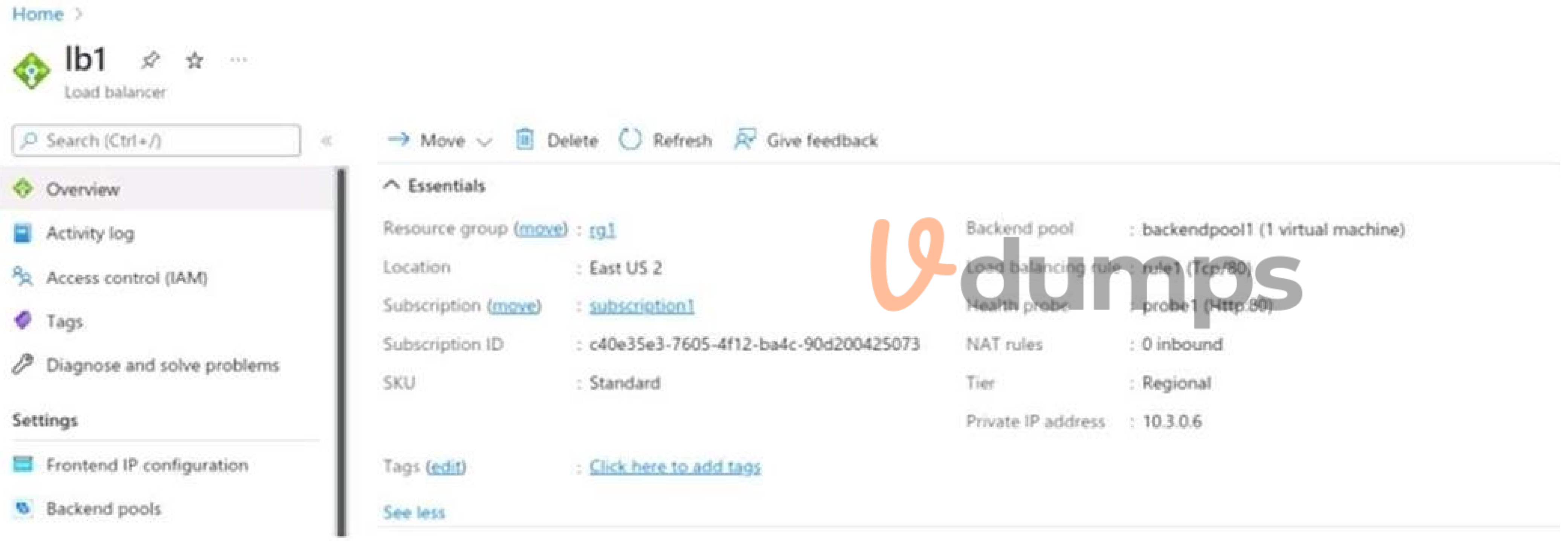
NAT subnet : vnet2/subnet1

NAT IPs : 10.3.0.7

Load balancer : lb1

Visibility : All

You create a load balancer name in Subscription1 and configure the backend pool shown in the lb1 exhibit. (Click tie 1b1 tab.)



Home >

lb1

Load balancer

Essentials

Resource group (move) : rg1

Location : East US 2

Subscription (move) : subscription1

Subscription ID : c40e35e3-7605-4f12-ba4c-90d200425073

SKU : Standard

Tags (edit) : Click here to add tags

See less

Backend pool : backendpool1 (1 virtual machine)

Load balancing rule : rule1 (Tcp/80)

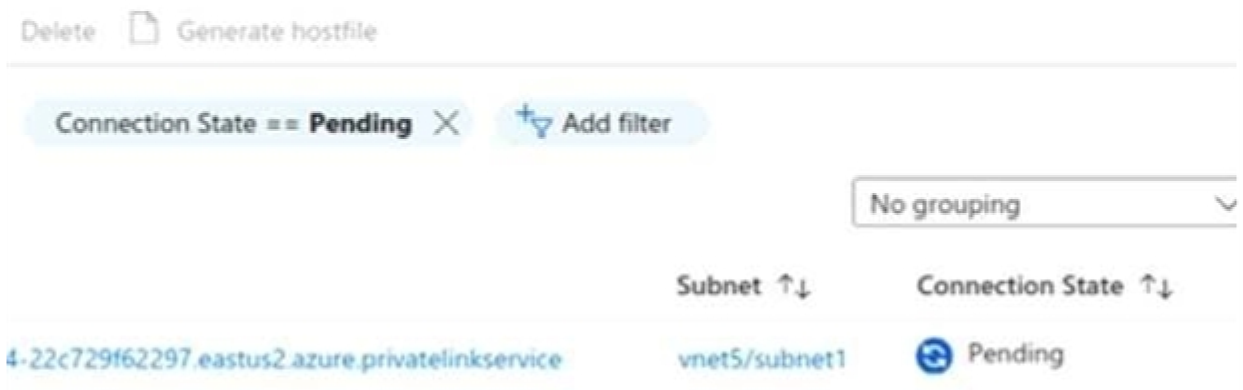
Health probe : probe1 (Http:80)

NAT rules : 0 inbound

Tier : Regional

Private IP address : 10.3.0.6

You create a private endpoint in Subscription2 as shown in the privateendpoint4 exhibit. (Click the privateendpoint4)

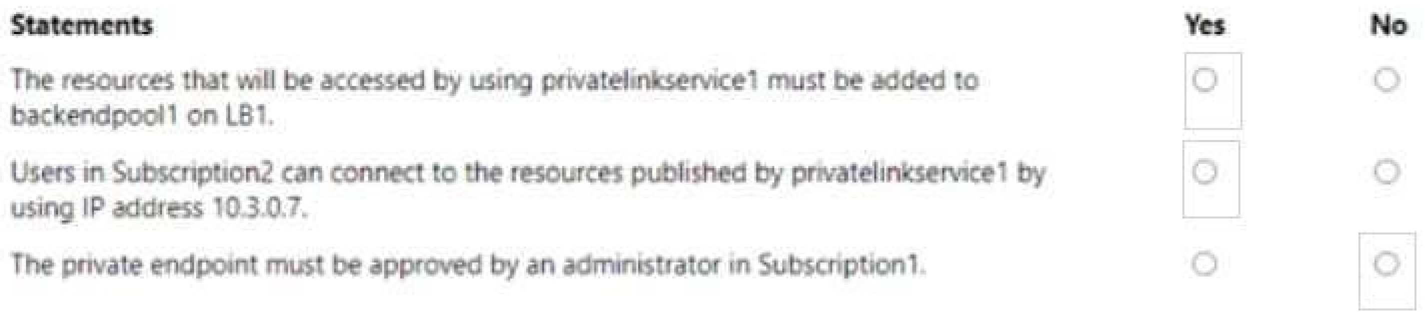


Connection State == **Pending**

	Subnet	Connection State
4-22c729f62297.eastus2.azure.privatelinkservice	vnet5/subnet1	Pending

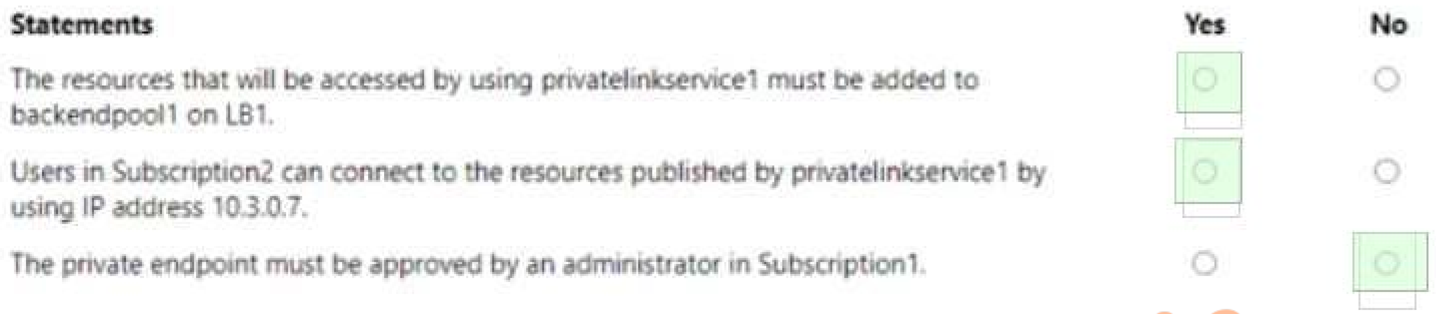
For each of the following statements, select YES if the statement is true. Otherwise. select No.

Hot Area:



Statements	Yes	No
The resources that will be accessed by using privatelinkservice1 must be added to backendpool1 on LB1.	○	○
Users in Subscription2 can connect to the resources published by privatelinkservice1 by using IP address 10.3.0.7.	○	○
The private endpoint must be approved by an administrator in Subscription1.	○	○

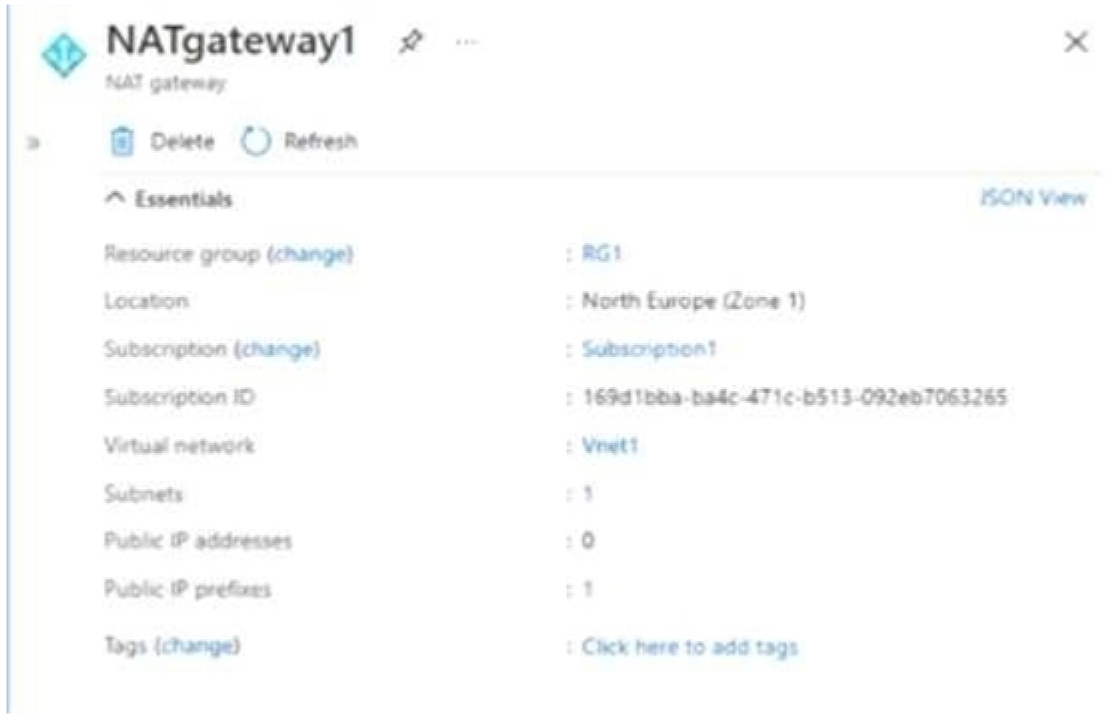
Answer Area:



Statements	Yes	No
The resources that will be accessed by using privatelinkservice1 must be added to backendpool1 on LB1.	[✓ ○]	○
Users in Subscription2 can connect to the resources published by privatelinkservice1 by using IP address 10.3.0.7.	[✓ ○]	○
The private endpoint must be approved by an administrator in Subscription1.	○	[✓ ○]

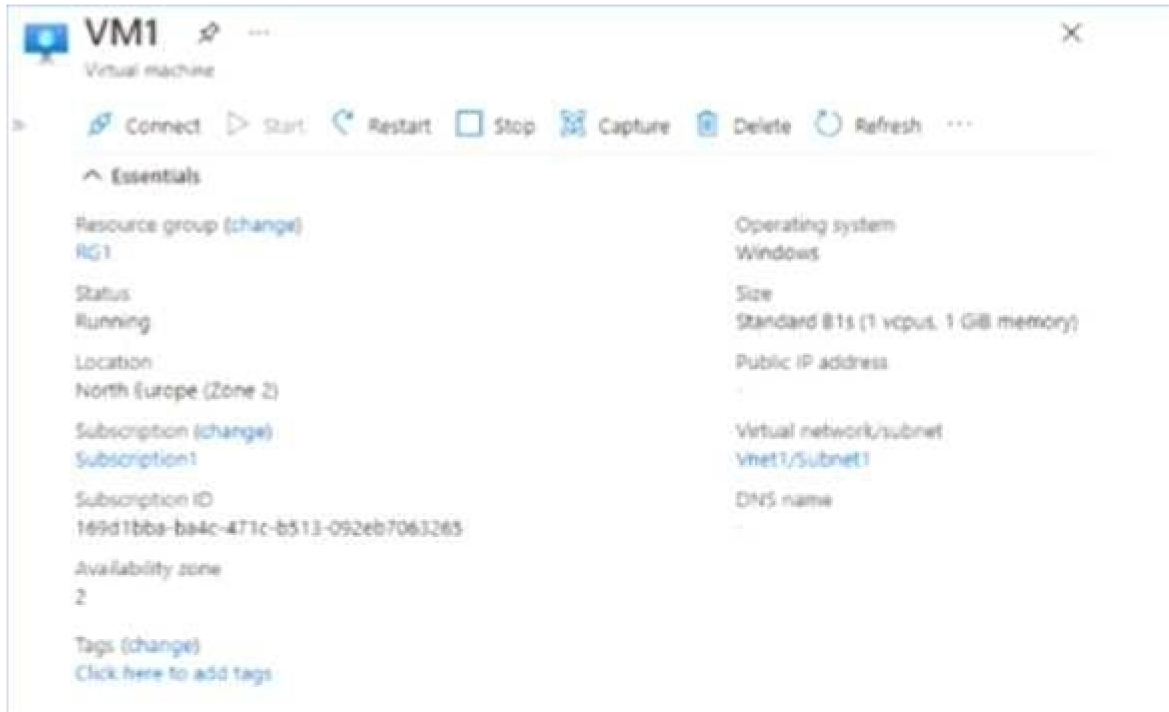
Section:
Explanation:

QUESTION 47
HOTSPOT
You have an Azure virtual network named Vnet1 that contains two subnets named Subnet1 and Subnet2. You have the NAT gateway shown in the NATgateway1 exhibit, (Click the NATgateway1 tab)



Resource group (change)	: RG1
Location	: North Europe (Zone 1)
Subscription (change)	: Subscription1
Subscription ID	: 169d1bba-ba4c-471c-b513-092eb7063265
Virtual network	: Vnet1
Subnets	: 1
Public IP addresses	: 0
Public IP prefixes	: 1
Tags (change)	: Click here to add tags

You have the virtual machine shown in the VM1 exhibit, (Click the VM1 tab)



VM1
Virtual machine

Essentials

Resource group (change)
RG1

Status
Running

Location
North Europe (Zone 2)

Subscription (change)
Subscription1

Subscription ID
169d1bba-ba4c-471c-b513-092eb7063265

Availability zone
2

Tags (change)
Click here to add tags

Operating system
Windows

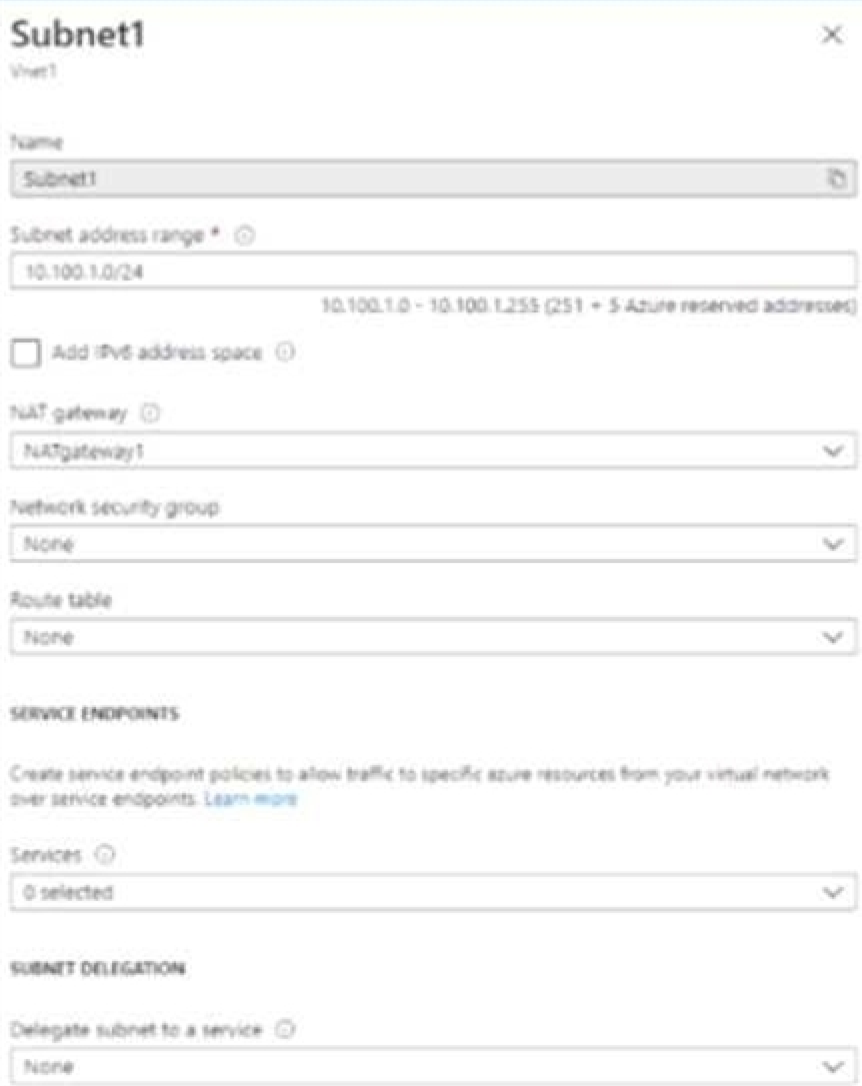
Size
Standard B1s (1 vcpus, 1 GiB memory)

Public IP address
-

Virtual network/subnet
Vnet1/Subnet1

DNS name
-

Subnet1 is configured as shown in the Subnet1 exhibit, (Click the Subnet1 tab)



Subnet1
Vnet1

Name
Subnet1

Subnet address range *
10.100.1.0/24
10.100.1.0 - 10.100.1.255 (251 + 5 Azure reserved addresses)

□ Add IPv6 address space

NAT gateway
NATgateway1

Network security group
None

Route table
None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

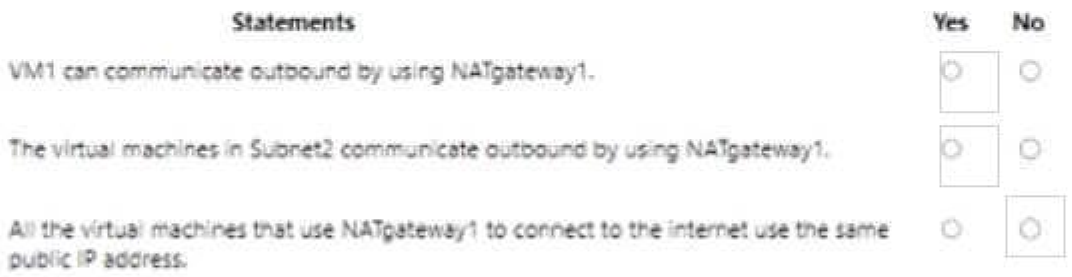
Services
0 selected

SUBNET DELEGATION

Delegate subnet to a service
None

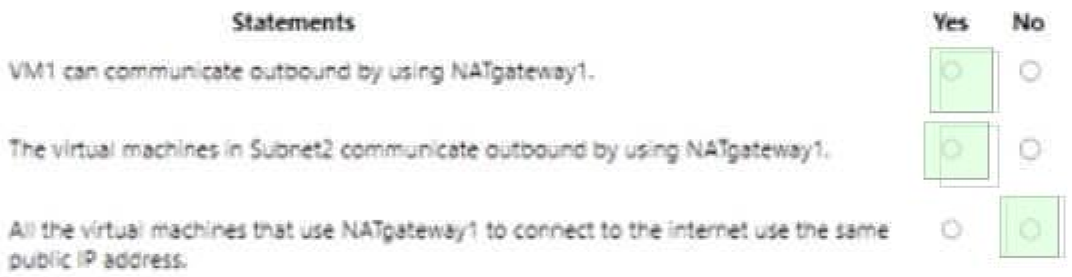
For each of the following statements, select Yes if the statement is true. Otherwise, select No

Hot Area:



Statements	Yes	No
VM1 can communicate outbound by using NATgateway1.	○	○
The virtual machines in Subnet2 communicate outbound by using NATgateway1.	○	○
All the virtual machines that use NATgateway1 to connect to the internet use the same public IP address.	○	○

Answer Area:



Statements	Yes	No
VM1 can communicate outbound by using NATgateway1.	[✓ ○]	○
The virtual machines in Subnet2 communicate outbound by using NATgateway1.	[✓ ○]	○
All the virtual machines that use NATgateway1 to connect to the internet use the same public IP address.	○	[✓ ○]

Section:
Explanation:

QUESTION 48

You have an Azure subscription that is linked to an Azure AD tenant named contoso.onmicrosoft.com. The subscription contains the following resources:

- A virtual network named Vnet1

- An App Service plan named ASPI

- An Azure App Service named webapp1

- An Azure private DNS zone named private.contoso.com

- Virtual machines on Vnet1 that cannot communicate outside the virtual network

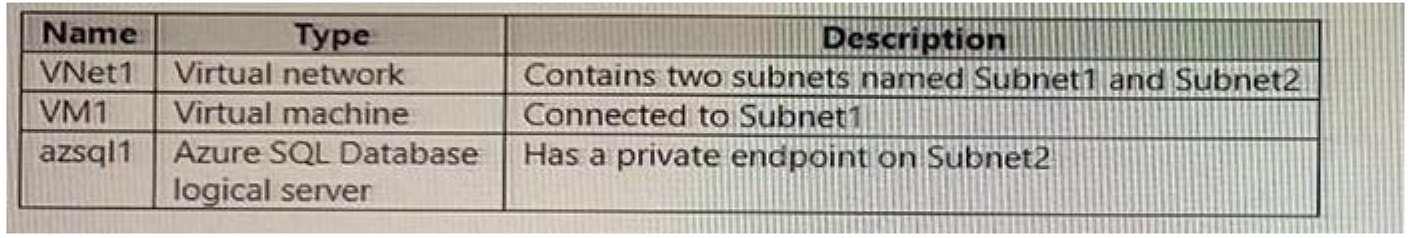
You need to ensure that the virtual machines on Vnet1 can access webapp1 by using a URL of https:/Avwwprivate.contosocom. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a private endpoint for webapp1.
B. Create a service endpoint for webapp1.
C. Create a CNAME record that maps www.pnvate.contoso.com to webapp1.privatelink.azurewebsites.net.
D. Create a CNAME record that maps wwwprivatemntoso.com to webapp1.contoso.onmicrosoft.com.
E. Register an enterprise application in Azure AD for webapp1.
F. Create a CNAME record that maps wow.private.contoso.com to webapp 1 private@ntoso.com.

Correct Answer: A, D
Section:

QUESTION 49
You have an Azure subscription that contains the resources is shown in the following table.



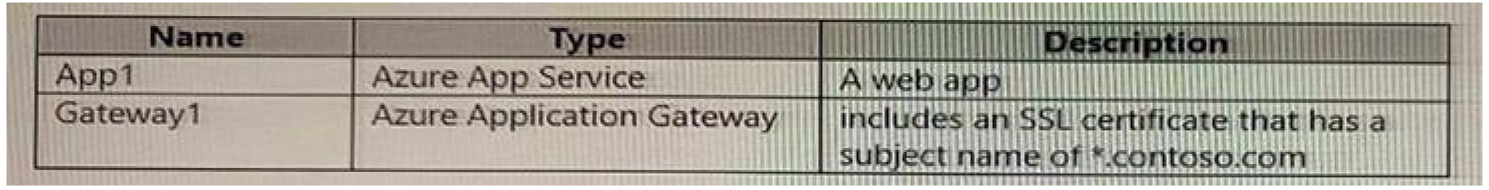
Name	Type	Description
VNet1	Virtual network	Contains two subnets named Subnet1 and Subnet2
VM1	Virtual machine	Connected to Subnet1
azsql1	Azure SQL Database logical server	Has a private endpoint on Subnet2

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 ink.database.windows.net
D. a private DNS zone named privatelink.database.windows.net

Correct Answer: C
Section:

QUESTION 50
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure App Service	A web app
Gateway1	Azure Application Gateway	includes an SSL certificate that has a subject name of *.contoso.com

Gateway1 provides access to App1 by using a URL of http://app1.contoso.com.
You create a new web app named App2.
You need to configure Gateway1 to enable minimize administrative effort.
What should you configure on Gateway1?

A. a backend pool and a routing
B. a listener and a routing rule
C. a listener, a backend pool, and a rule
D. a listener and a backend pool

Correct Answer: B

Section:

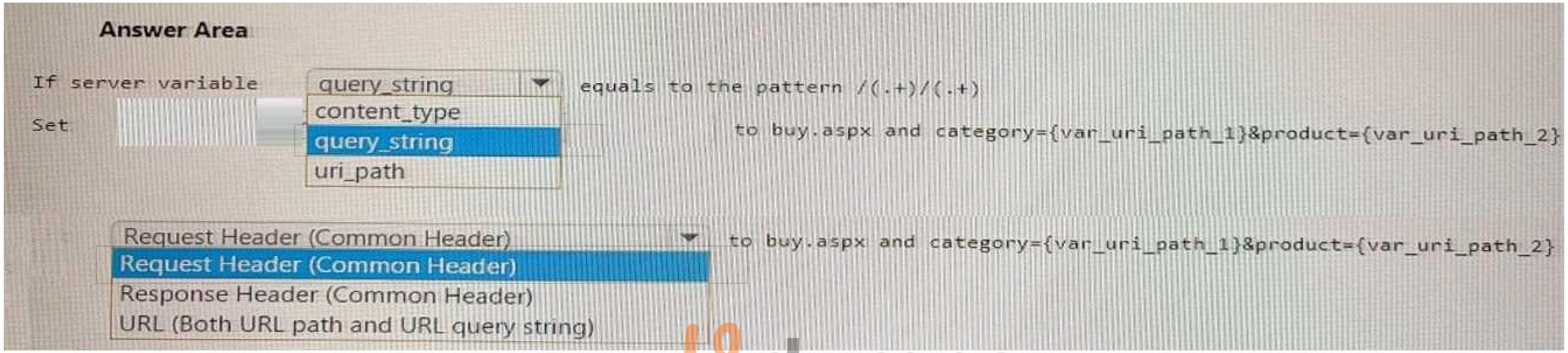
QUESTION 51

HOTSPOT

You have an Azure application gateway named AppGw1.

You need to create a rewrite rule for AppGw1. The solution must rewrite the URL of requests from https://www.contoso.com/fashion/shirts to ttps://www.contoso.com/buy.aspx?categoryfashion&product=shirts. How should you complete the rule? To answer NOTE: Each correct selection is worth one point appropriate options in the answer area.

Hot Area:



Answer Area

If server variable [query_string ▾] equals to the pattern /(.+)/(.+)

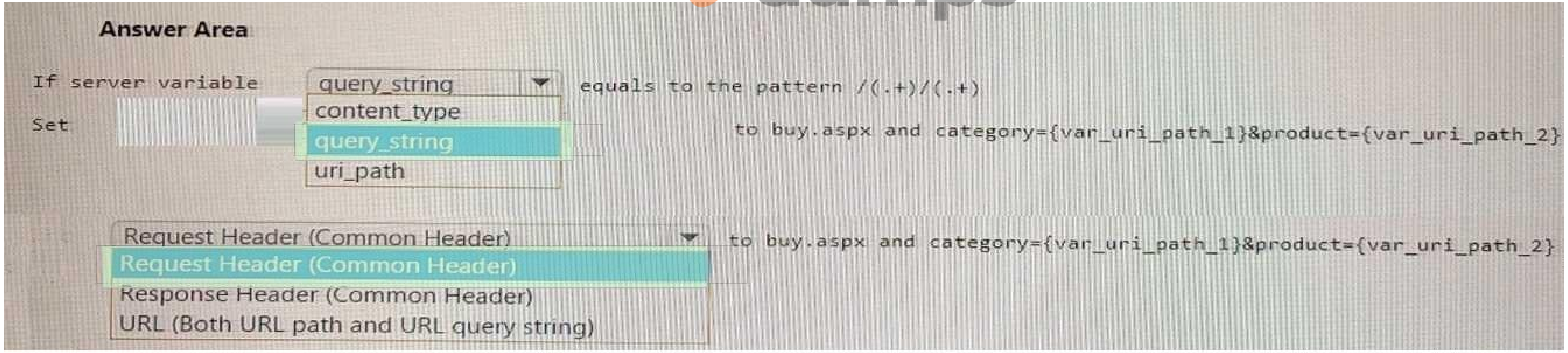
Set [▾] to buy.aspx and category={var_uri_path_1}&product={var_uri_path_2}

content_type
query_string
uri_path

[Request Header (Common Header) ▾] to buy.aspx and category={var_uri_path_1}&product={var_uri_path_2}

Request Header (Common Header)
Response Header (Common Header)
URL (Both URL path and URL query string)

Answer Area:



Answer Area

If server variable [query_string ▾] equals to the pattern /(.+)/(.+)

Set [▾] to buy.aspx and category={var_uri_path_1}&product={var_uri_path_2}

content_type
query_string
uri_path

[Request Header (Common Header) ▾] to buy.aspx and category={var_uri_path_1}&product={var_uri_path_2}

Request Header (Common Header)
Response Header (Common Header)
URL (Both URL path and URL query string)

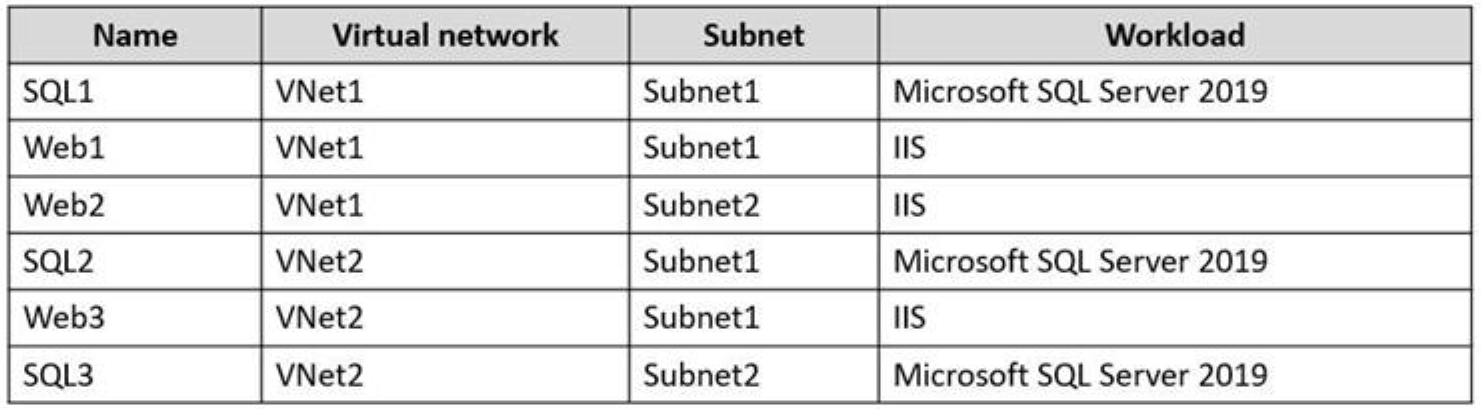
Section:

Explanation:

QUESTION 52

HOTSPOT

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

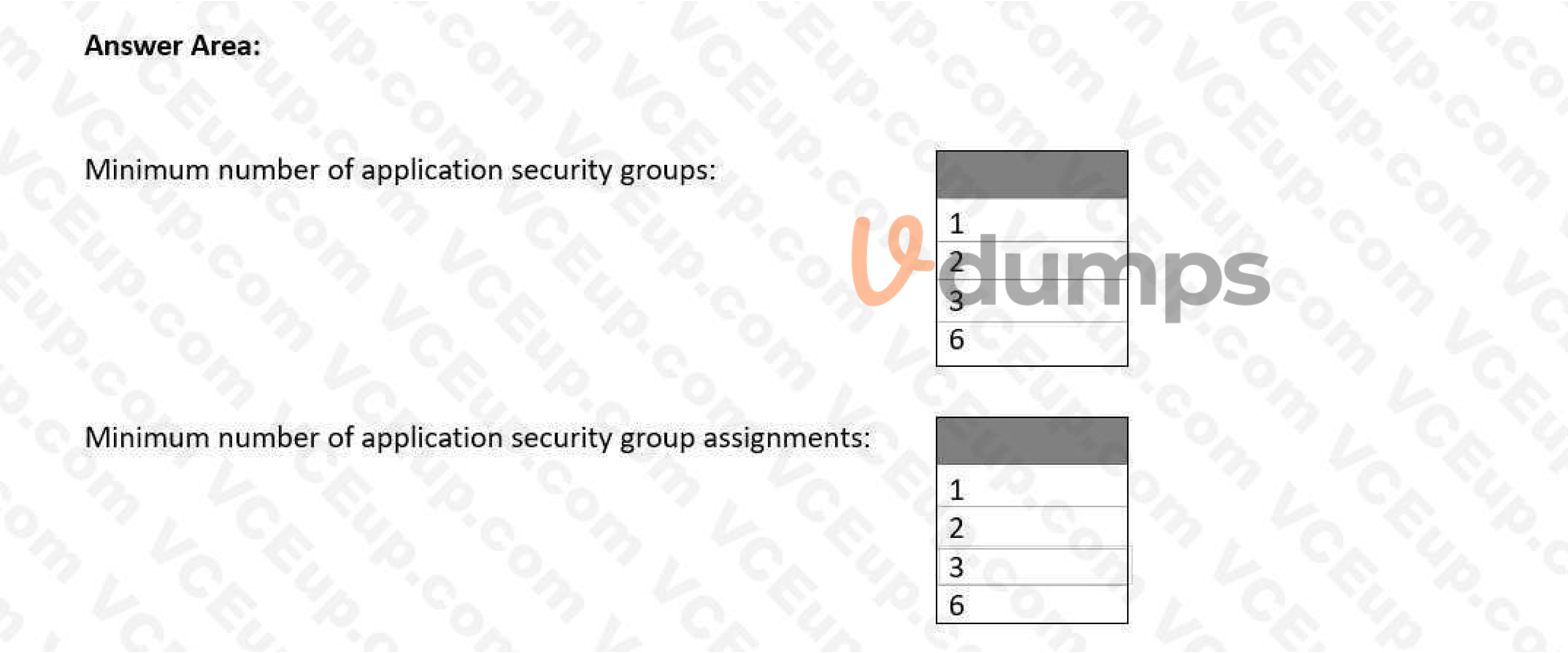


Name	Virtual network	Subnet	Workload
SQL1	VNet1	Subnet1	Microsoft SQL Server 2019
Web1	VNet1	Subnet1	IIS
Web2	VNet1	Subnet2	IIS
SQL2	VNet2	Subnet1	Microsoft SQL Server 2019
Web3	VNet2	Subnet1	IIS
SQL3	VNet2	Subnet2	Microsoft SQL Server 2019

VNet1 and VNet2 are NOT connected to each other.

You need to block traffic from SQL Server 2019 to IIS by using application security groups. The solution must minimize administrative effort. How should you configure the application security groups? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

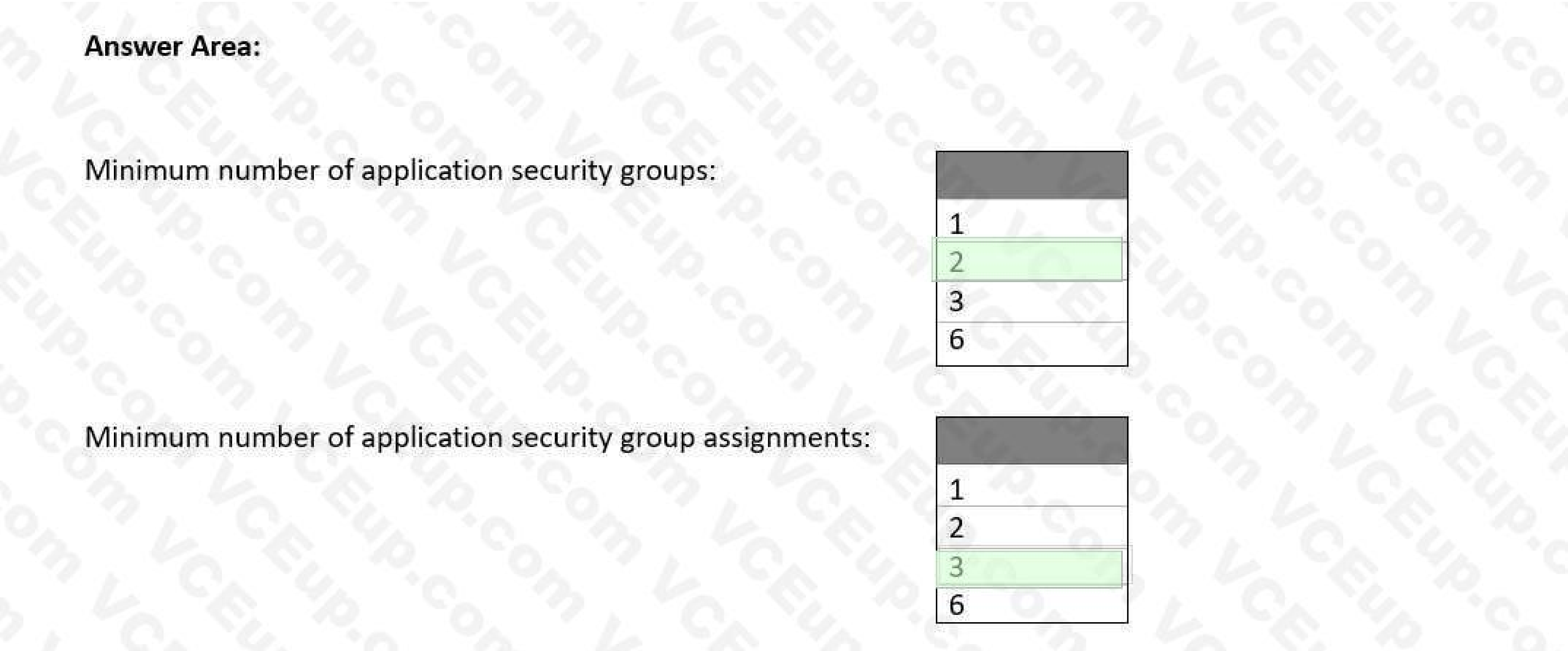


Answer Area:

Minimum number of application security groups:

Minimum number of application security group assignments:

Answer Area:



Answer Area:

Minimum number of application security groups:

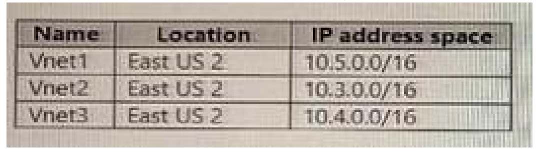
- 1
- [✓ 2]
- 3
- 6

Minimum number of application security group assignments:

- 1
- 2
- [✓ 3]
- 6

Section:
Explanation:
"All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in."
https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

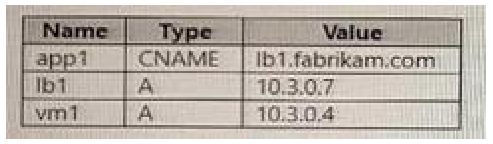
QUESTION 53
HOTSPOT
You have an Azure subscription that contains the virtual networks.shown in the following table.



Name	Location	IP address space
Vnet1	East US 2	10.5.0.0/16
Vnet2	East US 2	10.3.0.0/16
Vnet3	East US 2	10.4.0.0/16

You have a virtual machine named VM5 that has the following IP address configurations:
- IP address: 10.4.0.5
- Subnet mask:255.255.255.0
- Default gateway:10.4.0.1
- DNSserver:168.63.129.16

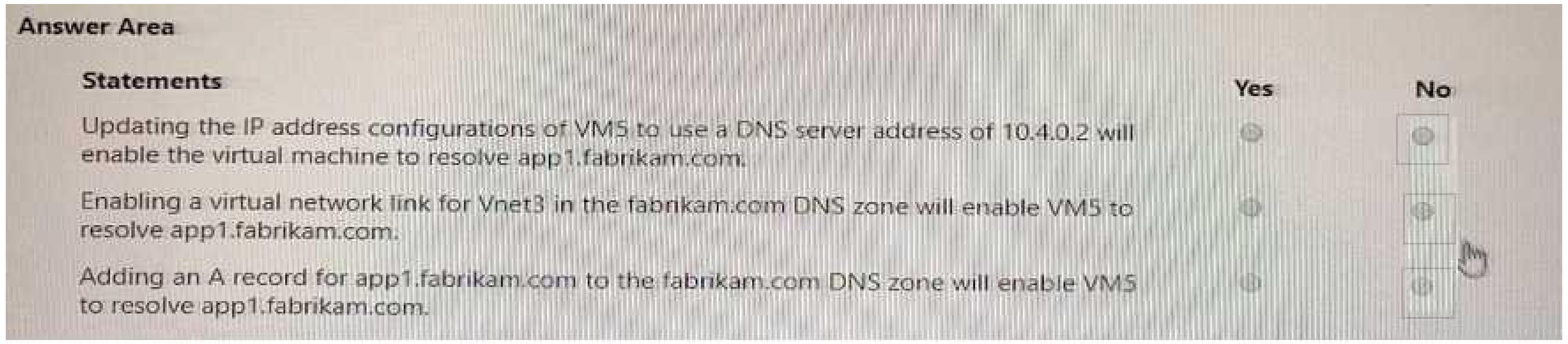
You have an Azure Private DNS zone named, fabrikam.com that contains the records shown in, the following table.



Name	Type	Value
app1	CNAME	lb1.fabrikam.com
lb1	A	10.3.0.7
vm1	A	10.3.0.4

The virtual network links in the fabrikam.com DNS /one are configured as shown in the exhibit. (Click the Exhibit tab.) VMS fails to resolve the IP address for.appKfabrik3in.com.
For each of the following statements, select Yes if, the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

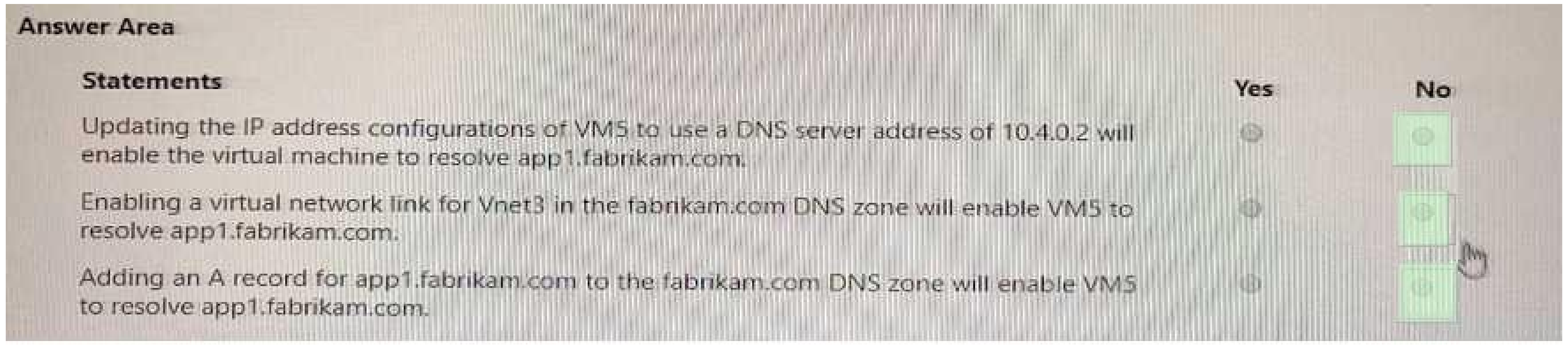
Hot Area:



Answer Area

Statements	Yes	No
Updating the IP address configurations of VM5 to use a DNS server address of 10.4.0.2 will enable the virtual machine to resolve app1.fabrikam.com.	○	○
Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	○	○
Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Updating the IP address configurations of VM5 to use a DNS server address of 10.4.0.2 will enable the virtual machine to resolve app1.fabrikam.com.	○	[✓ ○]
Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	○	[✓ ○]
Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	○	[✓ ○]

Section:
Explanation:

QUESTION 54
You have two Azure virtual networks named Vnet1 and Vnet2.
You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN. You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit Vnet2 can use the. You discover that Client1 cannot communicate with Vnet2.
You need to ensure that Client1 can communication with Vnet2.
Solution: You resize the gateway of Vnet1 to a larger SKU.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 55
You have an Azure Front Door instance named FD1 that is protected by using Azure Web Application Firewall (WAF). FD1 uses a frontend host named app1.contoso.com to provide access to Azure web apps hosted in the East US Azure region and the West US Azure region. You need to configure FD1 to block requests to app1.contoso.com from all countries other than the United States. What should you include in the WAF policy?

A. a frontend host association
B. a managed rule set
C. a custom rule that uses a rate limit rule
D. a custom rule that uses a match rule

Correct Answer: D

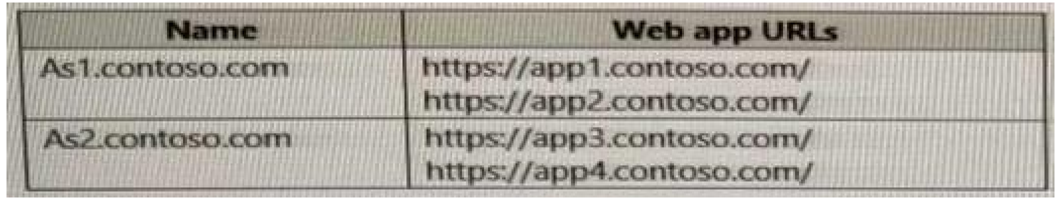
Section:
Explanation:

QUESTION 56
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 Standard Load Balancer that has Floating IP enabled
B. Azure Application Gateway V2 that has multiple listeners
C. Azure Application Gateway v2 that has multiple site hosting enabled
D. Azure Standard Load Balancer that has high availability (HA) ports enabled

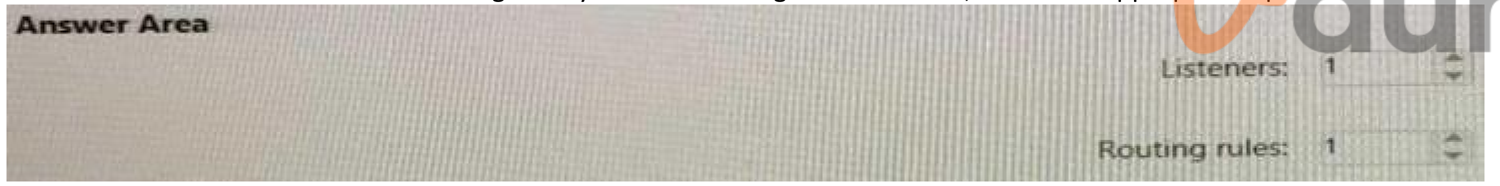
Correct Answer: B
Section:

QUESTION 57
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 application gateway 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.



Answer Area

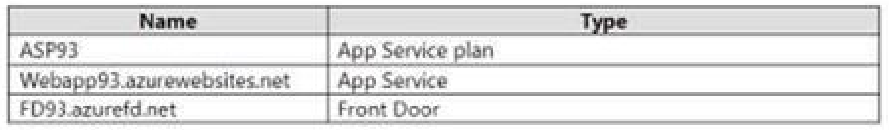
Listeners: 1

Routing rules: 1

A. 1, 2

Correct Answer: A
Section:

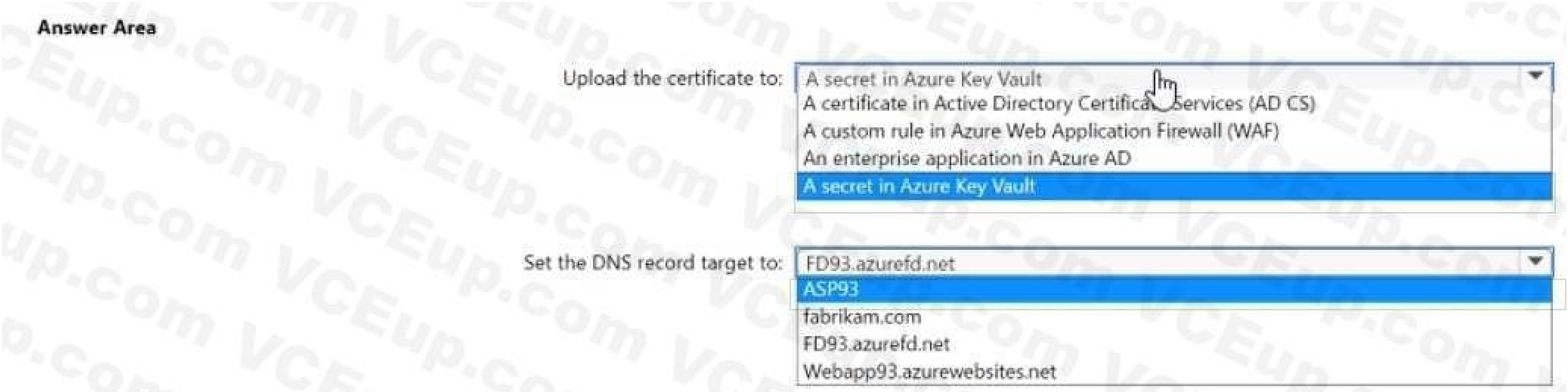
QUESTION 58
HOTSPOT
You are planning an Azure Front Door deployment that will contain the resources shown in the following table.



Name	Type
ASP93	App Service plan
Webapp93.azurewebsites.net	App Service
FD93.azurefd.net	Front Door

Users will connect to the App Service through Front Door by using a URL of
https://www.fabrikarn.com. You obtain a certificate for the host name of www.fabfikam.com.
You need to configure a DNS record for www.fabrikam.com and upload the certificate to Azure. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

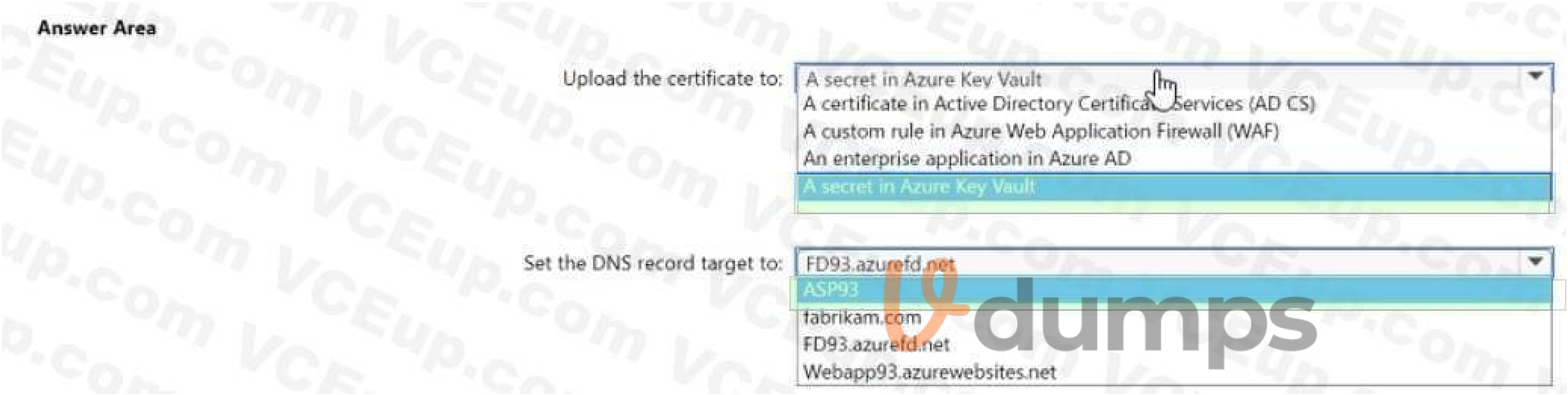
Upload the certificate to: A secret in Azure Key Vault

- A certificate in Active Directory Certificate Services (AD CS)
- A custom rule in Azure Web Application Firewall (WAF)
- An enterprise application in Azure AD
- A secret in Azure Key Vault

Set the DNS record target to: FD93.azurefd.net

- ASP93
- fabrikam.com
- FD93.azurefd.net
- Webapp93.azurewebsites.net

Answer Area:



Answer Area

Upload the certificate to: A secret in Azure Key Vault

- A certificate in Active Directory Certificate Services (AD CS)
- A custom rule in Azure Web Application Firewall (WAF)
- An enterprise application in Azure AD
- A secret in Azure Key Vault

Set the DNS record target to: FD93.azurefd.net

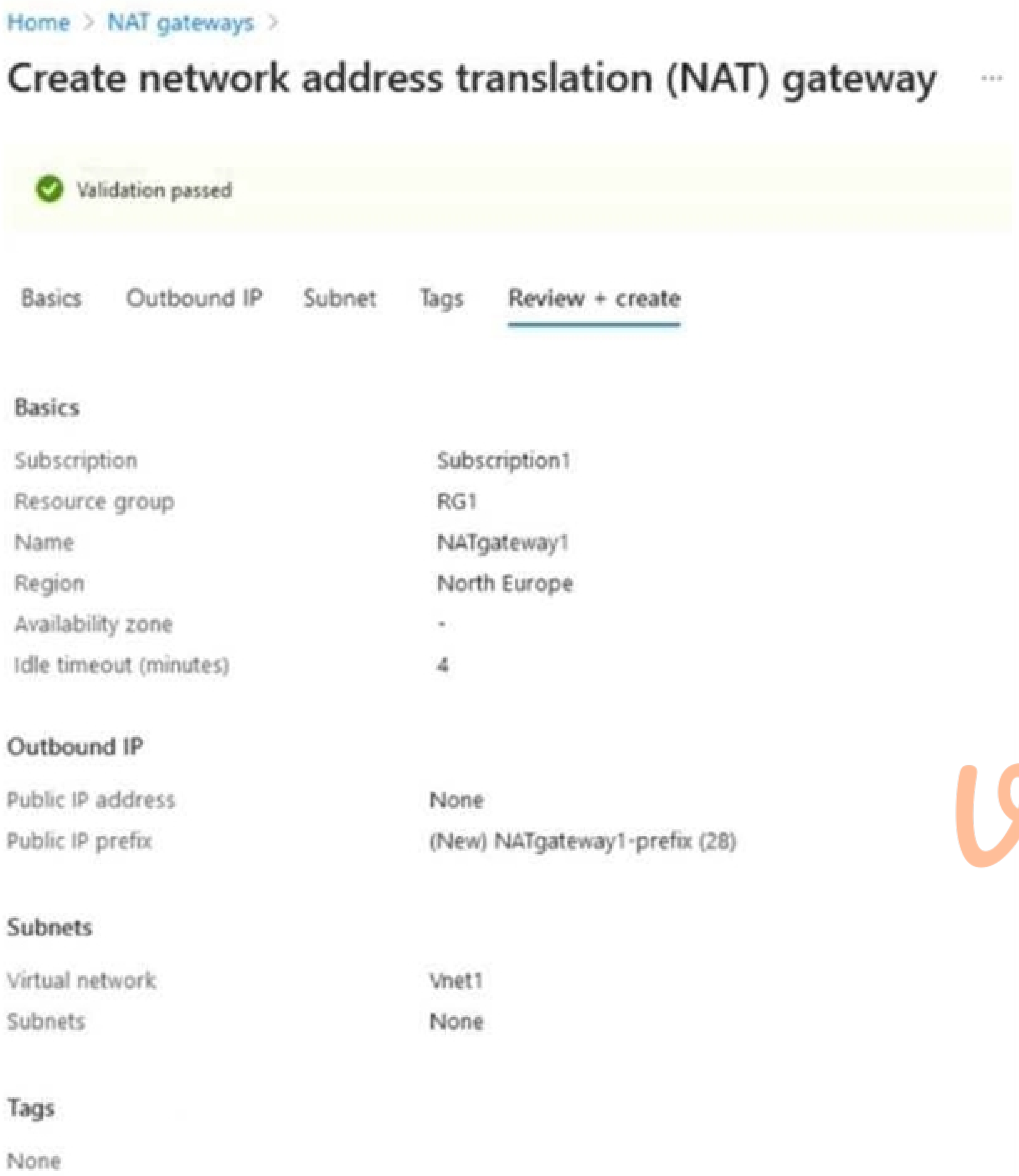
- ASP93
- fabrikam.com
- FD93.azurefd.net
- Webapp93.azurewebsites.net

Section:
Explanation:

QUESTION 59

HOTSPOT

You have an Azure virtual network named Vnet1 that contains two subnets named Subnet1 and Subnet2. Both subnets contain virtual machines. You create a NAT gateway named NATgateway1 as shown in the following exhibit.



Home > NAT gateways >

Create network address translation (NAT) gateway ...

Validation passed

Basics   Outbound IP   Subnet   Tags   Review + create

Basics

Subscription	Subscription1
Resource group	RG1
Name	NATgateway1
Region	North Europe
Availability zone	-
Idle timeout (minutes)	4

Outbound IP

Public IP address	None
Public IP prefix	(New) NATgateway1-prefix (28)

Subnets

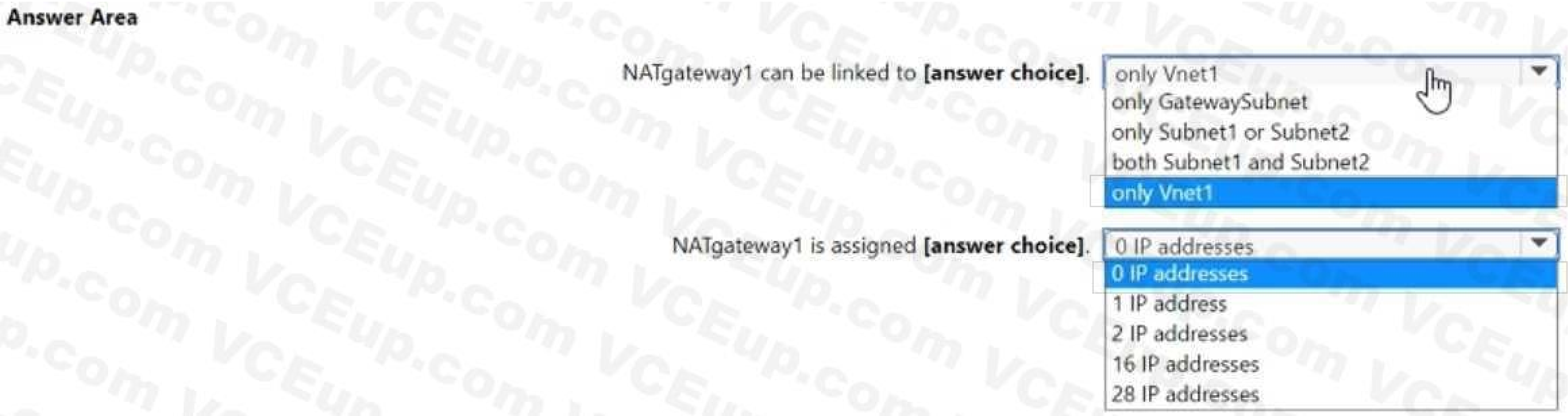
Virtual network	Vnet1
Subnets	None

Tags

None

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

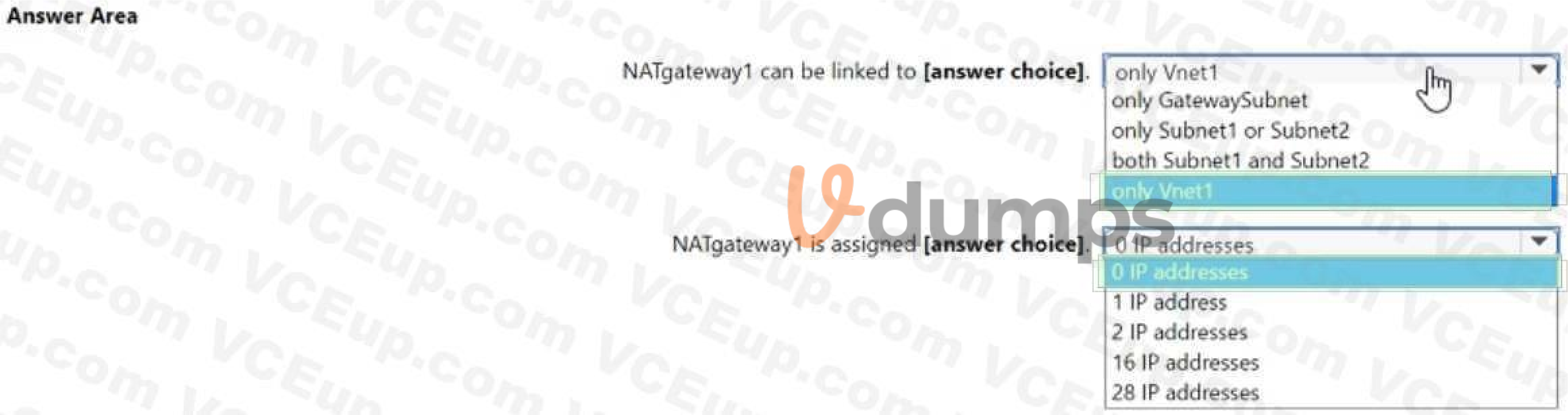
NATgateway1 can be linked to **[answer choice]**.

- only Vnet1
- only GatewaySubnet
- only Subnet1 or Subnet2
- both Subnet1 and Subnet2
- only Vnet1

NATgateway1 is assigned **[answer choice]**.

- 0 IP addresses
- 0 IP addresses
- 1 IP address
- 2 IP addresses
- 16 IP addresses
- 28 IP addresses

Answer Area:



Answer Area

NATgateway1 can be linked to **[answer choice]**.

- only Vnet1
- only GatewaySubnet
- only Subnet1 or Subnet2
- both Subnet1 and Subnet2
- only Vnet1

NATgateway1 is assigned **[answer choice]**.

- 0 IP addresses
- 0 IP addresses
- 1 IP address
- 2 IP addresses
- 16 IP addresses
- 28 IP addresses

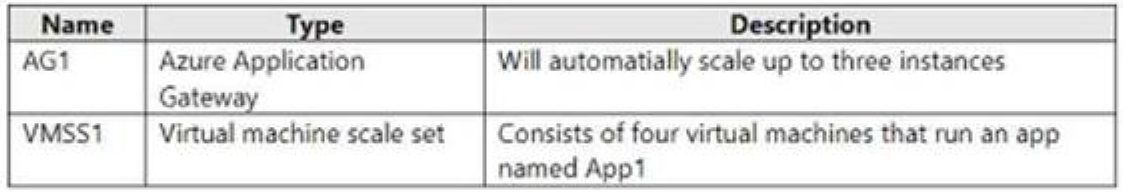
Section:

Explanation:

QUESTION 60

HOTSPOT

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the resources shown in the following table.



Name	Type	Description
AG1	Azure Application Gateway	Will automatially scale up to three instances
VMSS1	Virtual machine scale set	Consists of four virtual machines that run an app named App1

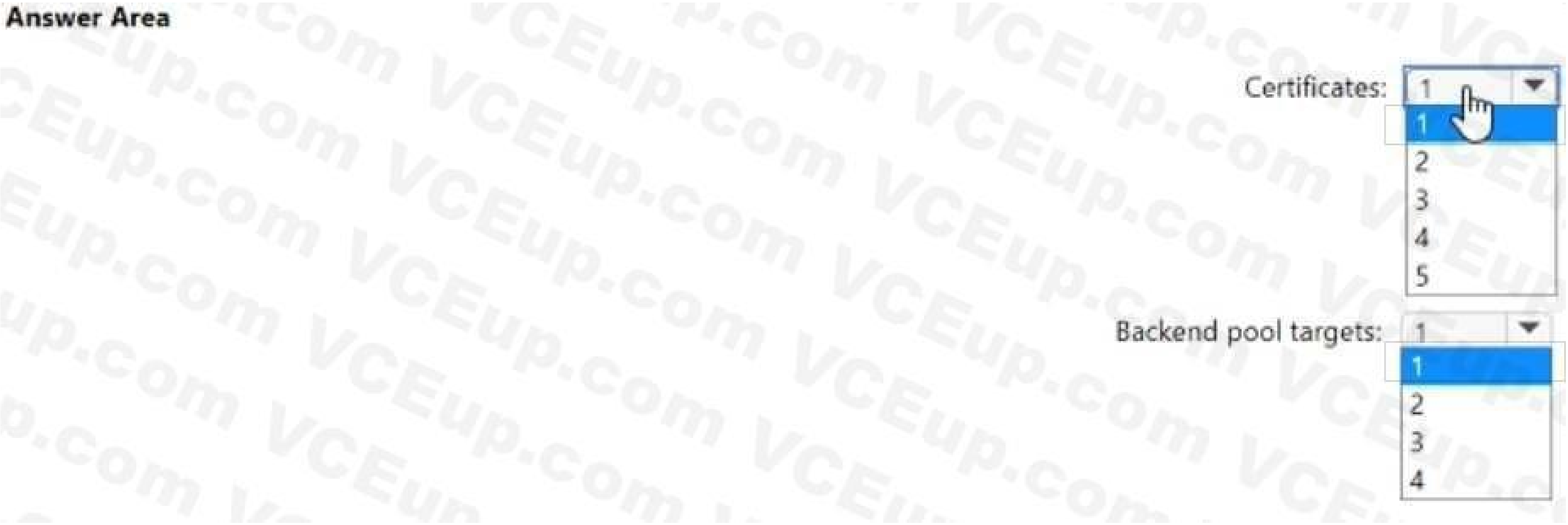
You need to publish App1 by using AG1 and a URL of https://app1.contoso.com. The solution must meet the following requirements:

- TLS connections must terminate on AG1.
- Minimize the number of targets in the backend pool of AG1.
- Minimize the number of deployed copies of the SSL certificate of App1.

How many locations should you import to the certificate, and how many targets should you add to the backend pool of AG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

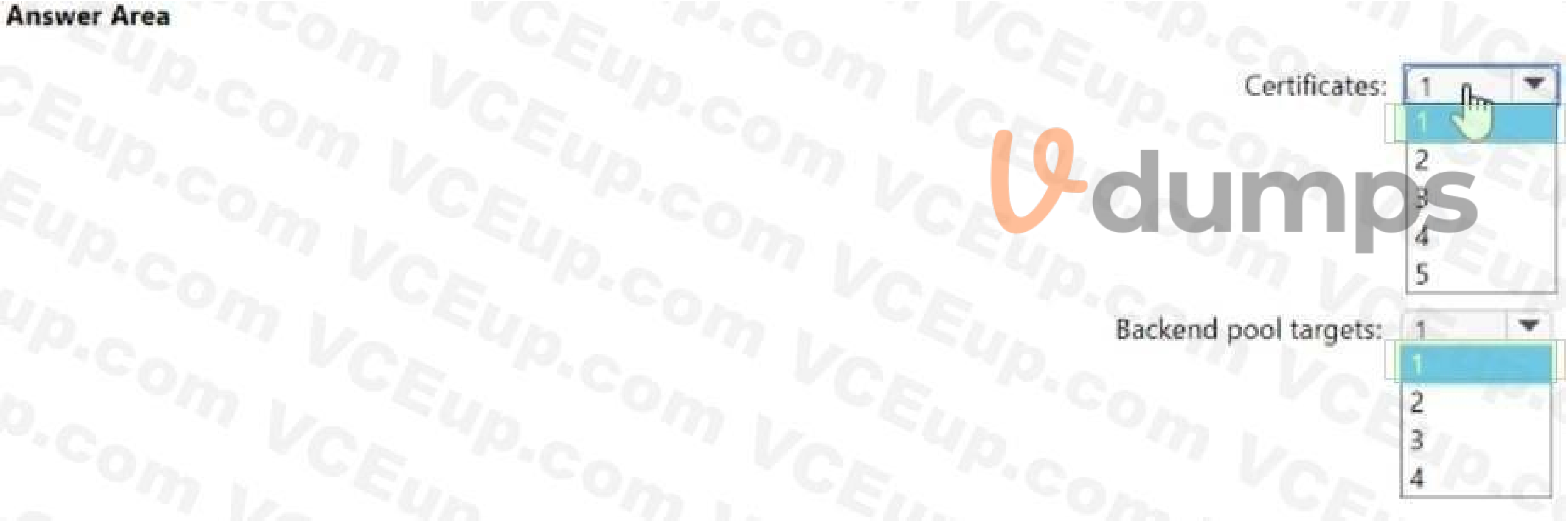
Hot Area:


Answer Area

Certificates: 1

Backend pool targets: 1

Answer Area:


Answer Area

Certificates: 1

Backend pool targets: 1

Section:

Explanation:

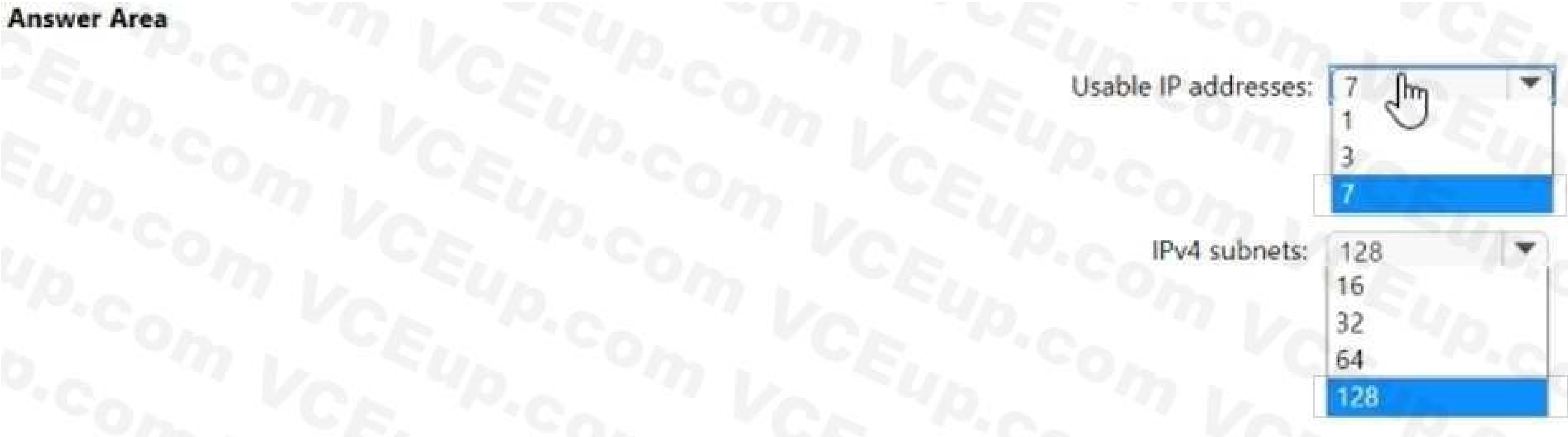
QUESTION 61

HOTSPOT

You have an Azure subscription that contains a virtual network named Vnetl. Vnetl has a /24 IPv4 address space. You need to subdivide Vnet1. The solution must maximize the number of usable subnets.

What is the maximum number of IPv4 subnets you can create, and how many usable IP addresses will be available per subnet? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

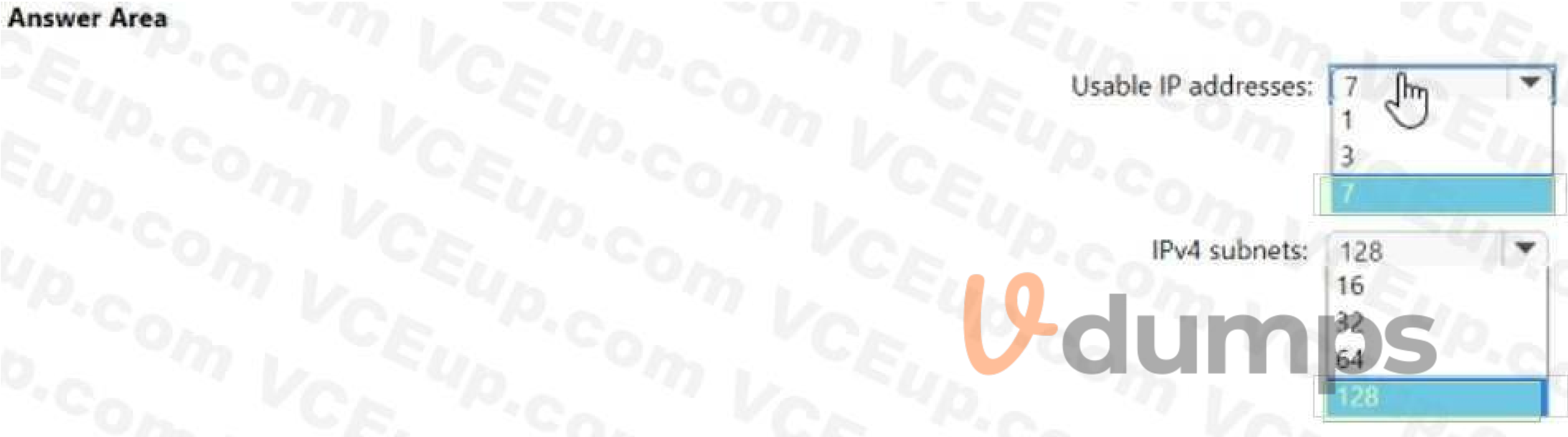


Answer Area

Usable IP addresses: 7
1
3
7

IPv4 subnets: 128
16
32
64
128

Answer Area:



Answer Area

Usable IP addresses: 7
1
3
7

IPv4 subnets: 128
16
32
64
128

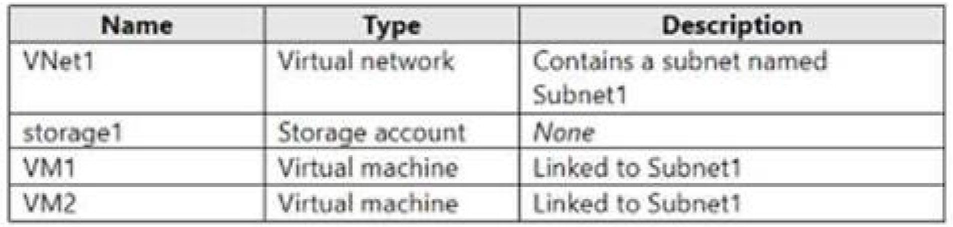
Section:
Explanation:

QUESTION 62
You have a network security group named NSG1.
You need to enable network security group (NSG) flow logs for NSG1. The solution must support retention policies. What should you create first?

A. A standard general-purpose v2 Azure Storage account
B. An Azure Log Analytics workspace
C. A premium Block blobs Azure Storage account
D. A standard general-purpose v1 Azure Storage account

Correct Answer: A
Section:

QUESTION 63
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
VNet1	Virtual network	Contains a subnet named Subnet1
storage1	Storage account	*None*
VM1	Virtual machine	Linked to Subnet1
VM2	Virtual machine	Linked to Subnet1

You need to ensure that VM1 and VM2 can connect only to storage1. The solution must meet the following requirements:

- Prevent VM1 and VM2 from accessing any other storage accounts.
- Ensure that storage1 is accessible from the internet.

What should you use?

A. a network security group (NSG)

B. a private endpoint

C. a private link

D. a service endpoint policy

Correct Answer: D
Section:

QUESTION 64

Your company has five offices. Each office has a firewall device and a local internet connection. The offices connect to a third-party SD-WAN. You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains a virtual network gateway named Gateway1. Each office connects to Gateway1 by using a Site-to-Site VPN connection. You need to replace the third-party SD-WAN with an Azure Virtual WAN. What should you include in the solution?

A. Delete Gateway1.

B. Create new Point-to-Site (P2S) VPN connections on the firewall devices.

C. Create an Azure Traffic Manager profile.

D. Enable active-active mode on Gateway1.

Correct Answer: B
Section:
Explanation:

QUESTION 65

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains 20 subnets and 500 virtual machines. Each subnet contains a virtual machine that runs network monitoring software.
You have a network security group (NSG) named NSG1 associated to each subnet.
When a new subnet is created in Vnet1, an automated process creates an additional network monitoring virtual machine in the subnet and links the subnet to NSG1.
You need to create an inbound security rule in NS61 that will allow connections to the network monitoring virtual machines from an IP address of 131.107.1.15. The solution must meet the following requirements:

- Ensure that only the monitoring virtual machines receive a connection from 131.107.1.15.
- Minimize changes to NSG1 when a new subnet is created.

What should you use as the destination in the inbound security rule?

A. a virtual network

B. an IP address

C. an application security group

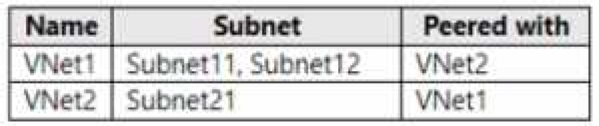
D. a service tag

Correct Answer: C
Section:

QUESTION 66

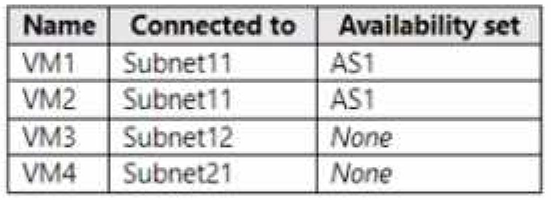
HOTSPOT

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



Name	Subnet	Peered with
VNet1	Subnet11, Subnet12	VNet2
VNet2	Subnet21	VNet1

The subscription contains the virtual machines shown in the following table.



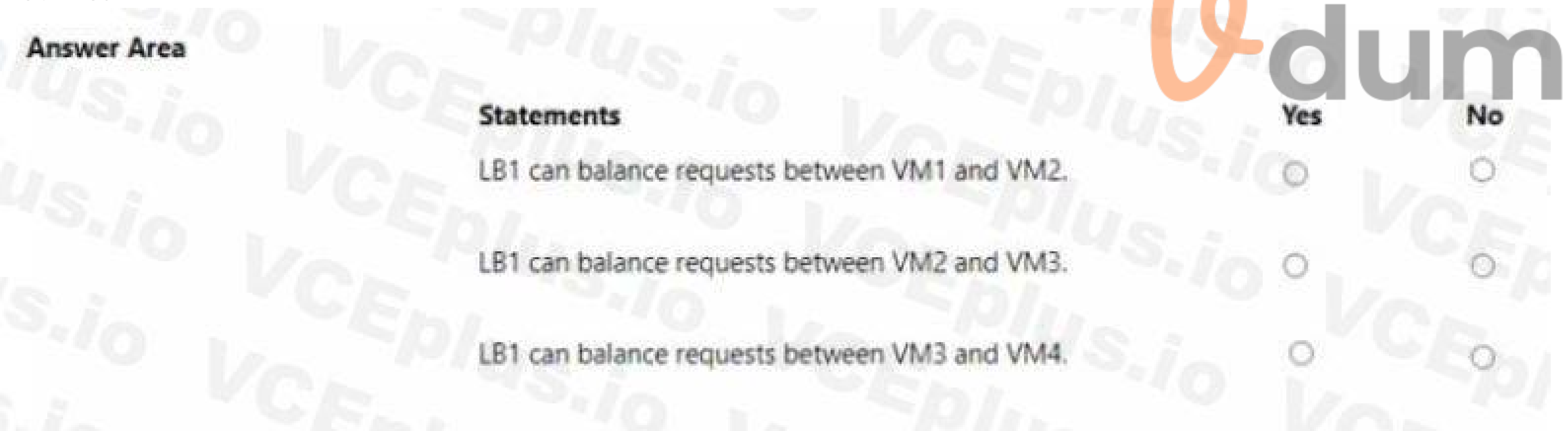
Name	Connected to	Availability set
VM1	Subnet11	AS1
VM2	Subnet11	AS1
VM3	Subnet12	*None*
VM4	Subnet21	*None*

You create a load balancer named LB1 that has the following configurations:

- SKU: Basic
- Type: Internal
- Subnet: Subnetl2
- Virtual network VNet1

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

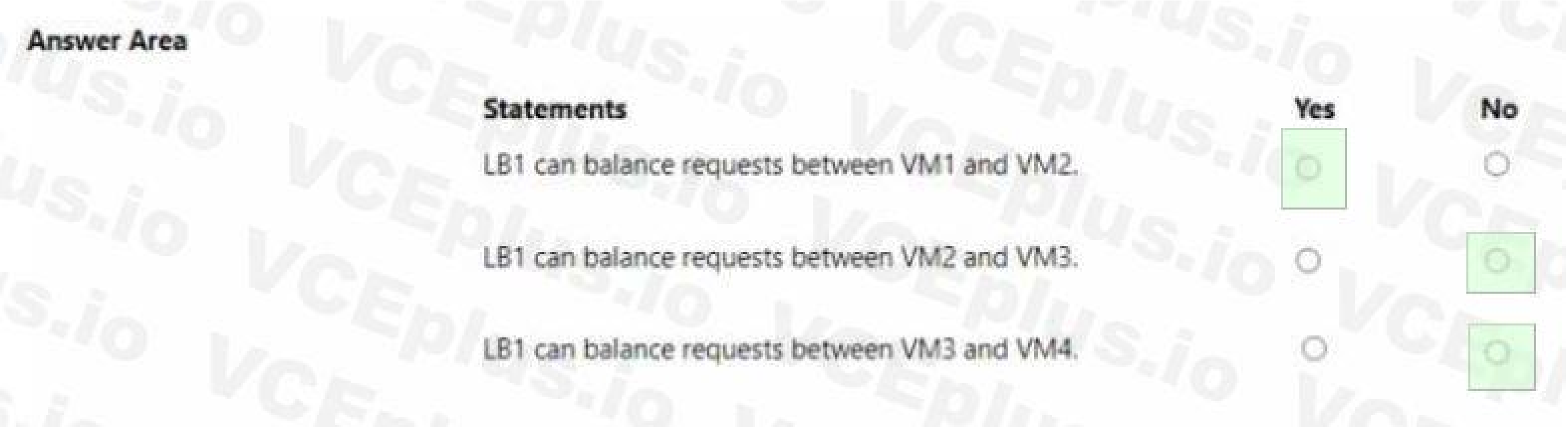
Hot Area:



Answer Area

Statements	Yes	No
LB1 can balance requests between VM1 and VM2.	○	○
LB1 can balance requests between VM2 and VM3.	○	○
LB1 can balance requests between VM3 and VM4.	○	○

Answer Area:



Answer Area

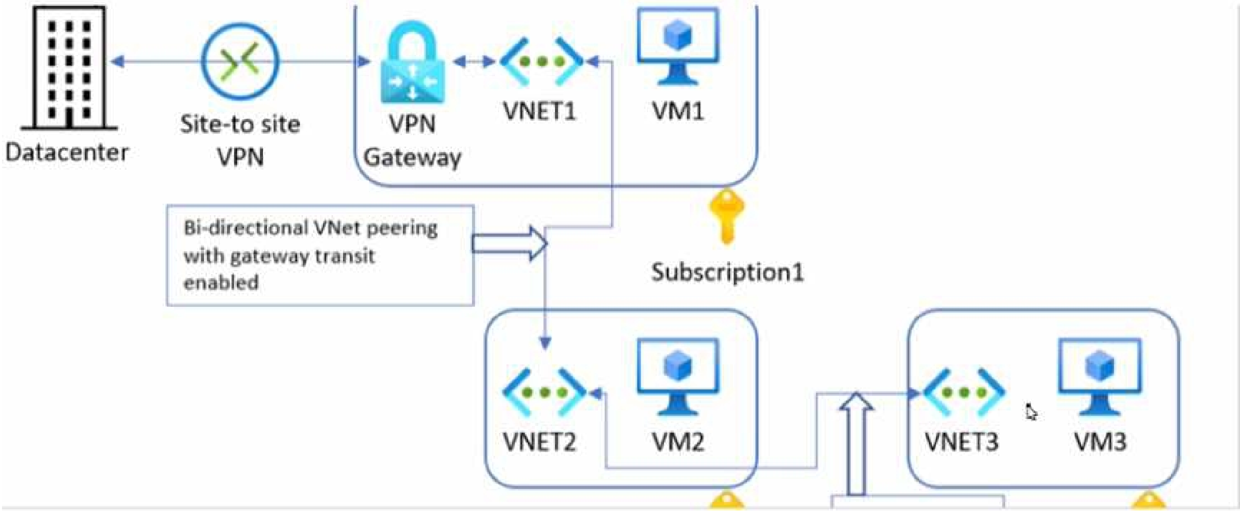
Statements	Yes	No
LB1 can balance requests between VM1 and VM2.	[✓ ○]	○
LB1 can balance requests between VM2 and VM3.	○	[✓ ○]
LB1 can balance requests between VM3 and VM4.	○	[✓ ○]

Section:
Explanation:

QUESTION 67

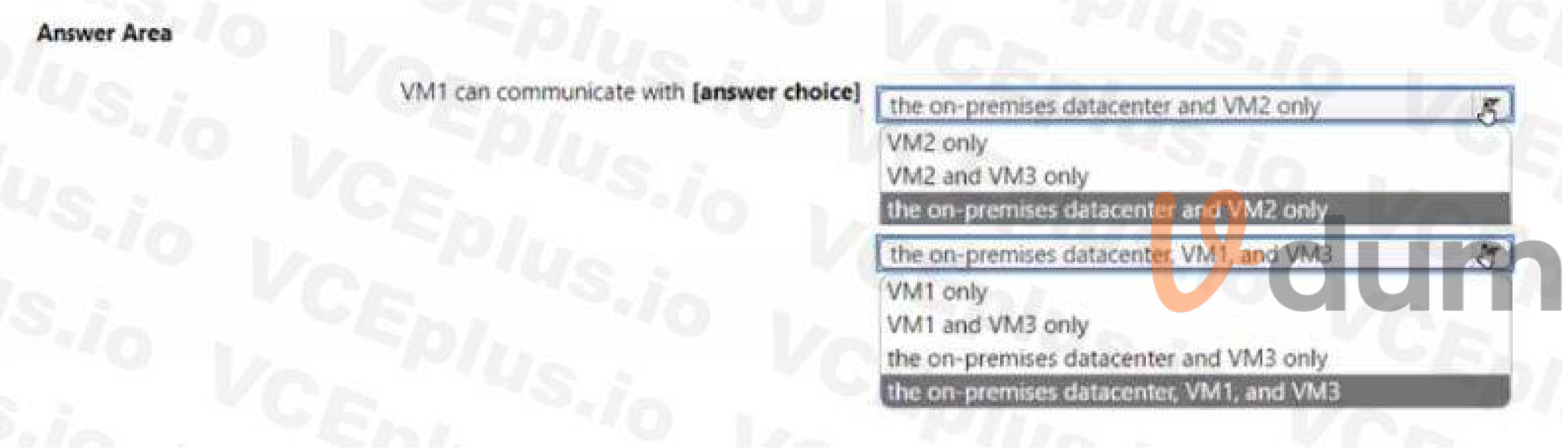
HOTSPOT

You have the Azure environment 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

VM1 can communicate with **[answer choice]**

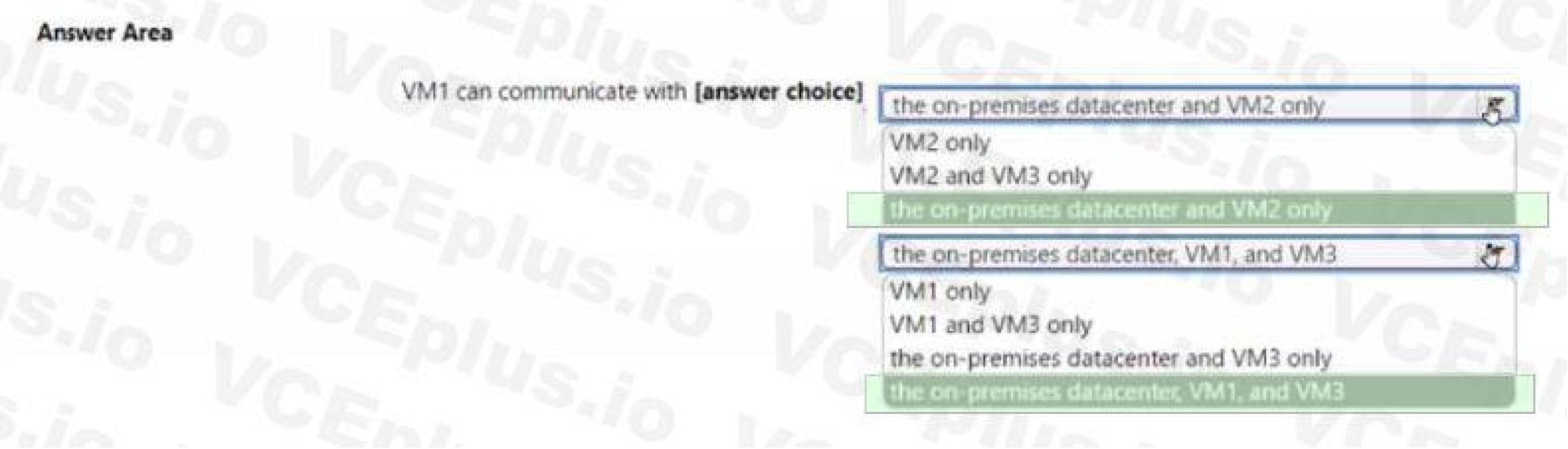
the on-premises datacenter and VM2 only

VM2 only
VM2 and VM3 only
the on-premises datacenter and VM2 only

the on-premises datacenter, VM1, and VM3

VM1 only
VM1 and VM3 only
the on-premises datacenter and VM3 only
the on-premises datacenter, VM1, and VM3

Answer Area:



Answer Area

VM1 can communicate with **[answer choice]**

the on-premises datacenter and VM2 only

VM2 only
VM2 and VM3 only
the on-premises datacenter and VM2 only

the on-premises datacenter, VM1, and VM3

VM1 only
VM1 and VM3 only
the on-premises datacenter and VM3 only
the on-premises datacenter, VM1, and VM3

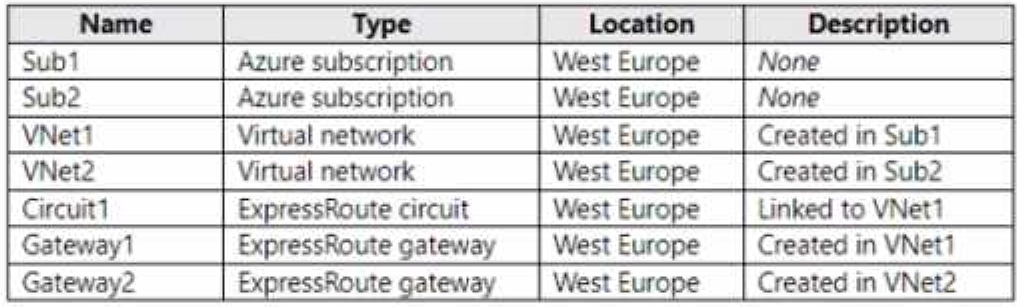
Section:

Explanation:

QUESTION 68

HOTSPOT

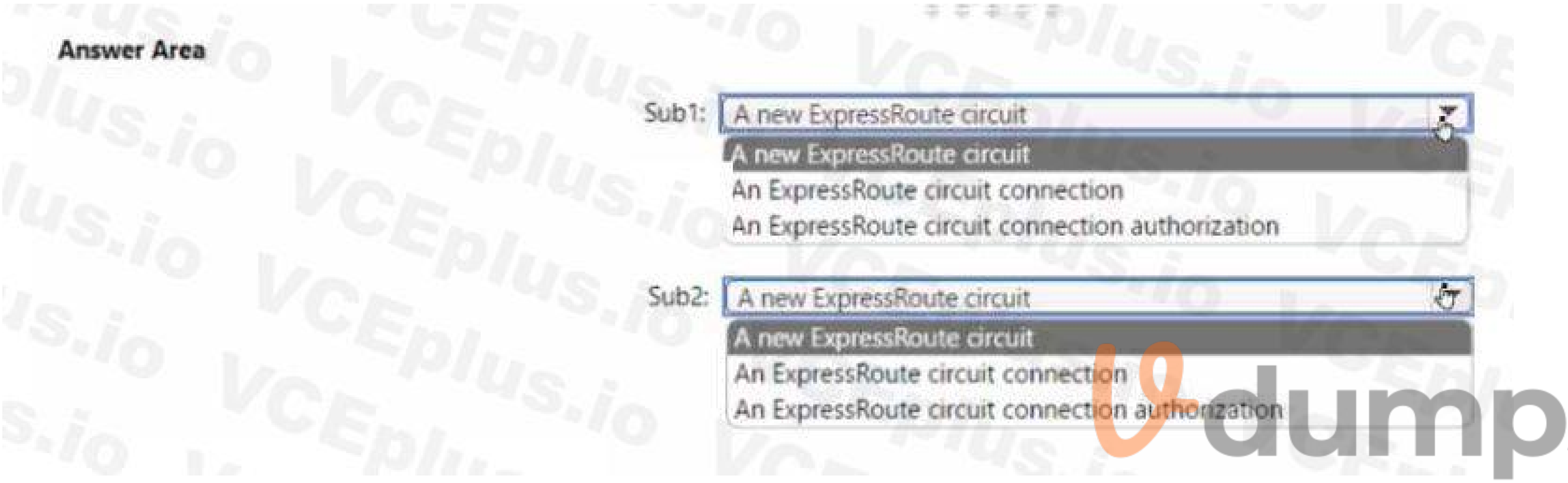
You have the Azure resources shown in the following table.



Name	Type	Location	Description
Sub1	Azure subscription	West Europe	*None*
Sub2	Azure subscription	West Europe	*None*
VNet1	Virtual network	West Europe	Created in Sub1
VNet2	Virtual network	West Europe	Created in Sub2
Circuit1	ExpressRoute circuit	West Europe	Linked to VNet1
Gateway1	ExpressRoute gateway	West Europe	Created in VNet1
Gateway2	ExpressRoute gateway	West Europe	Created in VNet2

You need to link VNei2 to Circuit1
What should you create in each subscription? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

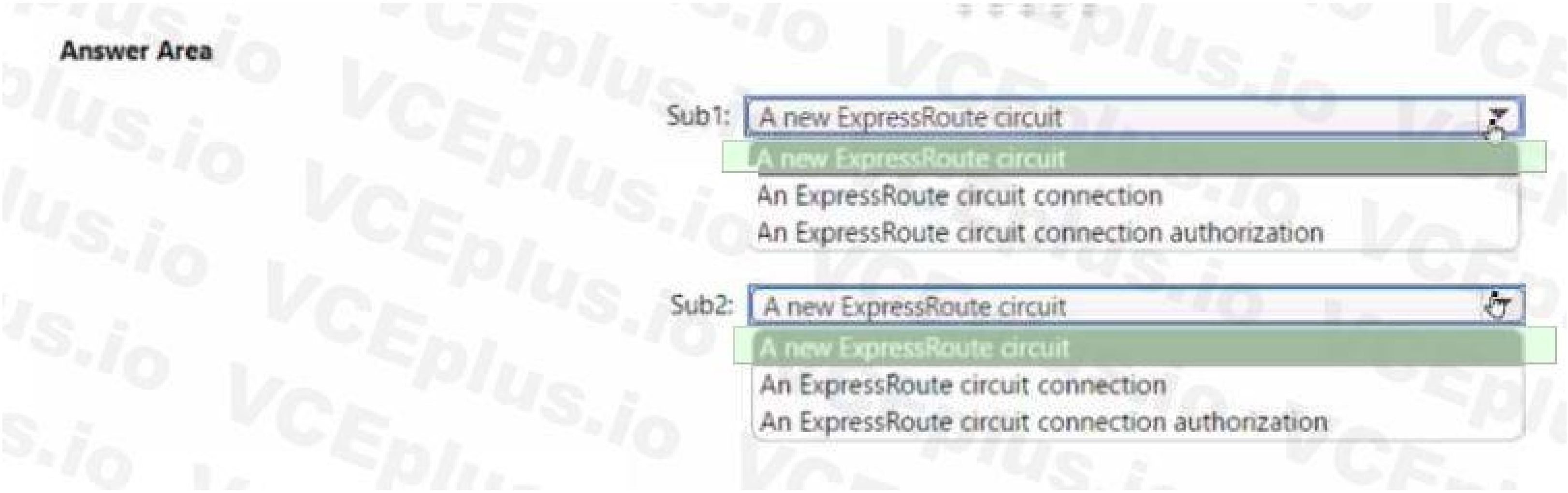


Answer Area

Sub1: A new ExpressRoute circuit
- A new ExpressRoute circuit
- An ExpressRoute circuit connection
- An ExpressRoute circuit connection authorization

Sub2: A new ExpressRoute circuit
- A new ExpressRoute circuit
- An ExpressRoute circuit connection
- An ExpressRoute circuit connection authorization

Answer Area:



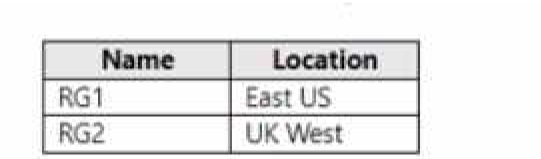
Answer Area

Sub1: A new ExpressRoute circuit
- [✓ A new ExpressRoute circuit]
- An ExpressRoute circuit connection
- An ExpressRoute circuit connection authorization

Sub2: A new ExpressRoute circuit
- [✓ A new ExpressRoute circuit]
- An ExpressRoute circuit connection
- An ExpressRoute circuit connection authorization

Section:
Explanation:

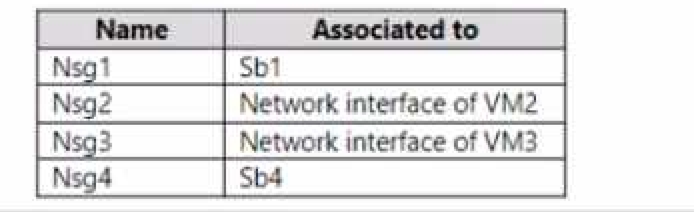
QUESTION 69
HOTSPOT
You have an Azure subscription that contains the resource groups shown in the following table.



Name	Location
RG1	East US
RG2	UK West

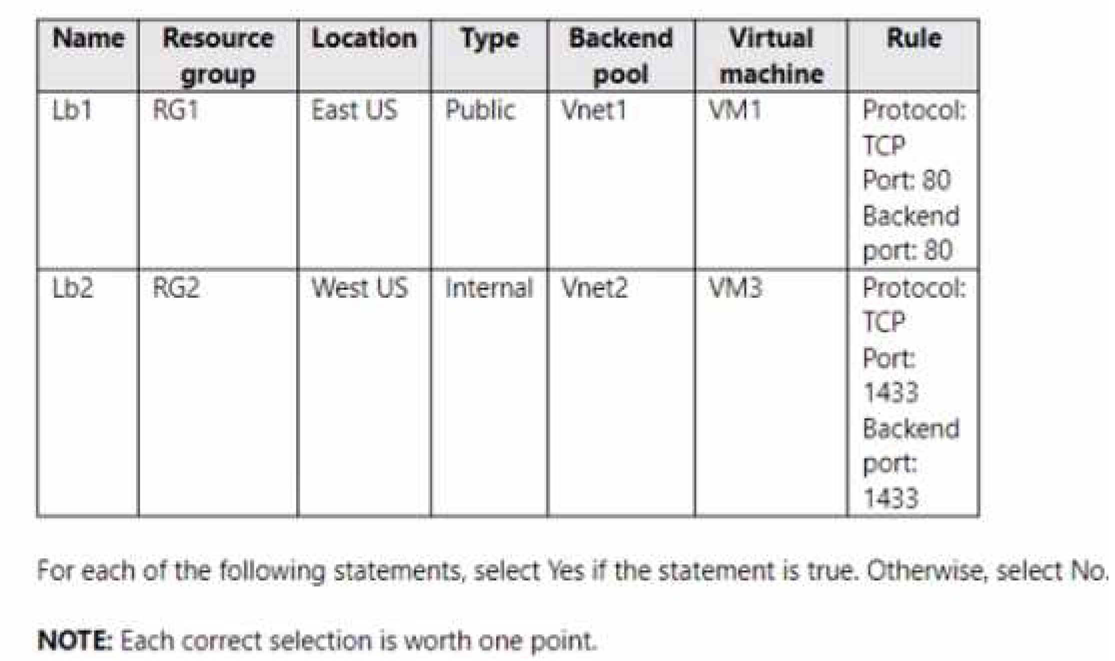
You have the virtual networks shown in the following table.

Vne1l 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.

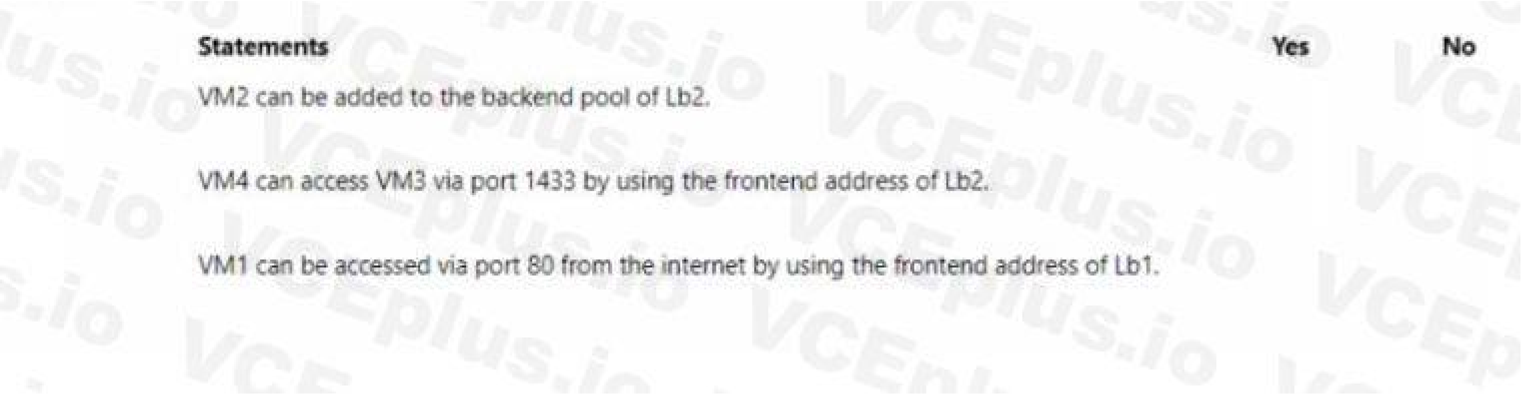


Name	Resource group	Location	Type	Backend pool	Virtual machine	Rule
Lb1	RG1	East US	Public	Vnet1	VM1	Protocol: TCP Port: 80 Backend port: 80
Lb2	RG2	West US	Internal	Vnet2	VM3	Protocol: TCP Port: 1433 Backend port: 1433

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

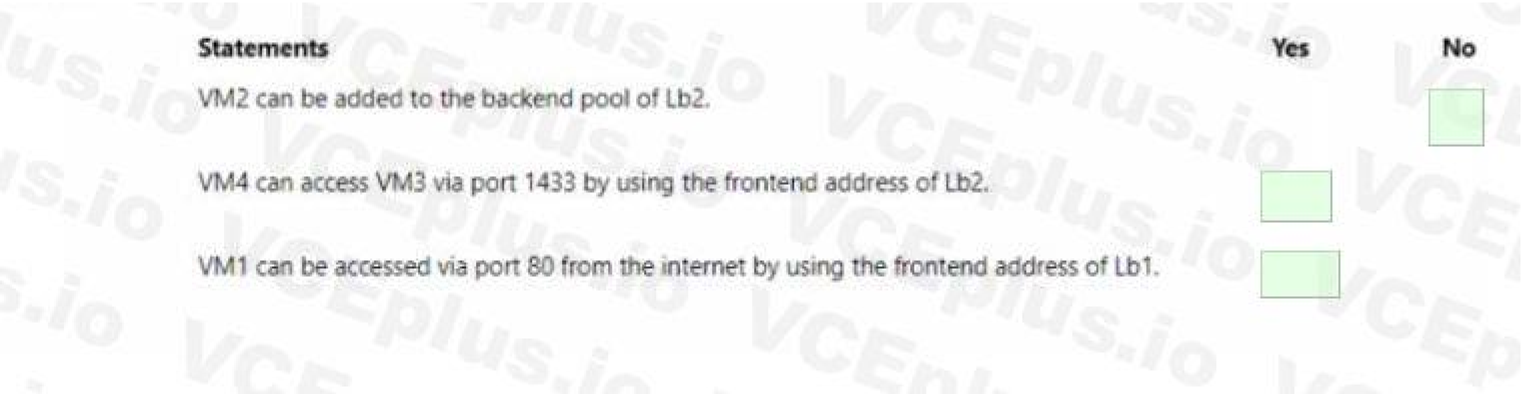
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
VM2 can be added to the backend pool of Lb2.		
VM4 can access VM3 via port 1433 by using the frontend address of Lb2.		
VM1 can be accessed via port 80 from the internet by using the frontend address of Lb1.		

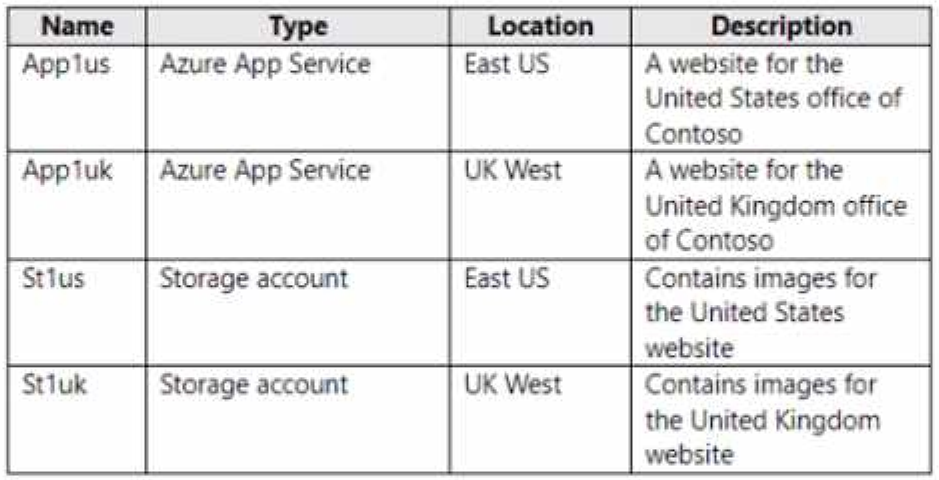
Answer Area:



Statements	Yes	No
VM2 can be added to the backend pool of Lb2.		🟩
VM4 can access VM3 via port 1433 by using the frontend address of Lb2.	🟩	
VM1 can be accessed via port 80 from the internet by using the frontend address of Lb1.	🟩	

Section:
Explanation:

QUESTION 70
DRAG DROP
Your company, named Contoso, Ltd, has an Azure subscription that contains the resources show in the following table.



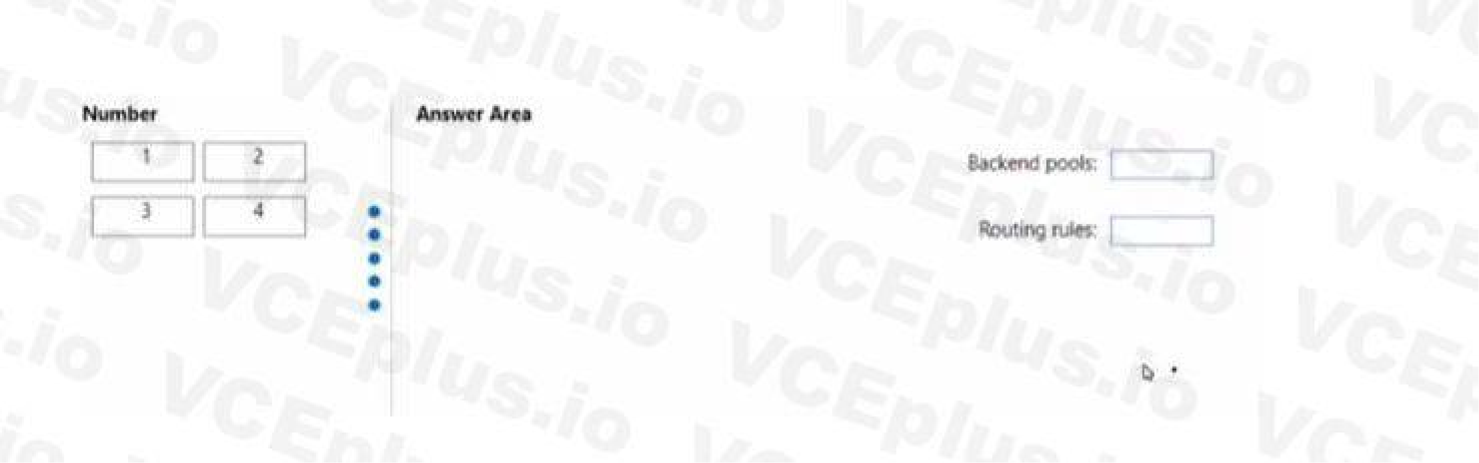
Name	Type	Location	Description
App1us	Azure App Service	East US	A website for the United States office of Contoso
App1uk	Azure App Service	UK West	A website for the United Kingdom office of Contoso
St1us	Storage account	East US	Contains images for the United States website
St1uk	Storage account	UK West	Contains images for the United Kingdom website

You plan to deploy Azure Front Door. The solution must meet the following requirement:

- Requests to a URL of https://contoso.azurefd.net/uk must be routed to App1uk.
- Requests to a URL of https://contoso.azurefd.net/us must be routed to App1us.
- Requests to a URL of https://contoso.azurefd.net/images must be routed to the storage account closest to the user.

What is the minimum number of backend pools and routing rules you should create? To answer, the appropriate number to the correct component. Each number may be used once, more than once, or not at all. You may need to drag the spilt bar between panes scroll to view content:
Note: Each correct selection is worth one point.

Select and Place:



Number

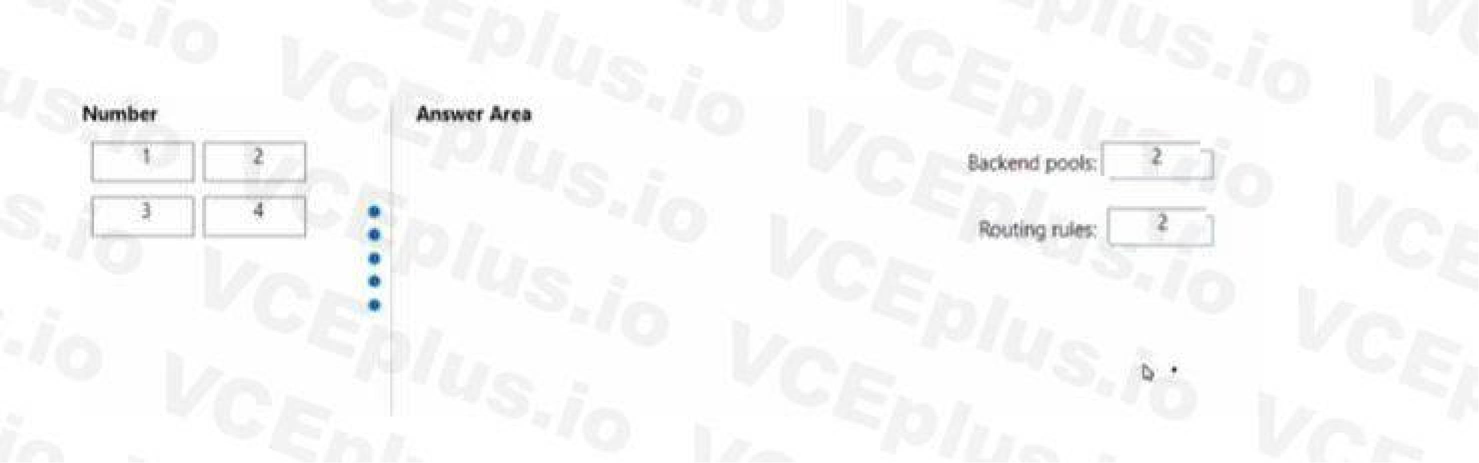
1 2
3 4

Answer Area

Backend pools:

Routing rules:

Correct Answer:

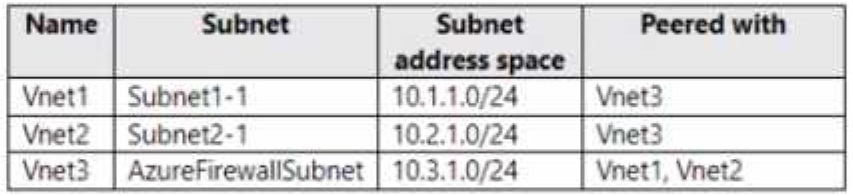


Backend pools: 2

Routing rules: 2

Section:
Explanation:

QUESTION 71
You have the Azure virtual networks shown in the following table.



Name	Subnet	Subnet address space	Peered with
Vnet1	Subnet1-1	10.1.1.0/24	Vnet3
Vnet2	Subnet2-1	10.2.1.0/24	Vnet3
Vnet3	AzureFirewallSubnet	10.3.1.0/24	Vnet1, Vnet2

You deploy Azure Firewall to Vnet3.
You need to ensure that the traffic from Subnet1-1 to Subnet2-1 passes through the firewall. What should you configure?

A. peering links between Vnet1 and Vnet2
B. a route table associated to Subnet1 -1 and Subnet2-1
C. an Azure private DNS zone
D. a route table associated to AzureFitewallSubnet

Correct Answer: D
Section:

QUESTION 72
You plan to implement an Azure virtual network that will contain 10 virtual subnets. The subnets will use IPv6 addresses. Each subnet will host up to 200 load-balanced virtual machines.
You need to recommend which subnet mask size to use for the virtual subnets.
What should you recommend?

A. /64
B. /120
C. /48
D. /24

Correct Answer: A
Section:

QUESTION 73

You have 10 on-premises networks that are connected by using a 3rd party Software Defined Wide Area Network (SD-WAN) solution. You have an Azure subscription that contains five virtual networks.
You plan to connect the Azure virtual networks and the on-premises networks by using an Azure Virtual WAN with a single virtual WAN hub.
You need to ensure that the Azure Virtual WAN can act as a node in the 3rd party SD-WAN solution.
What should you include in the solution?

A. An Azure Virtual WAN ExpressRoute gateway

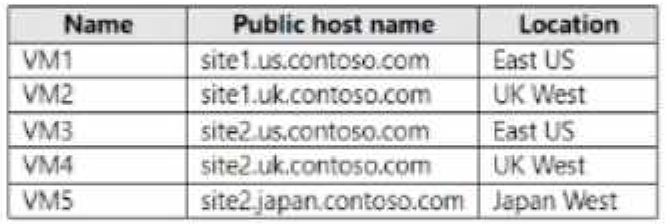
B. A Network Virtual Appliance (NVA)

C. A Site to site gateway (VPN gateway)

D. A Point to site gateway (User VPN gateway)

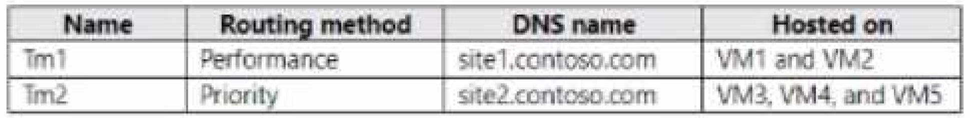
Correct Answer: B
Section:
Explanation:

QUESTION 74
HOTSPOT
You have an Azure subscription. The subscription contains virtual machines that host websites as shown in the following table.



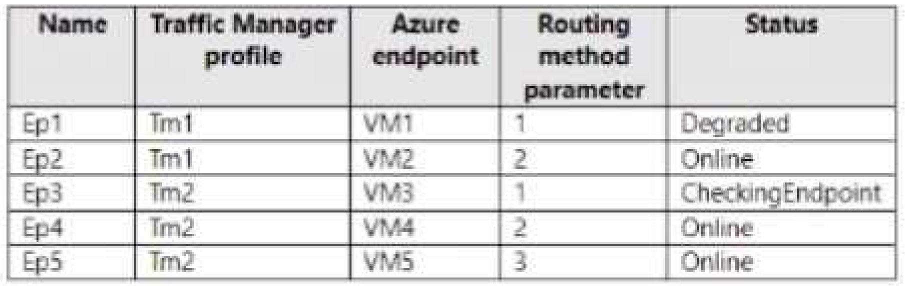
Name	Public host name	Location
VM1	site1.us.contoso.com	East US
VM2	site1.uk.contoso.com	UK West
VM3	site2.us.contoso.com	East US
VM4	site2.uk.contoso.com	UK West
VM5	site2.japan.contoso.com	Japan West

You have the Azure Traffic Manager profiles shown in the following table.



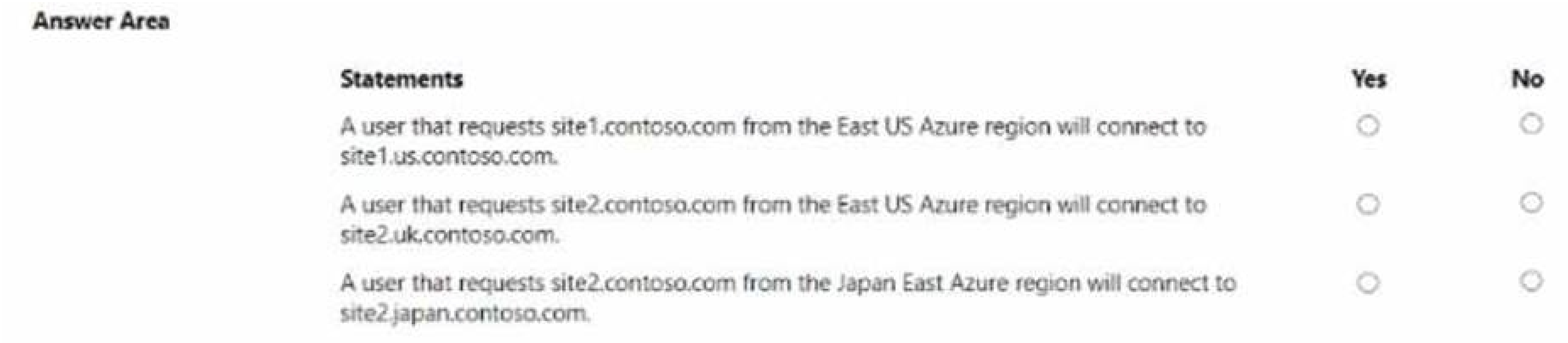
Name	Routing method	DNS name	Hosted on
Tm1	Performance	site1.contoso.com	VM1 and VM2
Tm2	Priority	site2.contoso.com	VM3, VM4, and VM5

You have the endpoints shown in the following table.



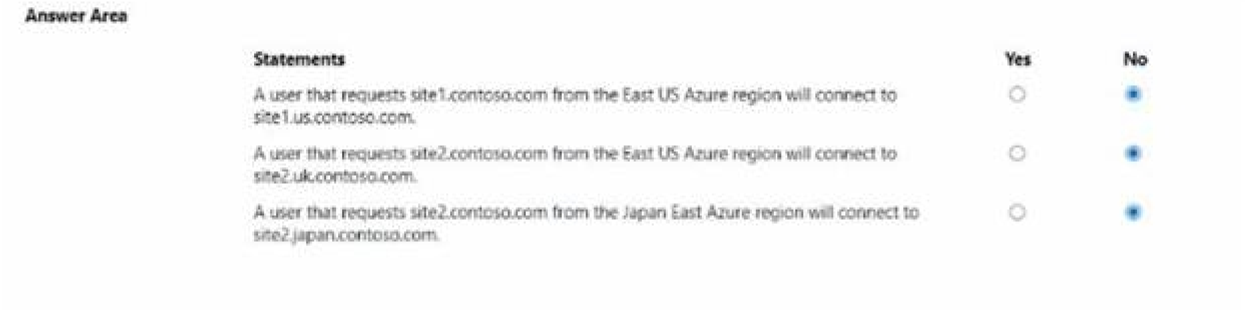
Name	Traffic Manager profile	Azure endpoint	Routing method parameter	Status
Ep1	Tm1	VM1	1	Degraded
Ep2	Tm1	VM2	2	Online
Ep3	Tm2	VM3	1	CheckingEndpoint
Ep4	Tm2	VM4	2	Online
Ep5	Tm2	VM5	3	Online

For each of the following statements, select Yes if the statement is true. Otherwise select No.
NOTE: Each connect selection is worth one point.
Answer:



Answer Area

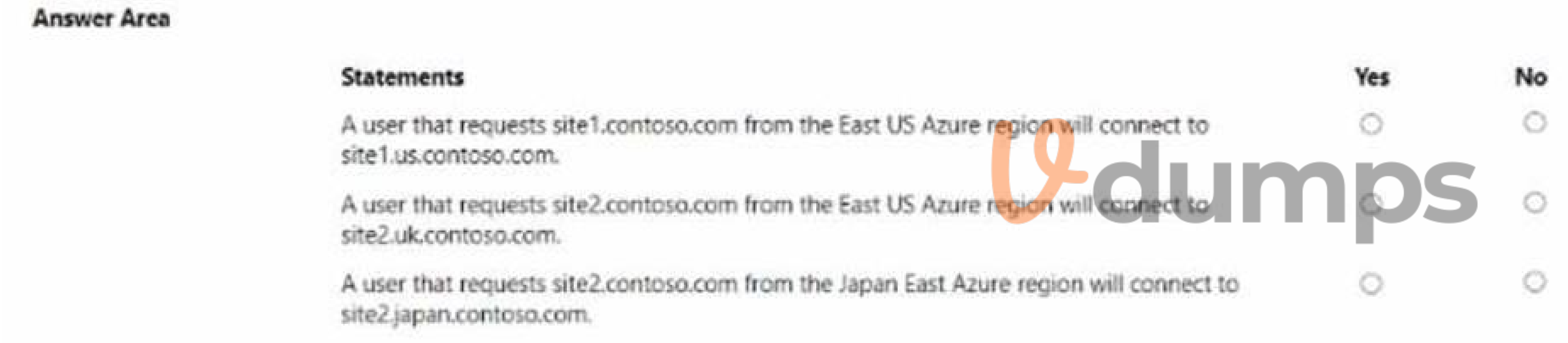
Statements	Yes	No
A user that requests site1.contoso.com from the East US Azure region will connect to site1.us.contoso.com.	○	○
A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com.	○	○
A user that requests site2.contoso.com from the Japan East Azure region will connect to site2.japan.contoso.com.	○	○



Answer Area

Statements	Yes	No
A user that requests site1.contoso.com from the East US Azure region will connect to site1.us.contoso.com.	○	●
A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com.	○	●
A user that requests site2.contoso.com from the Japan East Azure region will connect to site2.japan.contoso.com.	○	●

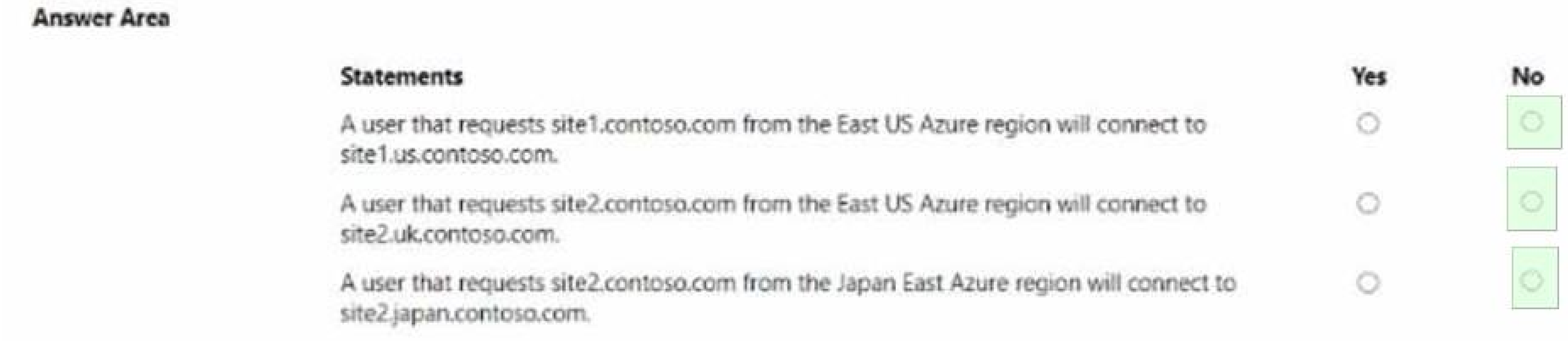
Hot Area:



Answer Area

Statements	Yes	No
A user that requests site1.contoso.com from the East US Azure region will connect to site1.us.contoso.com.	○	○
A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com.	○	○
A user that requests site2.contoso.com from the Japan East Azure region will connect to site2.japan.contoso.com.	○	○

Answer Area:



Answer Area

Statements	Yes	No
A user that requests site1.contoso.com from the East US Azure region will connect to site1.us.contoso.com.	○	[✓ ○]
A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com.	○	[✓ ○]
A user that requests site2.contoso.com from the Japan East Azure region will connect to site2.japan.contoso.com.	○	[✓ ○]

Section:

Explanation:

QUESTION 75

You plan to implement an Azure virtual network that will contain 10 virtual subnets. The subnets will use IPv6 addresses. Each subnet will host up to 200 load-balanced virtual machines.

You need to recommend a load balancing solution for the virtual network. The solution must meet the following requirements:

- The virtual machines and the load balancer must be accessible only from the virtual network.
- Costs must be minimized.

What should you include in the recommendation?

A. Basic Azure Load Balancer
B. Azure Application Gateway v1 Azure Application Gateway v2
C. Azure Standard Load Balancer
D. Azure Application Gateway v2

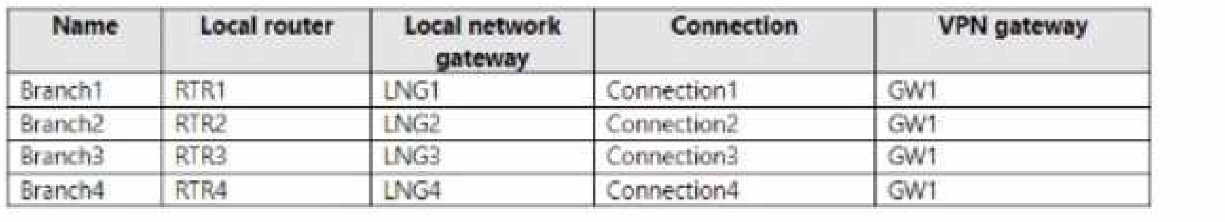
Correct Answer: C
Section:

QUESTION 76
You have three on-premises networks.
You have an Azure subscription that contains a Basic Azure virtual WAN. The virtual WAN contains a single virtual hub and a virtual network ateway that is limited to a throughput of 1 Gbps.
The on-premises networks connect to the virtual WAN by using Site-to-Site (S2S) VPN connections.
You need to increase the throughput of the virtual WAN to 3 Gbps. The solution must minimize administrative effort.
What should you do?

A. Upgrade the virtual WAN lo the Standard SKU.
B. Add an additional VPN gateway to the Azure subscription,
C. Create an additional virtual hub.
D. Increase the number of gateway scale units.

Correct Answer: D
Section:

QUESTION 77
Your company has four branch offices and an Azure Subscription. The subscription contains an Azure VPN gateway named GW1.
The branch offices are configured as shown in the following table.



Name	Local router	Local network gateway	Connection	VPN gateway
Branch1	RTR1	LNG1	Connection1	GW1
Branch2	RTR2	LNG2	Connection2	GW1
Branch3	RTR3	LNG3	Connection3	GW1
Branch4	RTR4	LNG4	Connection4	GW1

The branch office routers provide internet connectivity and Site-to-Site VPN connections to GW1.
The users in Branch1 report that they can connect to internet resources, but cannot access Azure resources.
You need to ensure that the Branch1 users can connect to the Azure Resources. The solution must meet the following requirements:
• Minimize downtime for all users.
• Minimize administrative effort.
What should you do first?

A. Reset RTR1.
B. Reset Connection1.
C. Reset GW1.
D. Recreate LNG1.

Correct Answer: B
Section:

QUESTION 78

HOTSPOT

You have an Azure subscription

You plan to use Azure Virtual WAN.

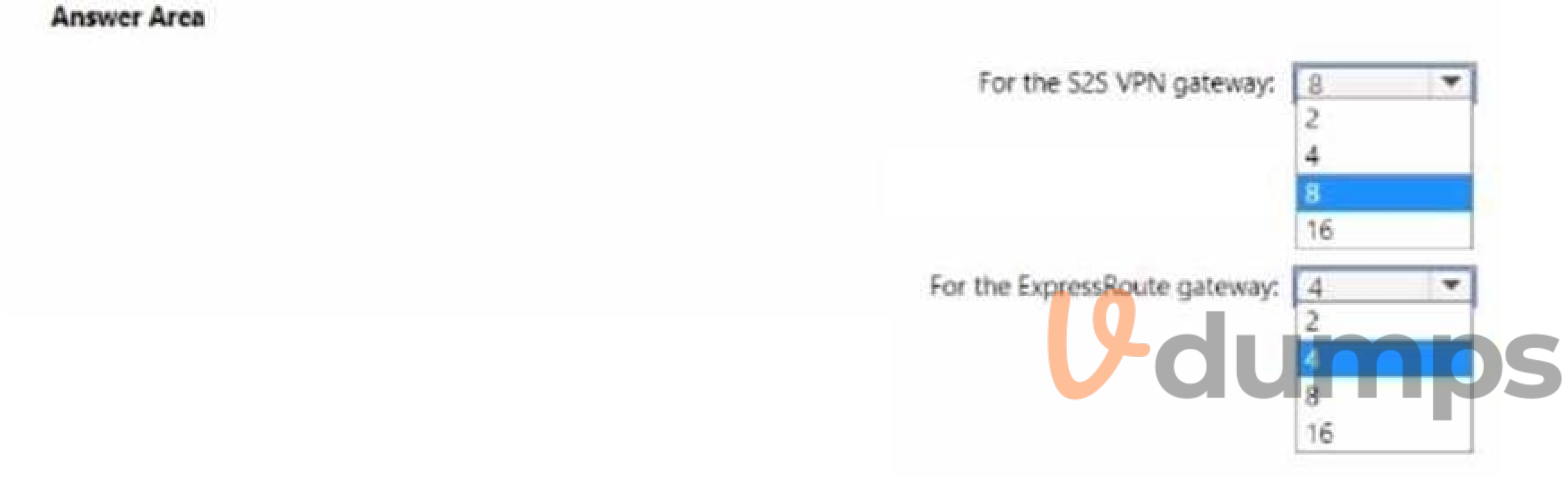
You need to deploy a virtual WAN hub that meets the following requirements:

- Supports 4 Gbps of Site-to-Site (S2S) VPN traffic
- Supports 8 Gbps of ExpressRoute traffic
- Minimizes costs

How many scale units should you configure? To answer select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Hot Area:

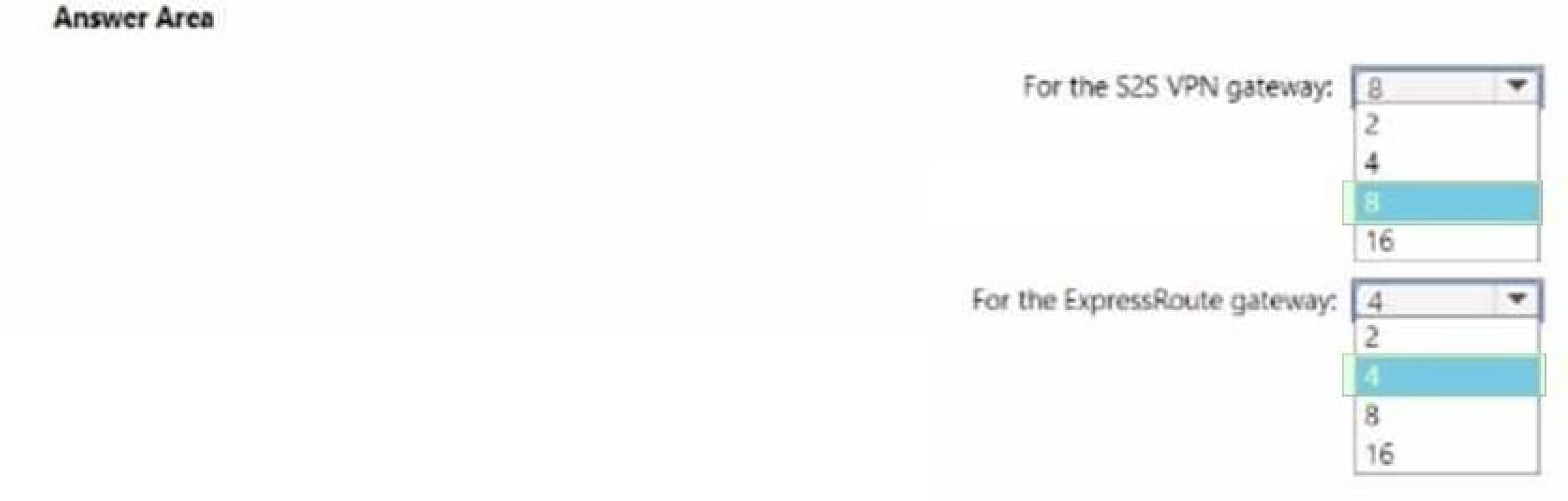


Answer Area

For the S2S VPN gateway: 8 ▼
2
4
8
16

For the ExpressRoute gateway: 4 ▼
2
4
8
16

Answer Area:



Answer Area

For the S2S VPN gateway: 8 ▼
2
4
[✓ 8]
16

For the ExpressRoute gateway: 4 ▼
2
[✓ 4]
8
16

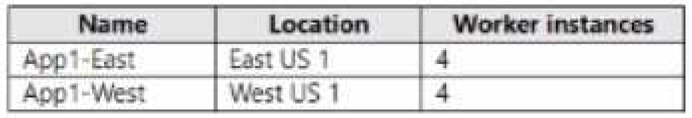
Section:

Explanation:

QUESTION 79

HOTSPOT

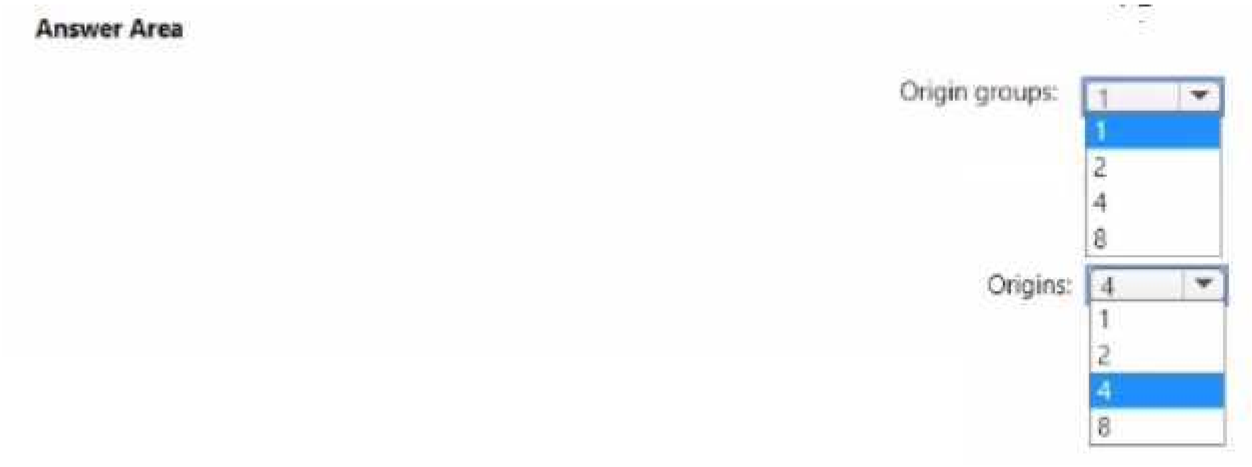
You have an Azure subscription that contains an app named Appl. App1 is deployed to the Azure App Service apps show in the following table.



Name	Location	Worker instances
App1-East	East US 1	4
App1-West	West US 1	4

You need to publish App1 by using Azure Front Door. The solution must ensure that all the requests to App1 are load balanced between all the available worker instances.
What is the minimum number of origin groups and origins that you should configure? To answer,
select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer:

Hot Area:

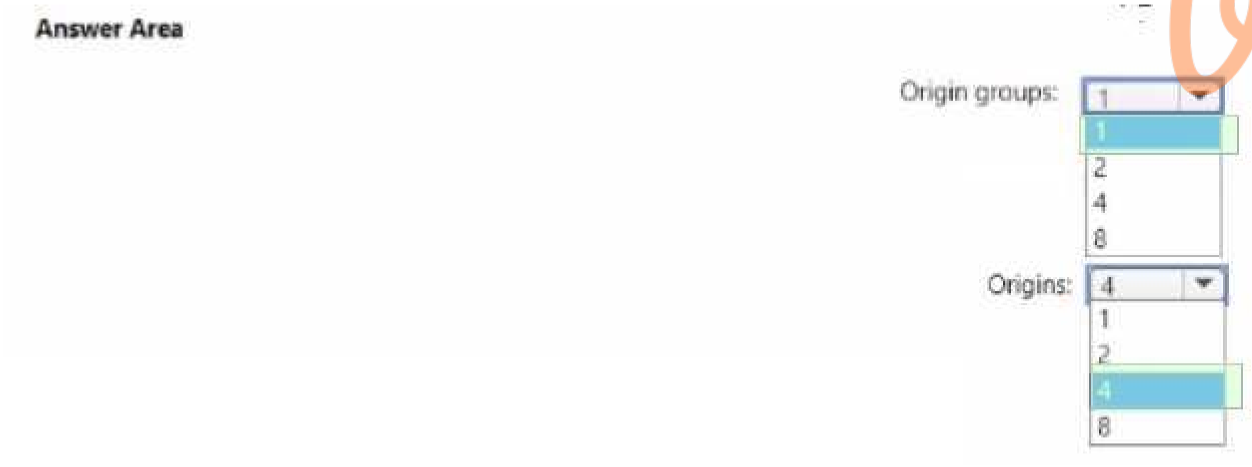


Answer Area

Origin groups: 1

Origins: 4

Answer Area:



Answer Area

Origin groups: 1

Origins: 4

Section:
Explanation:

QUESTION 80
You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains 20 subnets and 500 virtual machines. Each subnet contains a virtual machine that runs network monitoring software.
You have a network security group (NSG) named NSG1 associated to each subnet.
When a new subnet is created in Vnet1, an automated process creates an additional network monitoring virtual machine in the subnet and links the subnet to NSG1.
You need to create an inbound security rule in NS61 that will allow connections to the network monitoring virtual machines from an IP address of 131.107.1.15. The solution must meet the following requirements:

- Ensure that only the monitoring virtual machines receive a connection from 131.107.1.15.
- Minimize changes to NSG1 when a new subnet is created.

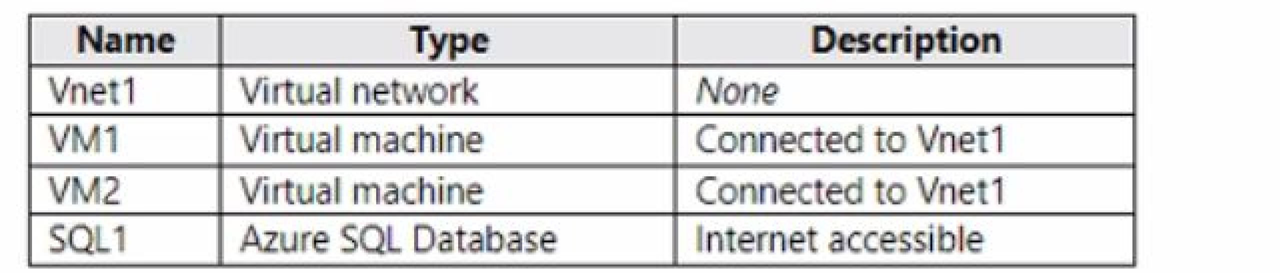
What should you use as the destination in the inbound security rule?

A. a virtual network

B. an IP address
C. an application security group
D. a service tag

Correct Answer: C
Section:

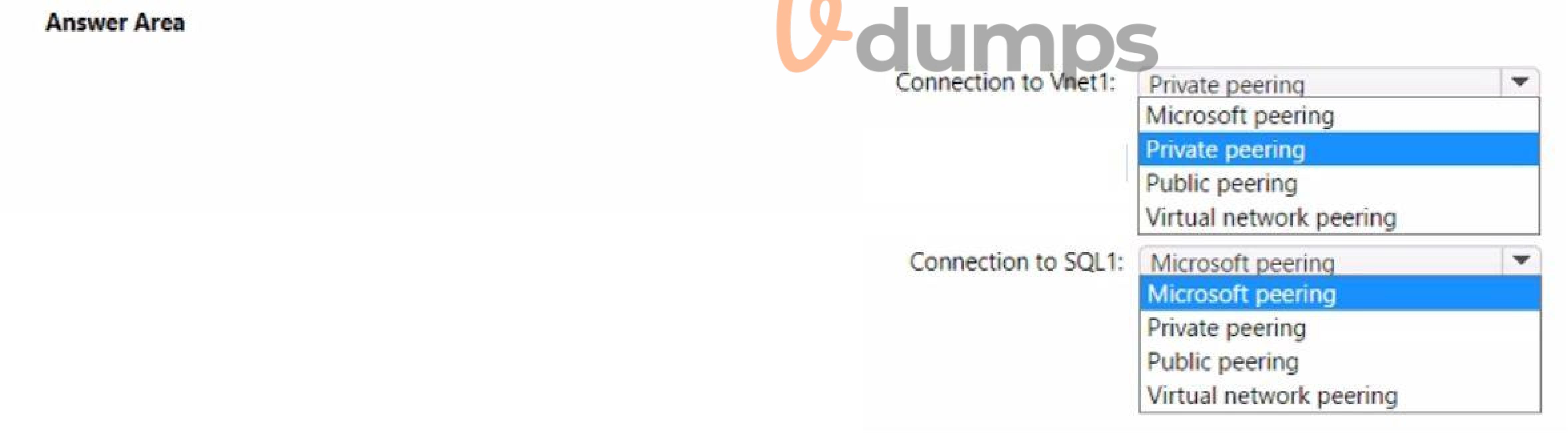
QUESTION 81
HOTSPOT
You have an on-premises network.
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
Vnet1	Virtual network	*None*
VM1	Virtual machine	Connected to Vnet1
VM2	Virtual machine	Connected to Vnet1
SQL1	Azure SQL Database	Internet accessible

You need to implement an ExpressRoute circuit to access the resources in the subscription. The solution must ensure that the on-premises network connects to the Azure resources by using the ExpressRoute circuit.
Which type of peering should you use for each connection? To answer, select the appropriate options in the answer are a.
NOTE: Each correct selection is worth one point.

Hot Area:

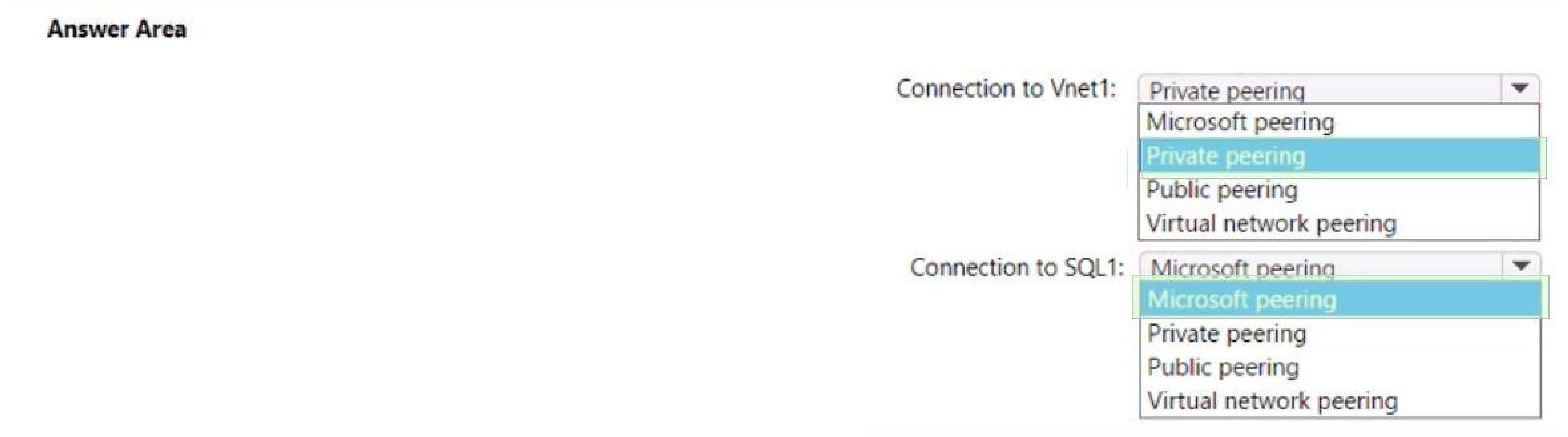


Answer Area

Connection to Vnet1: Private peering
- Microsoft peering
- Private peering
- Public peering
- Virtual network peering

Connection to SQL1: Microsoft peering
- Microsoft peering
- Private peering
- Public peering
- Virtual network peering

Answer Area:



Answer Area

Connection to Vnet1: Private peering

- Microsoft peering
- Private peering
- Public peering
- Virtual network peering

Connection to SQL1: Microsoft peering

- Microsoft peering
- Private peering
- Public peering
- Virtual network peering

Section:
Explanation:

QUESTION 82
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAF1.
You need to configure a rate limit for incoming requests to AFD1.
Solution: You modify the policy settings of WAF1.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 83
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAFT.
You need to configure a rate limit for incoming requests to AFD1.
Solution: You configure a custom rule for WAF1.
Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:

QUESTION 84

LAB 1

You plan to deploy a firewall to subnetl-2. The firewall will have an IP address of 10.1.2.4.

You need to ensure that traffic from subnetl-1 to the IP address range of 192.168.10.0/24 is routed through the firewall that will be deployed to subnetl-2. The solution must be achieved without using dynamic routing protocols.

A. See the Explanation below for step by step instructions

Correct Answer: A

Section:

Explanation:

To deploy a firewall to subnetl-2, you need to create a network virtual appliance (NVA) in the same virtual network as subnetl-2.An NVA is a virtual machine that performs network functions, such as firewall, routing, or load balancing1.

To create an NVA, you need to create a virtual machine in the Azure portal and select an image that has the firewall software installed.You can choose from the Azure Marketplace or upload your own image2.

To assign the IP address of 10.1.2.4 to the NVA, you need to create a static private IP address for the network interface of the virtual machine.You can do this in the IP configurations settings of the network interface3.

To ensure that traffic from subnetl-1 to the IP address range of 192.168.10.0/24 is routed through the NVA, you need to create a user-defined route (UDR) table and associate it with subnetl-1.A UDR table allows you to override the default routing behavior of Azure and specify custom routes for your subnets4.

To create a UDR table, you need to go to the Route tables service in the Azure portal and select + Create.You can give a name and a resource group for the route table5.

To create a custom route, you need to select Routes in the route table and select + Add.You can enter the following information for the route5:

Destination: 192.168.10.0/24

Next hop type: Virtual appliance

Next hop address: 10.1.2.4

To associate the route table with subnetl-1, you need to select Subnets in the route table and select + Associate.You can select the virtual network and subnet that you want to associate with the route table5.

QUESTION 85

LAB 2

You need to create an Azure Firewall instance named FW1 that meets the following requirements:

* Has an IP address from the address range of 10.1.255.0/24

* Uses a new Premium firewall policy named FW-pohcy1

* Routes traffic directly to the internet

A. See the Explanation below for step by step instructions

Correct Answer: A

Section:

Explanation:

To create an Azure Firewall instance, you need to go to the Azure portal and select Create a resource. Type firewall in the search box and press Enter.Select Firewall and then select Create1.

To assign an IP address from the address range of 10.1.255.0/24 to the firewall, you need to select a public IP address that belongs to that range.You can either create a new public IP address or use an existing one1.

To use a new Premium firewall policy named FW-policy1, you need to select Premium as the Firewall tier and create a new policy with the name FW-policy12.A Premium firewall policy allows you to configure advanced features such as TLS Inspection, IDPS, URL Filtering, and Web Categories3.

To route traffic directly to the internet, you need to enable SNAT (Source Network Address Translation) for the firewall.SNAT allows the firewall to use its public IP address as the source address for outbound traffic4.

QUESTION 86

LAB 3

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.

A. See the Explanation below for step by step instructions

Correct Answer: A
Section:
Explanation:
Here are the steps and explanations for creating a policy that can be linked to the planned application gateway and block connections from IP addresses in the 131.107.150.0/24 range:
To create a policy, you need to go to the Azure portal and selectCreate a resource.Search forWAF, selectWeb Application Firewall, then selectCreate1.
On theCreate a WAF policypage,Basicstab, 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
On theCustom rulestab, selectAdd a ruleto create a custom rule that blocks connections from IP addresses in the 131.107.150.0/24 range2. Enter or select the following information for the custom rule:
Rule name: Type a unique name for your custom rule
Priority: Type a number that indicates the order of evaluation for this rule
Rule type: Select Match rule
Match variable: Select RemoteAddr
Operator: Select IPMatch
Match values: Type 131.107.150.0/24
Action: Select Block
On theReview + createtab, review your settings and selectCreateto create your WAF policy1.
To link your policy to the planned application gateway, you need to go to theApplication Gatewayservice in the Azure portal and select your application gateway3.
On theWeb application firewalltab, select your WAF policy from the drop-down list and selectSave

QUESTION 87
LAB 4
You need to ensure that connections to the storage34280945 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name storage34280945.pnvatelinlcblob.core.windows.net.

A. See the Explanation below for step by step instructions

Correct Answer: A
Section:
Explanation:
Here are the steps and explanations for ensuring that connections to the storage34280945 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name stor-age34280945.pnvatelinlcblob.core.windows.net:
To allow access from a specific IP address range, you need to configure the Azure Storage firewall and virtual network settings for your storage account.You can do this in the Azure portal by selecting your storage account and then selecting Networking under Settings1.
On the Networking page, select Firewalls and virtual networks, and then select Selected networks under Allow access from1. This will block all access to your storage account except from the networks or resources that you specify.
Under Firewall, select Add rule, and then enter 10.1.1.0/24 as the IP address or range.You can also enter an optional rule name and description1. This will allow access from any IP address in the 10.1.1.0/24 range.
Select Save to apply your changes1.
To map a custom domain name to your storage account, you need to create a CNAME record with your domain provider that points to your storage account endpoint2. A CNAME record is a type of DNS record that maps a source domain name to a destination domain name.
Sign in to your domain registrar's website, and then go to the page for managing DNS settings2.
Create a CNAME record with the following information2:
Source domain name: stor-age34280945.pnvatelinlcblob.core.windows.net
Destination domain name: stor-age34280945.pnvatelinlcblob.core.windows.net
Save your changes and wait for the DNS propagation to take effect2.
To register the custom domain name with Azure, you need to go back to the Azure portal and select your storage account.Then select Custom domain under Blob service2.
On the Custom domain page, enter stor-age34280945.pnvatelinlcblob.core.windows.net as the custom domain name and select Save2.

QUESTION 88

LAB 5
You need to ensure that requests for wwwjelecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net.

A. See the Explanation below for step by step instructions

Correct Answer: A
Section:
Explanation:
Here are the steps and explanations for ensuring that requests for wwwjelecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net:
To use a custom domain with your Azure Front Door, you need to create a CNAME record with your domain provider that points to the Front Door default frontend host.A CNAME record is a type of DNS record that maps a source domain name to a destination domain name1.
To create a CNAME record, you need to sign in to your domain registrar's website and go to the page for managing DNS settings1.
Create a CNAME record with the following information1:
Source domain name: wwwjelecloud.com
Destination domain name: frontdoor1.azurefd.net
Save your changes and wait for the DNS propagation to take effect1.
To verify the custom domain, you need to go to the Azure portal and select your Front Door profile.Then select Domains under Settings and select Add2.
On the Add a domain page, select Non-Azure validated domain as the Domain type and enter wwwjelecloud.com as the Domain name.Then select Add2.
On the Domains page, select wwwjelecloud.com and select Verify.This will check if the CNAME record is correctly configured2.
Once the domain is verified, you can associate it with your Front Door endpoint. On the Domains page, select wwwjelecloud.com and select Associate endpoint.Then select your Front Door endpoint from the drop-down list and select Associate2.

QUESTION 89
LAB 6
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.

A. See the Explanation below for step by step instructions

Correct Answer: A
Section:
Explanation:
Here are the steps and explanations for ensuring that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address:
To use the same static public IP address for multiple hosts, you need to create a NAT gateway and associate it with subnet3-2.A NAT gateway is a resource that performs network address translation (NAT) for outbound traffic from a subnet1.It allows you to use a single public IP address for multiple private IP addresses2.
To create a NAT gateway, you need to go to the Azure portal and selectCreate a resource.Search forNAT gateway, selectNAT gateway, then selectCreate3.
On theCreate a NAT gatewaypage, enter or select the following information and accept the defaults for the remaining settings:
Subscription: Select your subscription name
Resource group: Select your resource group
Name: Type a unique name for your NAT gateway
Region: Select the same region as your virtual network
Public IP address: SelectCreate newand type a name for your public IP address.SelectStandardas the SKU andStaticas the assignment method4.
SelectReview + createand then selectCreateto create your NAT gateway3.
To associate the NAT gateway with subnet3-2, you need to go to theVirtual networksservice in the Azure portal and select your virtual network.
On theVirtual networkpage, selectSubnetsunderSettings, and then select subnet3-2 from the list.
On theEdit subnetpage, underNAT gateway, select your NAT gateway from the drop-down list. Then selectSave.

QUESTION 90
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals- Some question sets might have more than one correct solution, while others might not have a correct solution.
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.

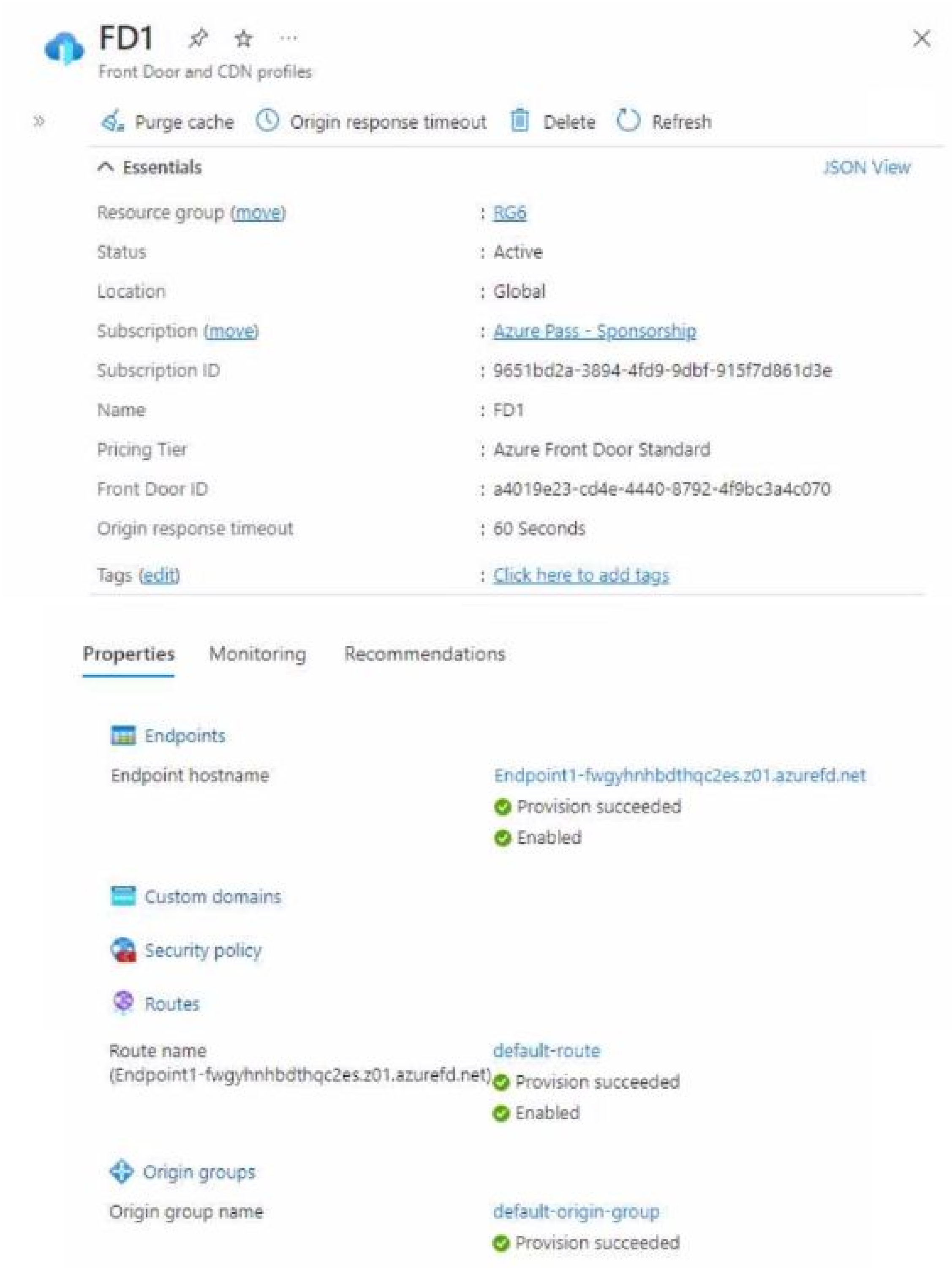
You have on Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.
Hub! has a security status of Unsecured.
You need to ensure that the security status of Hub1 is marked as Secured.
Solution: You implement Azure NAT Gateway.
Does this meet the requirement?

A. Yes

B. No

Correct Answer: B
Section:

QUESTION 91
You have an Azure subscription that contains an Azure Front Door named FD1. FD1 is configured as shown in the following exhibit.



FD1

Front Door and CDN profiles

Purge cache | Origin response timeout | Delete | Refresh

Essentials — JSON View

Resource group (move)	: RG6
Status	: Active
Location	: Global
Subscription (move)	: Azure Pass - Sponsorship
Subscription ID	: 9651bd2a-3894-4fd9-9dbf-915f7d861d3e
Name	: FD1
Pricing Tier	: Azure Front Door Standard
Front Door ID	: a4019e23-cd4e-4440-8792-4f9bc3a4c070
Origin response timeout	: 60 Seconds
Tags (edit)	: Click here to add tags

Properties | Monitoring | Recommendations

Endpoints

Endpoint hostname	Endpoint1-fwgyhnhbdthqc2es.z01.azurefd.net ✓ Provision succeeded ✓ Enabled

Custom domains

Security policy

Routes

Route name (Endpoint1-fwgyhnhbdthqc2es.z01.azurefd.net)	default-route ✓ Provision succeeded ✓ Enabled

Origin groups

Origin group name	default-origin-group ✓ Provision succeeded

You need to enable Azure Private Link for FD1.
What should you do first?

A. Create an origin group.

B. Add an endpoint.

C. Change Pricing Tier to Azure Front Door Premium.

D. Create a custom route.

Correct Answer: C
Section:

QUESTION 92

DRAG DROP

You have art Azure subscription.

You plan to deploy Azure Front Door with Azure Web Application Firewall (WAF).

You plan to implement custom rules and managed rules that meet the following requirements:

* Block malicious bots.

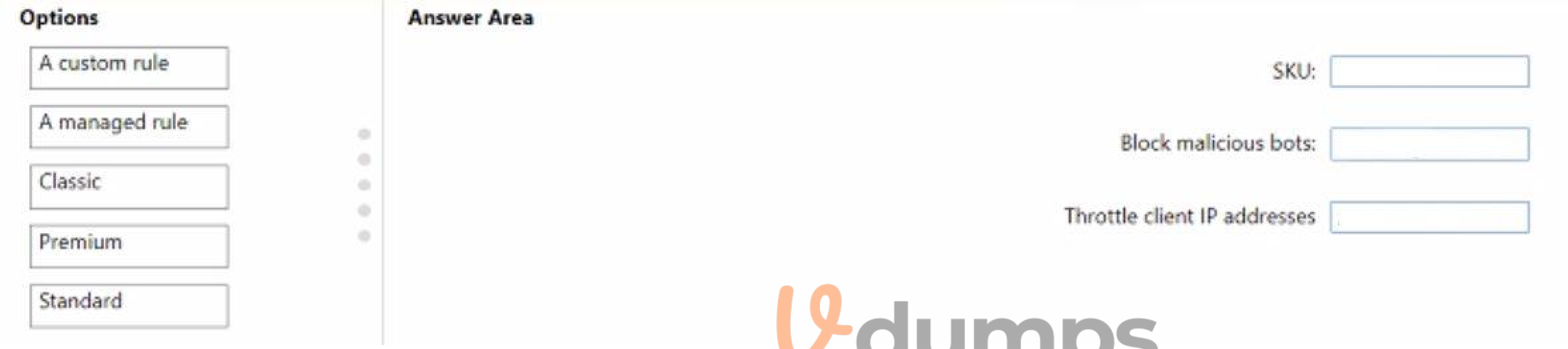
* Throttle client IP addresses that exceed 100 connections per minute.

You need to identify which Front Door SKU to configure, and which type of rule to configure for each requirement. The solution must minimize administrative effort and costs.

What should identify? To answer, drag the appropriate options to the correct targets. Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Options

A custom rule

A managed rule

Classic

Premium

Standard

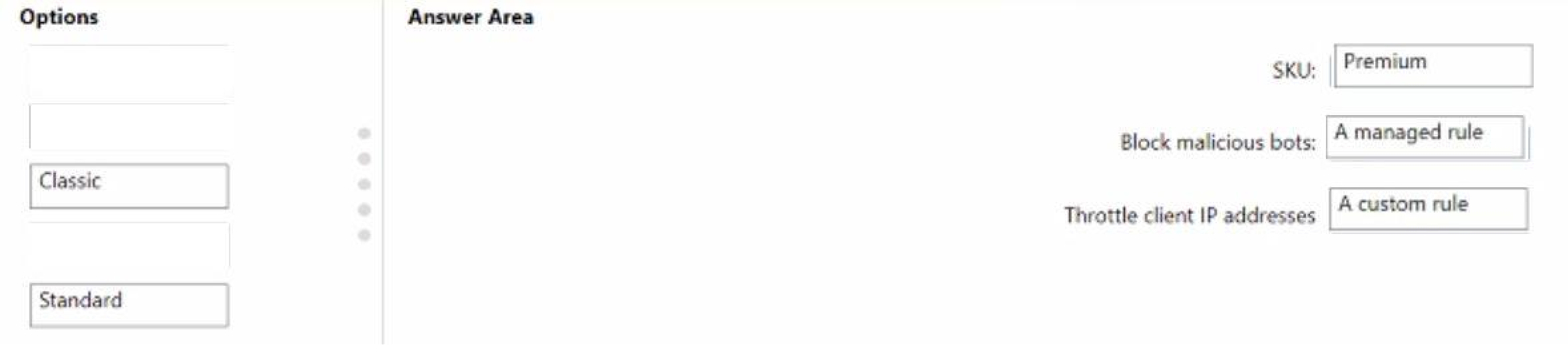
Answer Area

SKU:

Block malicious bots:

Throttle client IP addresses

Correct Answer:



Options

Classic

Standard

Answer Area

SKU: Premium

Block malicious bots: A managed rule

Throttle client IP addresses A custom rule

Section:

Explanation:

QUESTION 93

DRAG DROP

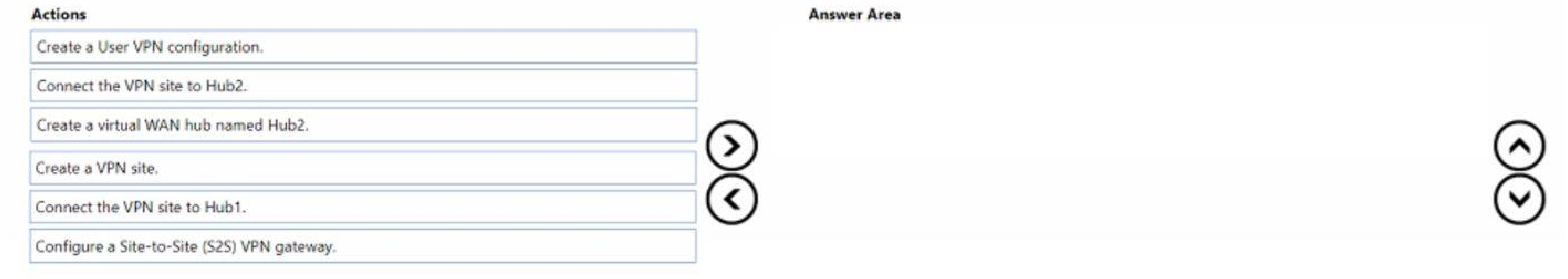
You have an on-premises network.

You have an Azure subscription that contains a virtual network named VNet1. VNet1 is connected to an Azure Virtual WAN hub named Hub1.

You need to enable connectivity between the on-premises network and VNet1 by using Hub1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

Create a User VPN configuration.

Connect the VPN site to Hub2.

Create a virtual WAN hub named Hub2.

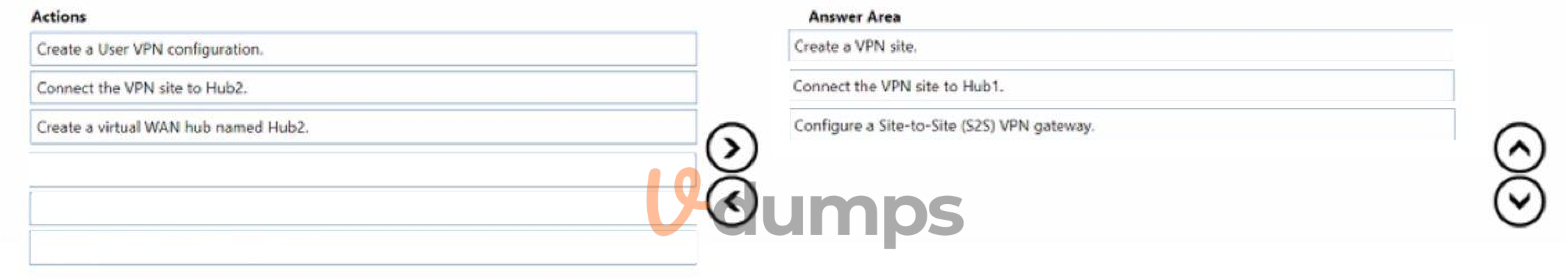
Create a VPN site.

Connect the VPN site to Hub1.

Configure a Site-to-Site (S2S) VPN gateway.

Answer Area

Correct Answer:



Actions

Create a User VPN configuration.

Connect the VPN site to Hub2.

Create a virtual WAN hub named Hub2.

Answer Area

Create a VPN site.

Connect the VPN site to Hub1.

Configure a Site-to-Site (S2S) VPN gateway.

Section:
Explanation:
Create a VPN site.
Connect the VPN site to Hub1.
Configure a Site-toSite (S2S) VPN gateway.

QUESTION 94
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 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 an Azure Front Door profile.
Does this meet the requirement?

A. Yes
B. No

Correct Answer: B
Section:

QUESTION 95

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 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 Web Application Firewall (WAF).

Does this meet the requirement?

A. Yes

B. No

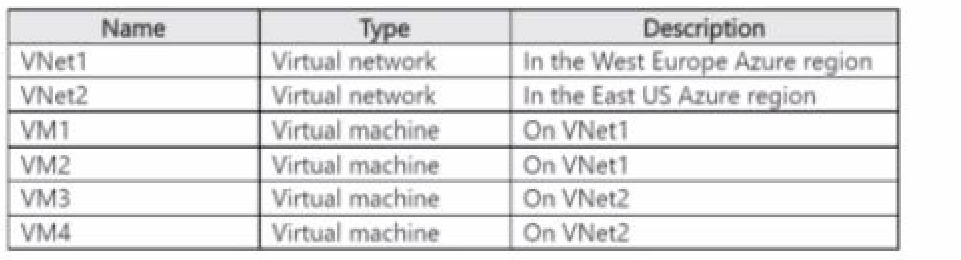
Correct Answer: B

Section:

QUESTION 96

HOTSPOT

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



Name	Type	Description
VNet1	Virtual network	In the West Europe Azure region
VNet2	Virtual network	In the East US Azure region
VM1	Virtual machine	On VNet1
VM2	Virtual machine	On VNet1
VM3	Virtual machine	On VNet2
VM4	Virtual machine	On VNet2

You plan to deploy an app named App1 to meet the following requirements.

* External users must be able to access App1 from the internet.

* App1 will be load balanced across all the virtual machines.

* App1 will be hosted on VM1, VM2. VM3. and VM4.

* App1 must be available if an Azure region fails.

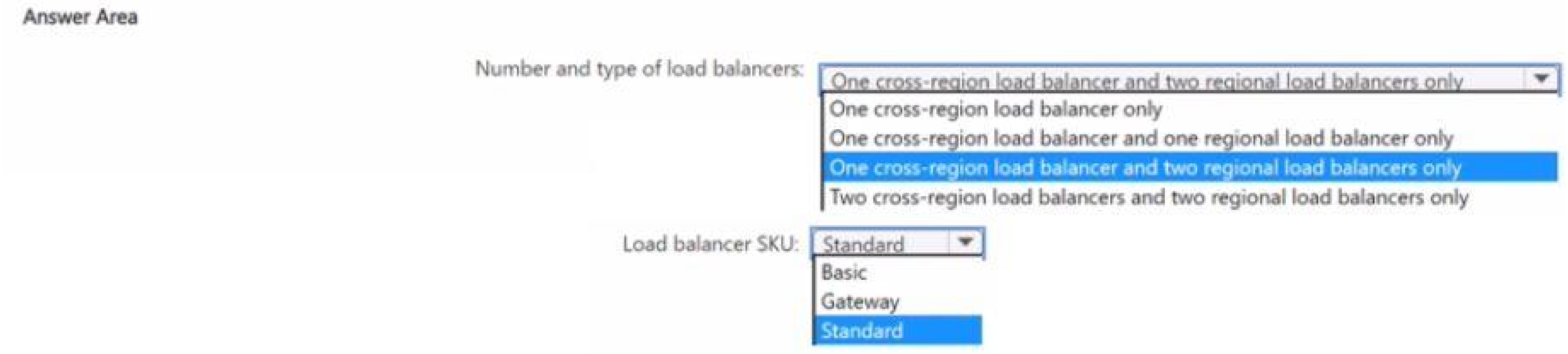
* Costs must be minimized.

You need to implement a global load balancer solution for App.

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

NOTE: Bach correct answer is worth one point.

Hot Area:



Answer Area

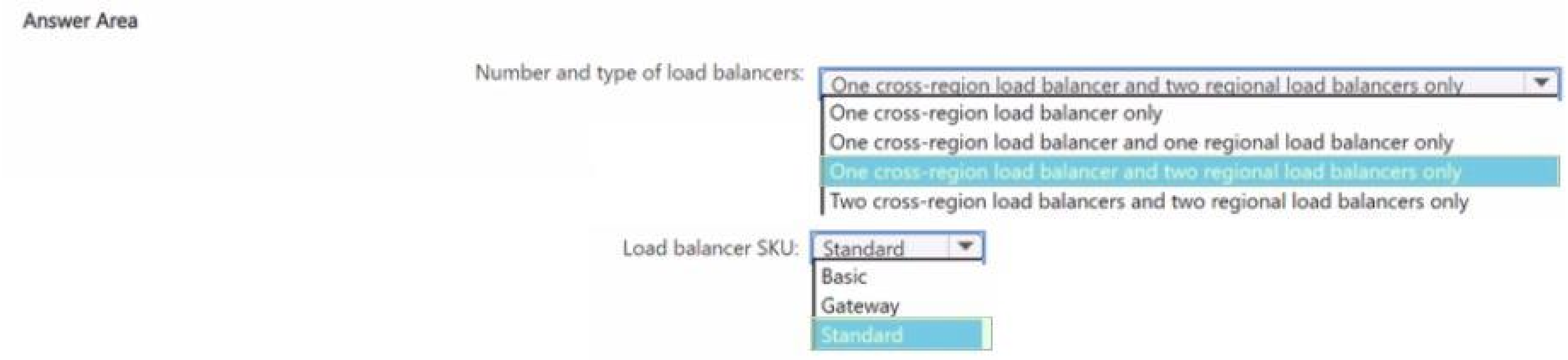
Number and type of load balancers: One cross-region load balancer and two regional load balancers only

- One cross-region load balancer only
- One cross-region load balancer and one regional load balancer only
- One cross-region load balancer and two regional load balancers only
- Two cross-region load balancers and two regional load balancers only

Load balancer SKU: Standard

- Basic
- Gateway
- Standard

Answer Area:



Answer Area

Number and type of load balancers: One cross-region load balancer and two regional load balancers only

- One cross-region load balancer only
- One cross-region load balancer and one regional load balancer only
- One cross-region load balancer and two regional load balancers only
- Two cross-region load balancers and two regional load balancers only

Load balancer SKU: Standard

- Basic
- Gateway
- Standard

Section:
Explanation:

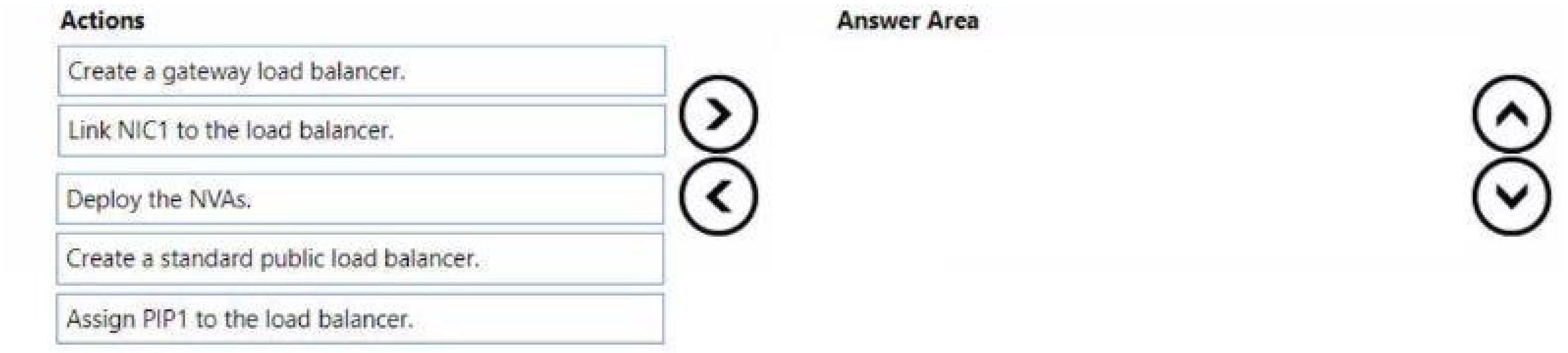
QUESTION 97
You have an Azure Private Link service named PL1 that uses an Azure load balancer named LB1. You need to ensure that PL1 can support a higher volume of outbound traffic. What should you do?

A. Redeploy LB1 with a different SKU.
B. Increase the number of NAT IP addresses assigned to PL1.
C. Deploy an Azure Application Gateway v2 instance to the source NAT subnet.
D. Increase the number of frontend IP configurations for LB1.

Correct Answer: B
Section:

QUESTION 98
DRAG DROP
You have an Azure subscription that contains a virtual machine named VM1. VM1 contains a NIC named NIC1 and a public IP address named PIP1.PIP1 is assigned to NIC1.
You plan to deploy four Network Virtual Appliances (NVAs).
You need to ensure that all the inbound traffic from the internet to PIP1 is inspected by the NVAs. The solution must ensure that the NVA deployment is highly available.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

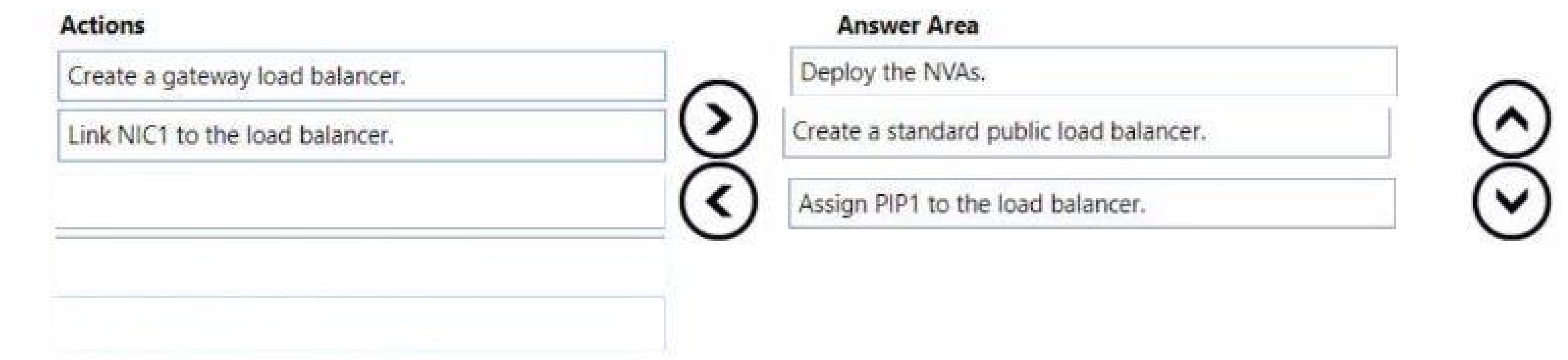


Actions

- Create a gateway load balancer.
- Link NIC1 to the load balancer.
- Deploy the NVAs.
- Create a standard public load balancer.
- Assign PIP1 to the load balancer.

Answer Area

Correct Answer:



Actions

- Create a gateway load balancer.
- Link NIC1 to the load balancer.

Answer Area

- Deploy the NVAs.
- Create a standard public load balancer.
- Assign PIP1 to the load balancer.

Section:
Explanation:
Deploy the NVAs.
Create a standard public load balancer.
Assign PIP1 to the load balancer.

QUESTION 99

HOTSPOT

You have an Azure subscription that contains a dual-stack virtual network named VNet1. VNet1 has the following IP address spaces:

* IPv4:192.168.0.0/24

* IPv6: fd0adbftdeca: deed: y48

You plan to deploy an Azure VPN gateway and multiple virtual machines to VNet1.

You need to configure the subnet masks for VNet1. The solution must meet the following requirements:

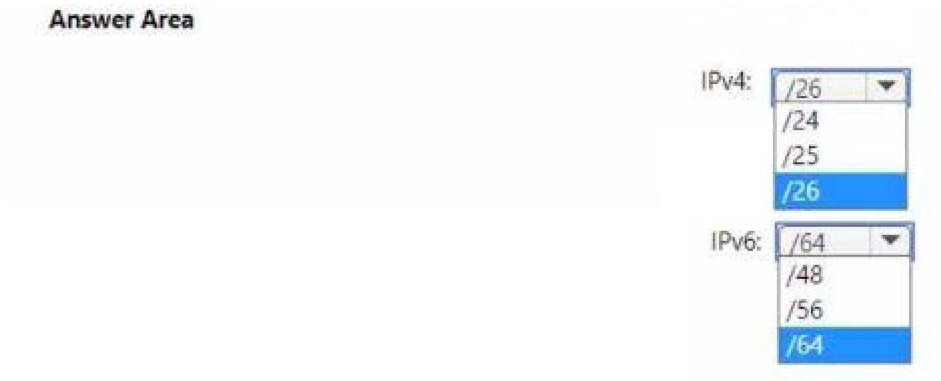
* Maximize the number of usable IP addresses.

* Support the deployment of the VPN gateway and the virtual machines.

Which subnet mask should you use for each address space? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

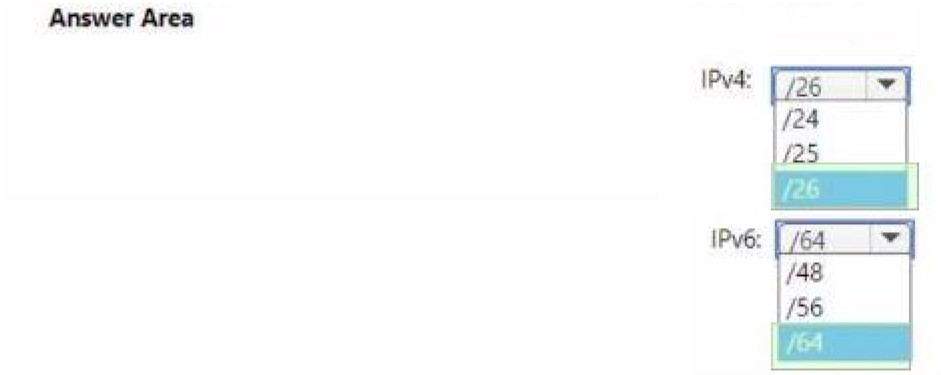


Answer Area

IPv4: /26
- /24
- /25
- /26

IPv6: /64
- /48
- /56
- /64

Answer Area:



Answer Area

IPv4: /26

/24

/25

/26

IPv6: /64

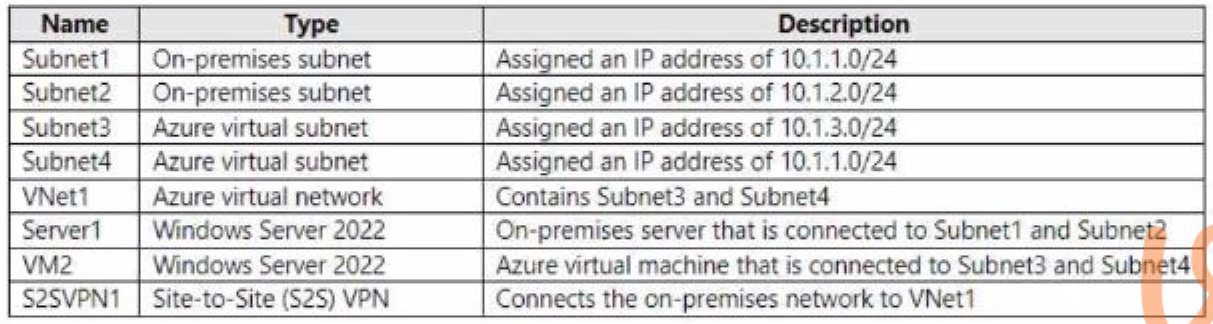
/48

/56

/64

Section:
Explanation:

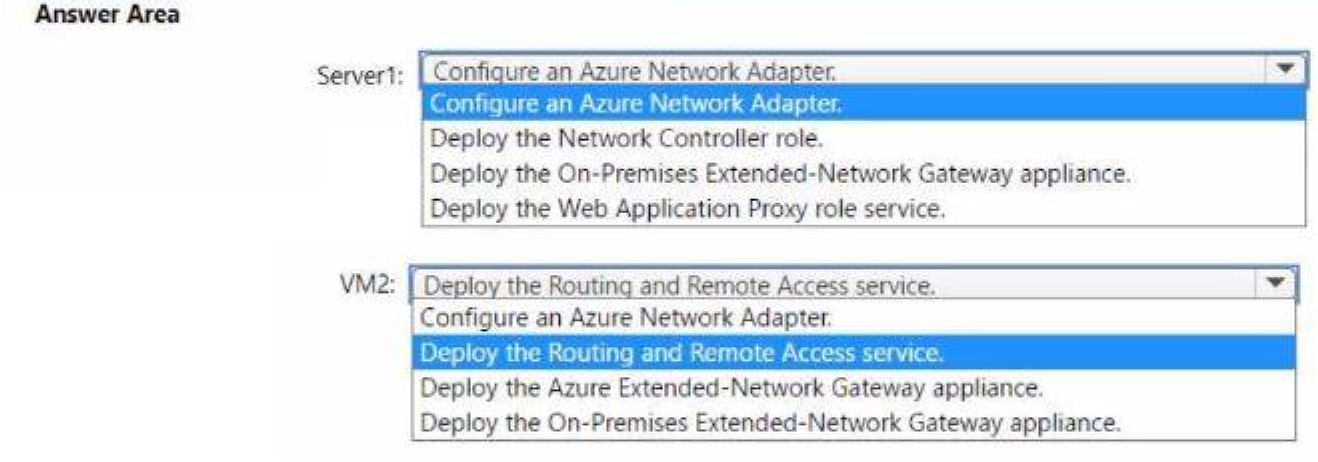
QUESTION 100
HOTSPOT
You have an on-premises network.
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
Subnet1	On-premises subnet	Assigned an IP address of 10.1.1.0/24
Subnet2	On-premises subnet	Assigned an IP address of 10.1.2.0/24
Subnet3	Azure virtual subnet	Assigned an IP address of 10.1.3.0/24
Subnet4	Azure virtual subnet	Assigned an IP address of 10.1.1.0/24
VNet1	Azure virtual network	Contains Subnet3 and Subnet4
Server1	Windows Server 2022	On-premises server that is connected to Subnet1 and Subnet2
VM2	Windows Server 2022	Azure virtual machine that is connected to Subnet3 and Subnet4
S2SVPN1	Site-to-Site (S2S) VPN	Connects the on-premises network to VNet1

You need to ensure that on-premises devices can communicate with Azure resources that are connected to Subnet4.
What should you do on each resource? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Server1: Configure an Azure Network Adapter.

Configure an Azure Network Adapter.

Deploy the Network Controller role.

Deploy the On-Premises Extended-Network Gateway appliance.

Deploy the Web Application Proxy role service.

VM2: Deploy the Routing and Remote Access service.

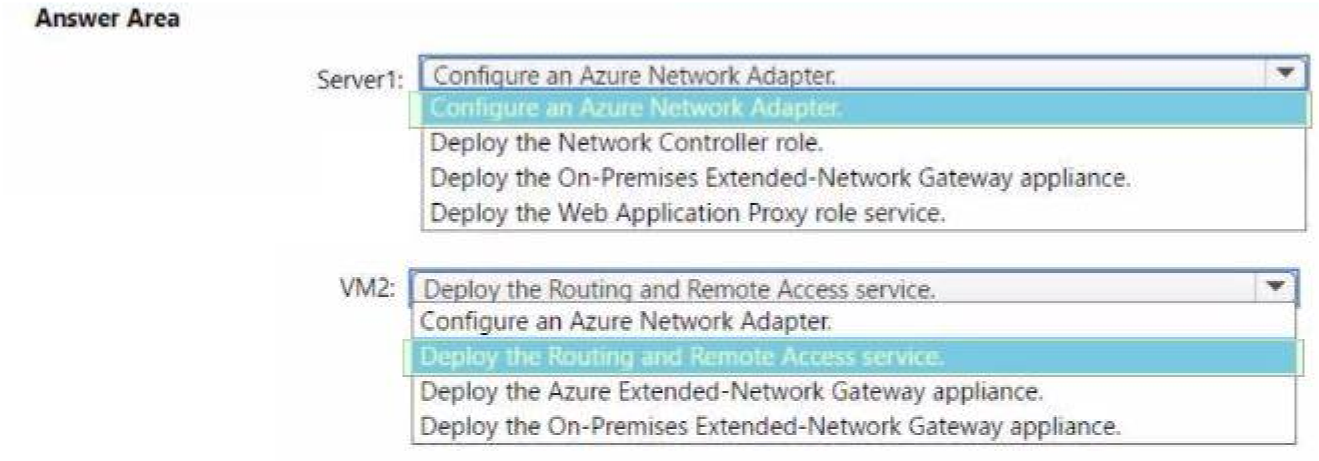
Configure an Azure Network Adapter.

Deploy the Routing and Remote Access service.

Deploy the Azure Extended-Network Gateway appliance.

Deploy the On-Premises Extended-Network Gateway appliance.

Answer Area:



Answer Area

Server1: Configure an Azure Network Adapter.

- Configure an Azure Network Adapter.
- Deploy the Network Controller role.
- Deploy the On-Premises Extended-Network Gateway appliance.
- Deploy the Web Application Proxy role service.

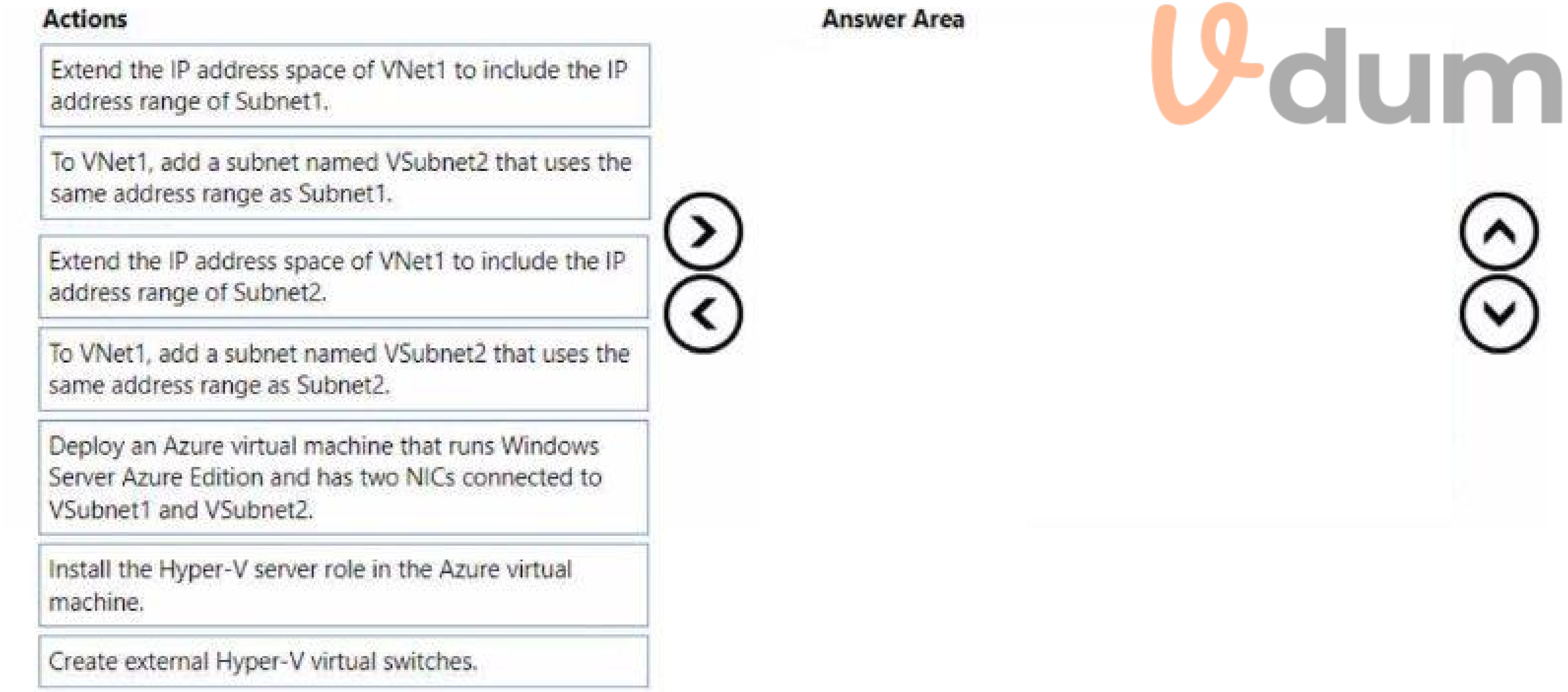
VM2: Deploy the Routing and Remote Access service.

- Configure an Azure Network Adapter.
- Deploy the Routing and Remote Access service.
- Deploy the Azure Extended-Network Gateway appliance.
- Deploy the On-Premises Extended-Network Gateway appliance.

Section:
Explanation:

QUESTION 101
DRAG DROP
Your on-premises network contains two subnets named Subnet1 and Subnet2. Subnet2 contains a Hyper-V host that contains two virtual machines named VM1 and VM2. VM1 and VM2 are connected to Subnet2.
You have an Azure virtual network named VNet1 that contains GatewaySubnet and a subnet named VSubnet1. VNet1 is connected to the on-premises network by using a Site-to-Site (S2S) VPN connection.
You plan to migrate VM1 to VNet1 and maintain the existing IP address of VM1. VM2 will remain on Subnet2.
You need to prepare the environment to ensure that VM1 can communicate with VM2 once the migration is complete.
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.'

Select and Place:

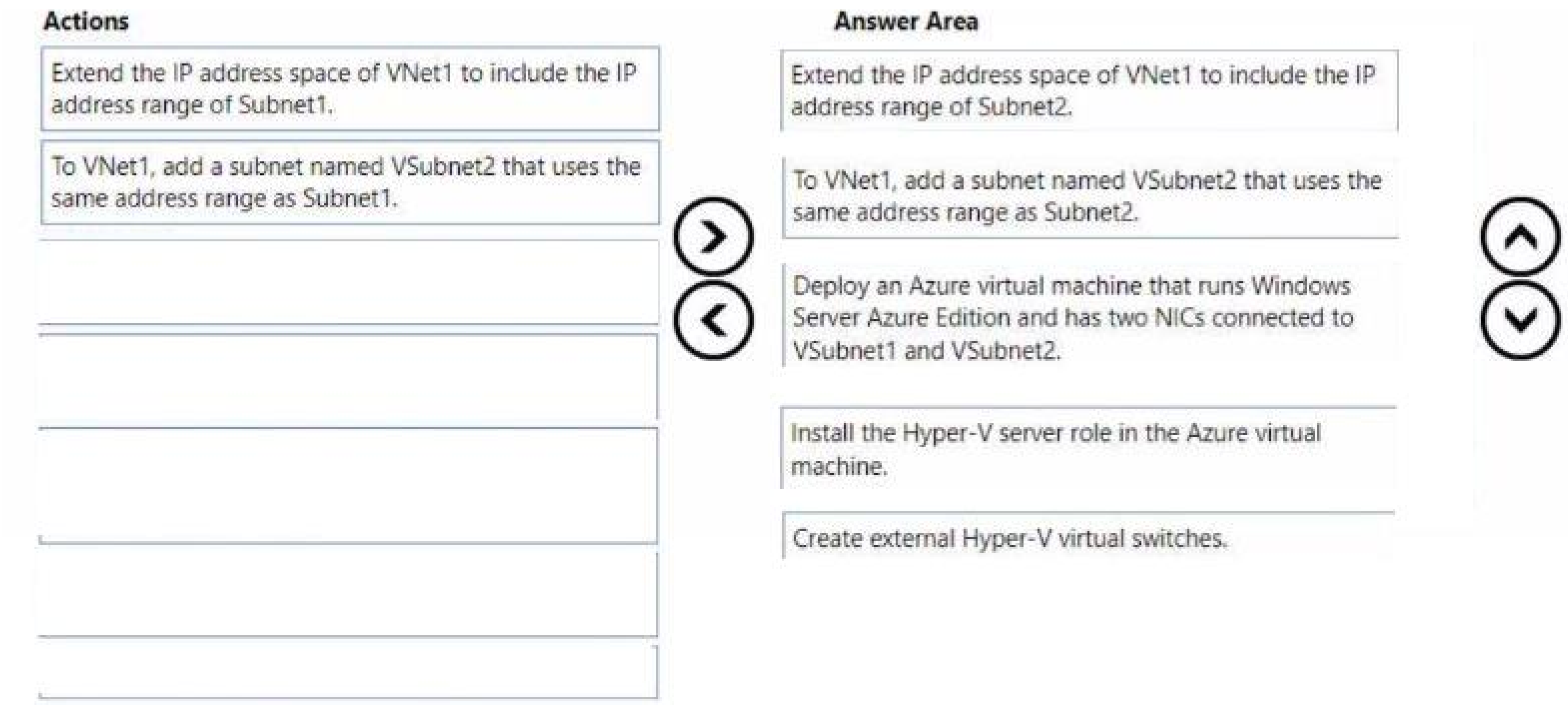


Actions

- Extend the IP address space of VNet1 to include the IP address range of Subnet1.
- To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet1.
- Extend the IP address space of VNet1 to include the IP address range of Subnet2.
- To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2.
- Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2.
- Install the Hyper-V server role in the Azure virtual machine.
- Create external Hyper-V virtual switches.

Answer Area

Correct Answer:



Actions

Extend the IP address space of VNet1 to include the IP address range of Subnet1.

To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet1.

Answer Area

Extend the IP address space of VNet1 to include the IP address range of Subnet2.

To VNet1, add a subnet named VSubnet2 that uses the same address range as Subnet2.

Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnet1 and VSubnet2.

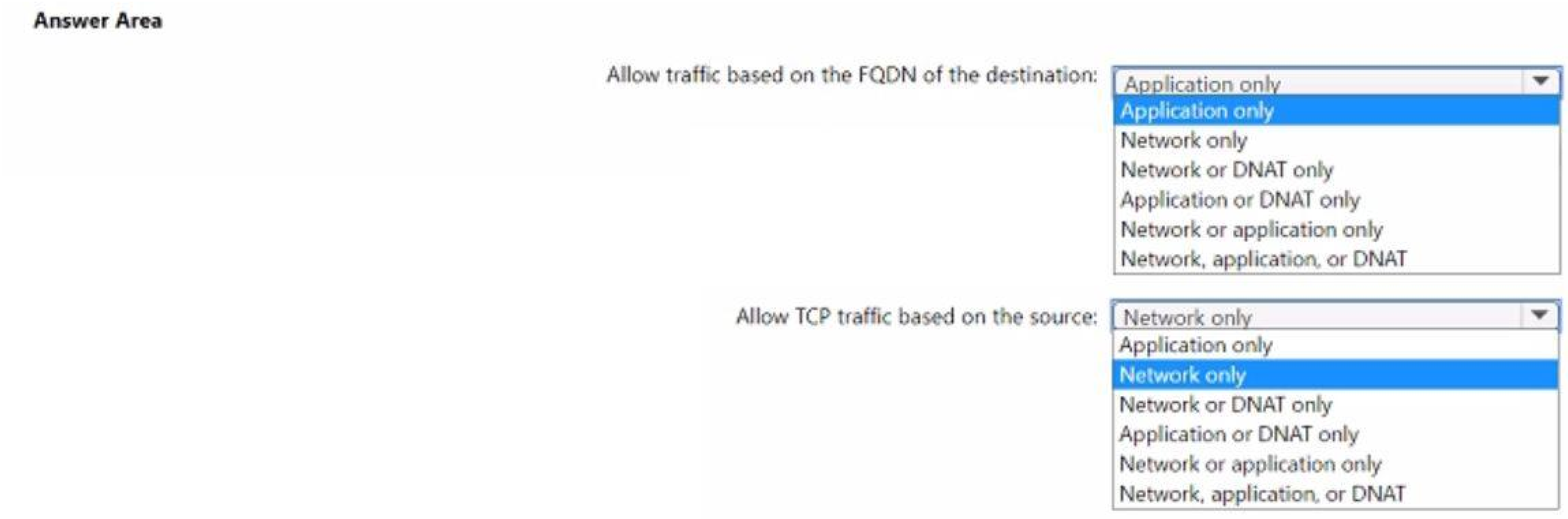
Install the Hyper-V server role in the Azure virtual machine.

Create external Hyper-V virtual switches.

Section:
Explanation:
Extend the IP address space of VNet1 to include the IP address range of Subnet2.
To VNet1, add a subnet named VSubnet2...
Deploy an Azure virtual machine that runs Windows...
Install the Hyper-V server role in the Azure virutual machine.
Create external Hyper-V virtual switches.

QUESTION 102
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

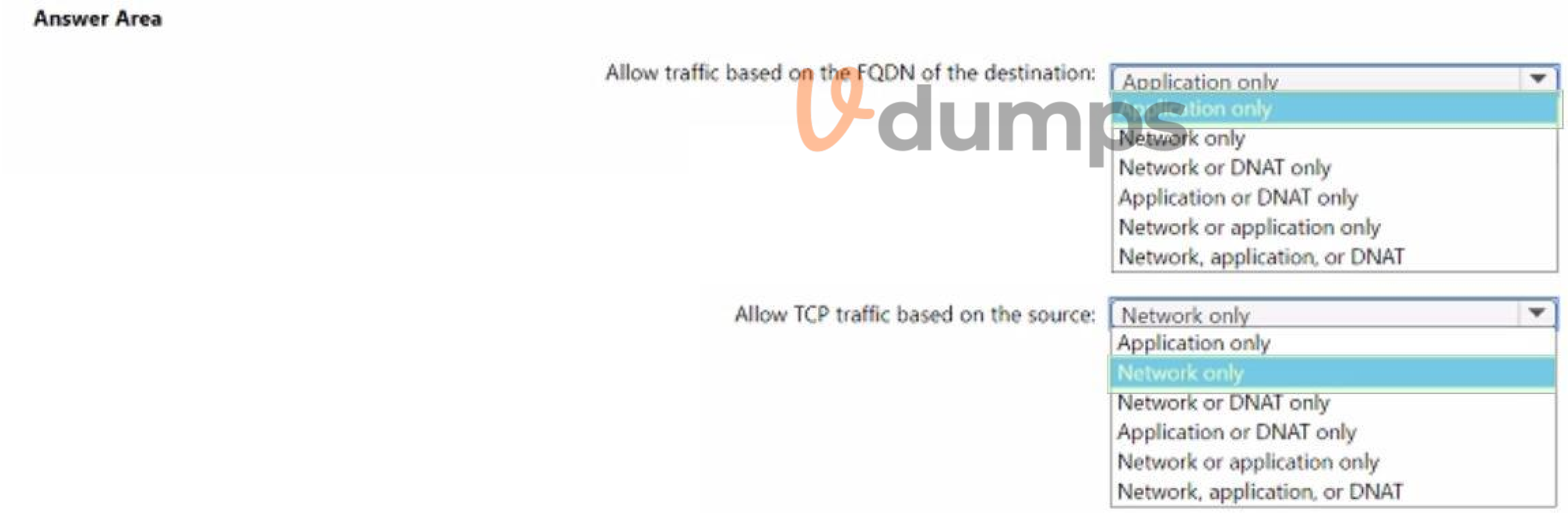
Allow traffic based on the FQDN of the destination: Application only

- 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: Network only

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

Answer Area:



Answer Area

Allow traffic based on the FQDN of the destination: Application only

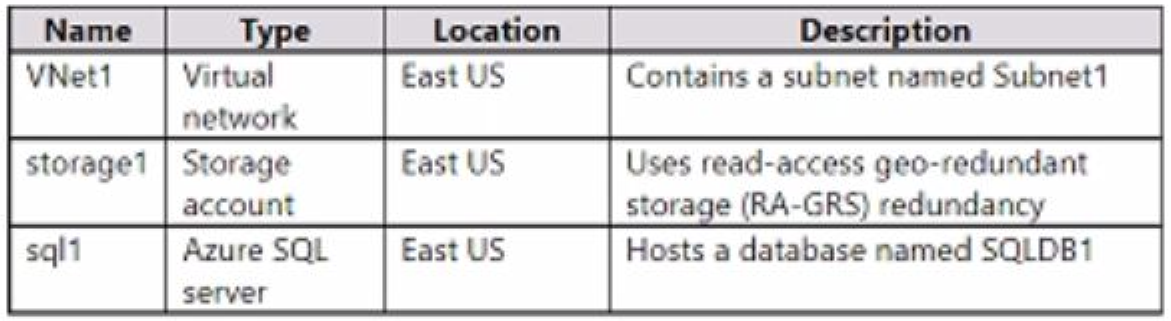
- [✓ Application only]
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Allow TCP traffic based on the source: Network only

- Application only
- [✓ Network only]
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Section:
Explanation:

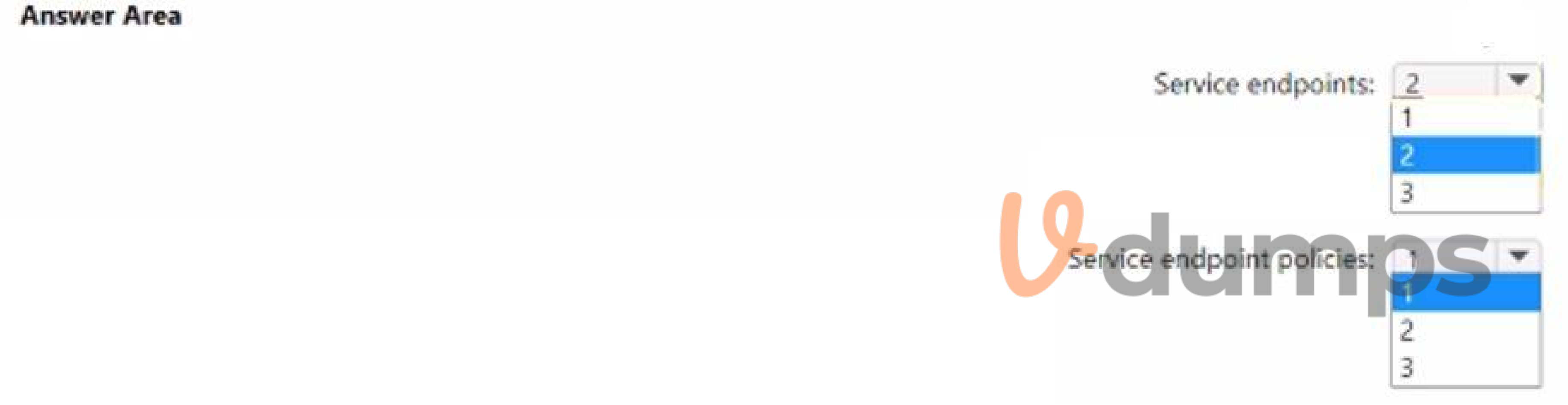
QUESTION 103
HOTSPOT
You have art Azure subscription that contains the resources shown in the following table.



Name	Type	Location	Description
VNet1	Virtual network	East US	Contains a subnet named Subnet1
storage1	Storage account	East US	Uses read-access geo-redundant storage (RA-GRS) redundancy
sql1	Azure SQL server	East US	Hosts a database named SQLDB1

You need to restrict access to storage1 and sql1 by using service endpoints. The solution must meet the following requirements:
* Allow access from Subnet1 to SQIDB1
* Implement service endpoint policies to restrict access to supported resources.
* Allow access from Subnet1 to storage1 and the read-only replica of storage1 in the paired Azure region.
What is the minimum number of service endpoints and service endpoint policies you should create? To answer, select the appropriate options m the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

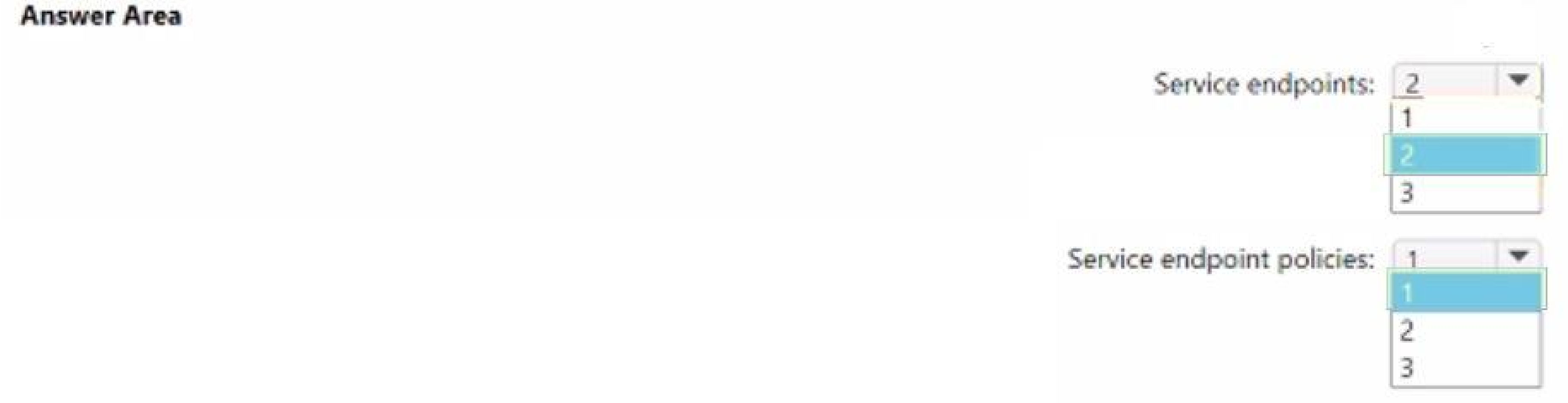


Answer Area

Service endpoints: 2

Service endpoint policies: 1

Answer Area:



Answer Area

Service endpoints: 2

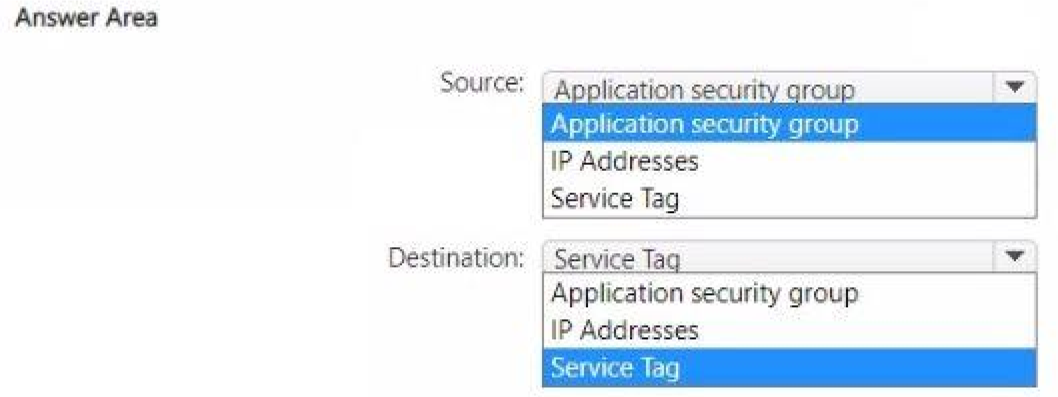
Service endpoint policies: 1

Section:
Explanation:

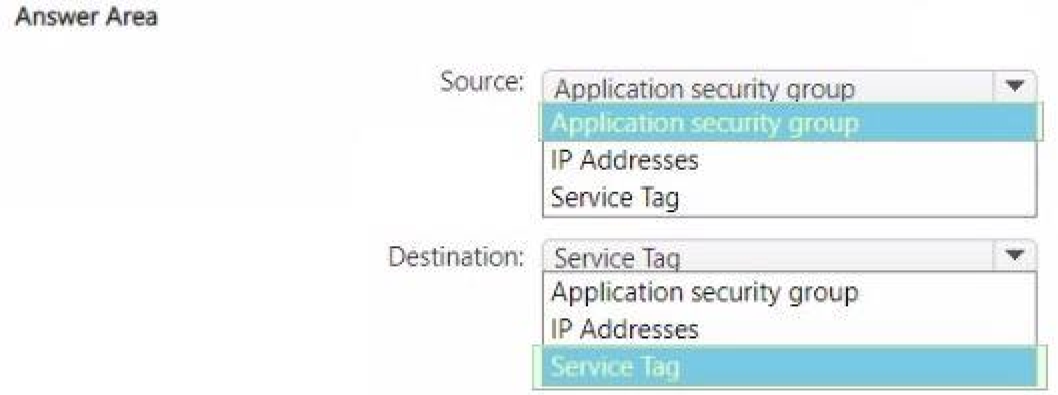
QUESTION 104
HOTSPOT
You have an Azure subscription. The subscription contains multiple Azure SQL Database resources and a virtual network named VNet1 that has five subnets. All the subnets are associated with a network security group (NSG)

named NSG1. NSG1 blocks all outbound traffic, unless specifically allowed by a rule.
Each subnet contains 50 virtual machines. Multiple virtual machines host instances of SQL Server on Virtual Machines and will be configured to replicate with the Azure SQL Database resources.
You need to configure a new outbound rule in NSG1 to allow the SQL Server on Virtual Machines instances to connect to the Azure SQL Database resources. The solution must meet the following requirements:
* Minimize modifications to NSG1 when additional instances of SQL Server on Virtual Machines are deployed.
* Ensure that only SQL Server on Virtual Machines instances can connect to the Azure SQL Database resources.
How should you configure each setting for the new outbound rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



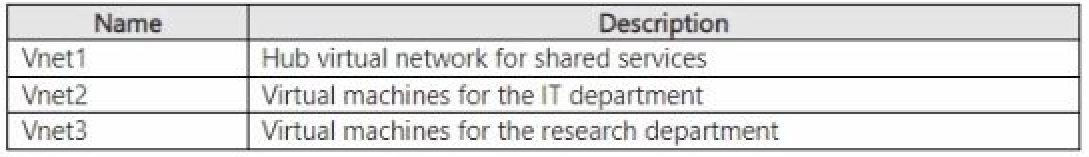
Section:
Explanation:

QUESTION 105
You have an Azure subscription that contains 100 network security groups (NSGs).
You need to ensure that you log the application of specific NSG rules.
Which type of log should you configure?

A. flow log
B. activity log
C. Azure resource log
D. audit log

Correct Answer: A
Section:

QUESTION 106
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. service endpoints

B. route tables

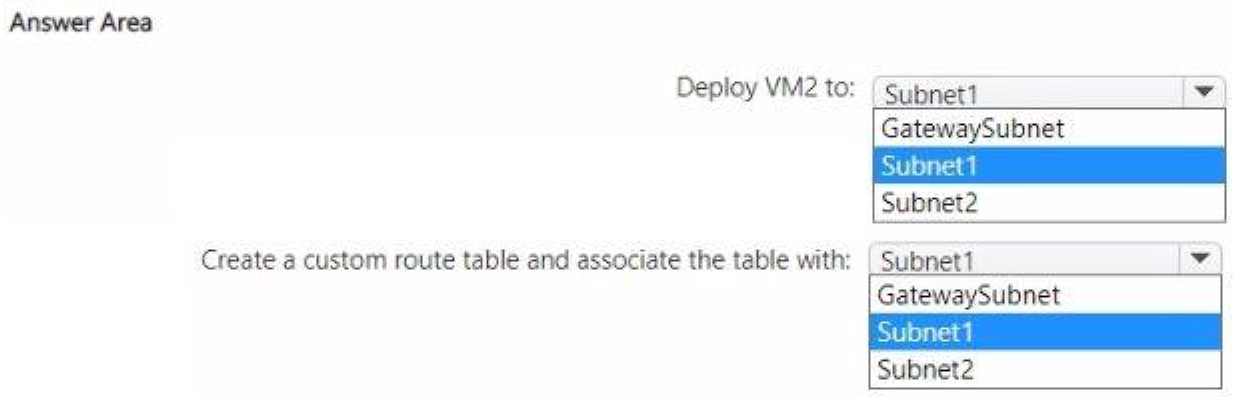
C. VNet-to-VNet VPN connections

D. peering

Correct Answer: D
Section:

QUESTION 107
HOTSPOT
You have an Azure subscription that contains a virtual machine named VM1 and a virtual network named Vnet1. Vnet1 contains three subnets named Subnet1, Subnet2 and GatewaySubnet. VM1 is connected to Subnet 1.
You plan to deploy a new virtual machine named VM2 that will perform network traffic routing and inspection.
You need to ensure that all the traffic from VM1 to the internet will be routed through VM2.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

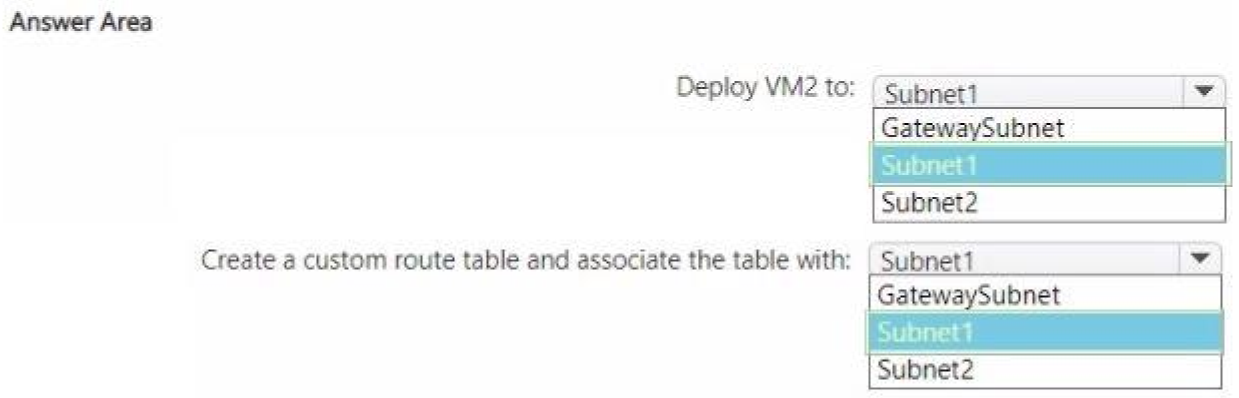


Answer Area

Deploy VM2 to: Subnet1
GatewaySubnet
Subnet1
Subnet2

Create a custom route table and associate the table with: Subnet1
GatewaySubnet
Subnet1
Subnet2

Answer Area:



Answer Area

Deploy VM2 to: Subnet1
GatewaySubnet
[✓ Subnet1]
Subnet2

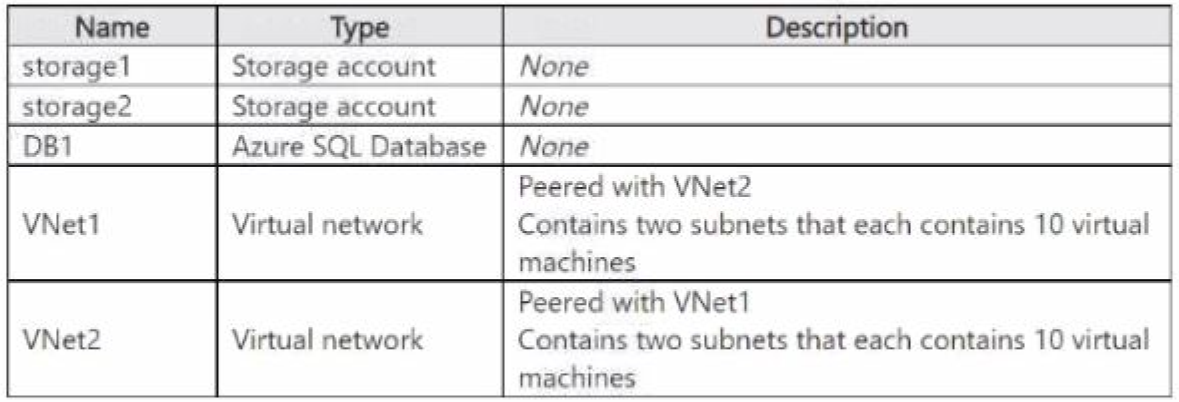
Create a custom route table and associate the table with: Subnet1
GatewaySubnet
[✓ Subnet1]
Subnet2

Section:

Explanation:

QUESTION 108

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



Name	Type	Description
storage1	Storage account	*None*
storage2	Storage account	*None*
DB1	Azure SQL Database	*None*
VNet1	Virtual network	Peered with VNet2 Contains two subnets that each contains 10 virtual machines
VNet2	Virtual network	Peered with VNet1 Contains two subnets that each contains 10 virtual machines

You need to ensure that the virtual machines can access storage1, storage2, and DB1 by using service endpoints.
What is the minimum number of service endpoints you should create?

A. 2

B. 3

C. 4

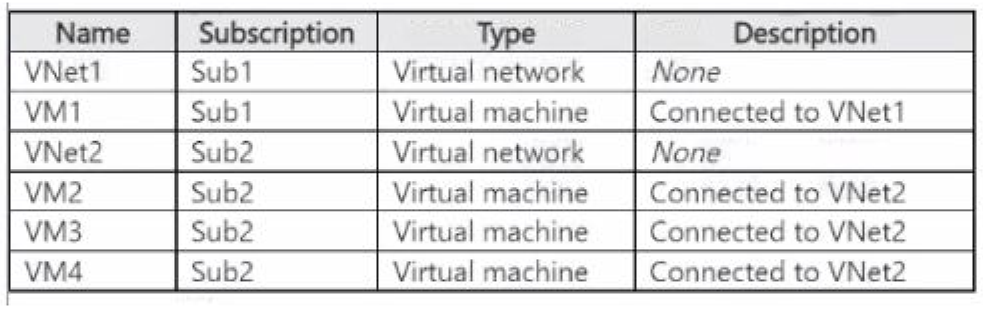
D. 12

Correct Answer: B
Section:

QUESTION 109

DRAG DROP

You have two Azure subscriptions named Sub1 and Sub2 that contain the resources shown in the following table.



Name	Subscription	Type	Description
VNet1	Sub1	Virtual network	*None*
VM1	Sub1	Virtual machine	Connected to VNet1
VNet2	Sub2	Virtual network	*None*
VM2	Sub2	Virtual machine	Connected to VNet2
VM3	Sub2	Virtual machine	Connected to VNet2
VM4	Sub2	Virtual machine	Connected to VNet2

VNet1 and VNet2 are NOT connected.

You plan to create an Azure Private Link service named Link1 that will be used to connect VNet1 and VNet2. You need to ensure that Link1 meets the following requirements:

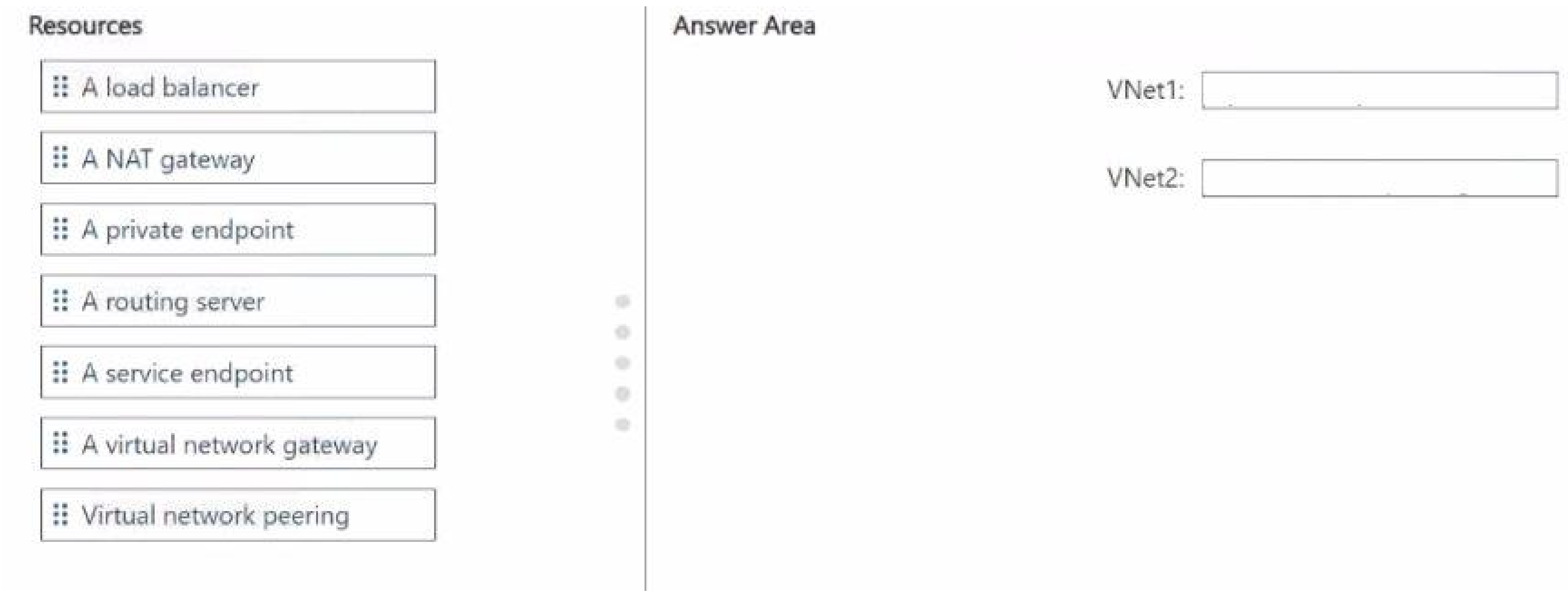
* Ensures that VM1 can connect only to a web app hosted on VM2

* Prevents VM1 from connecting to the other resources that are connected to VNet2

Which additional resources should you create for each virtual network? To answer, drag the appropriate resources to the correct virtual networks. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Resources

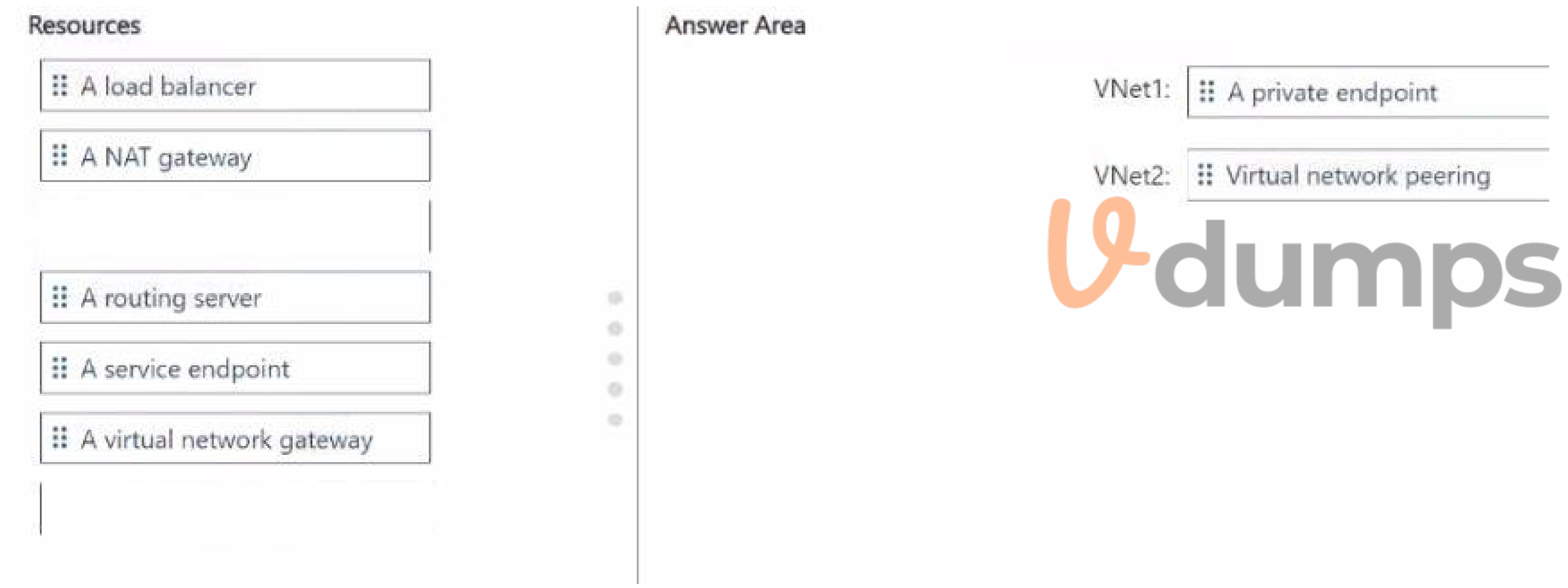
- A load balancer
- A NAT gateway
- A private endpoint
- A routing server
- A service endpoint
- A virtual network gateway
- Virtual network peering

Answer Area

VNet1:

VNet2:

Correct Answer:



Resources

- A load balancer
- A NAT gateway
- A routing server
- A service endpoint
- A virtual network gateway

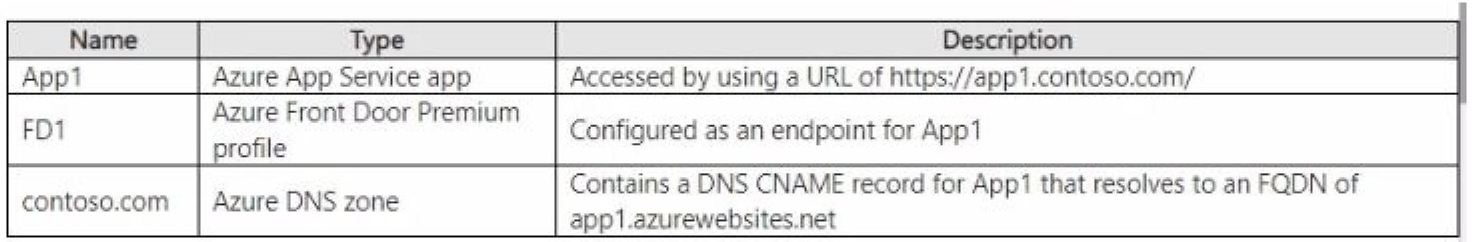
Answer Area

VNet1: A private endpoint

VNet2: Virtual network peering

Section:
Explanation:

QUESTION 110
DRAG DROP
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
App1	Azure App Service app	Accessed by using a URL of https://app1.contoso.com/
FD1	Azure Front Door Premium profile	Configured as an endpoint for App1
contoso.com	Azure DNS zone	Contains a DNS CNAME record for App1 that resolves to an FQDN of app1.azurewebsites.net

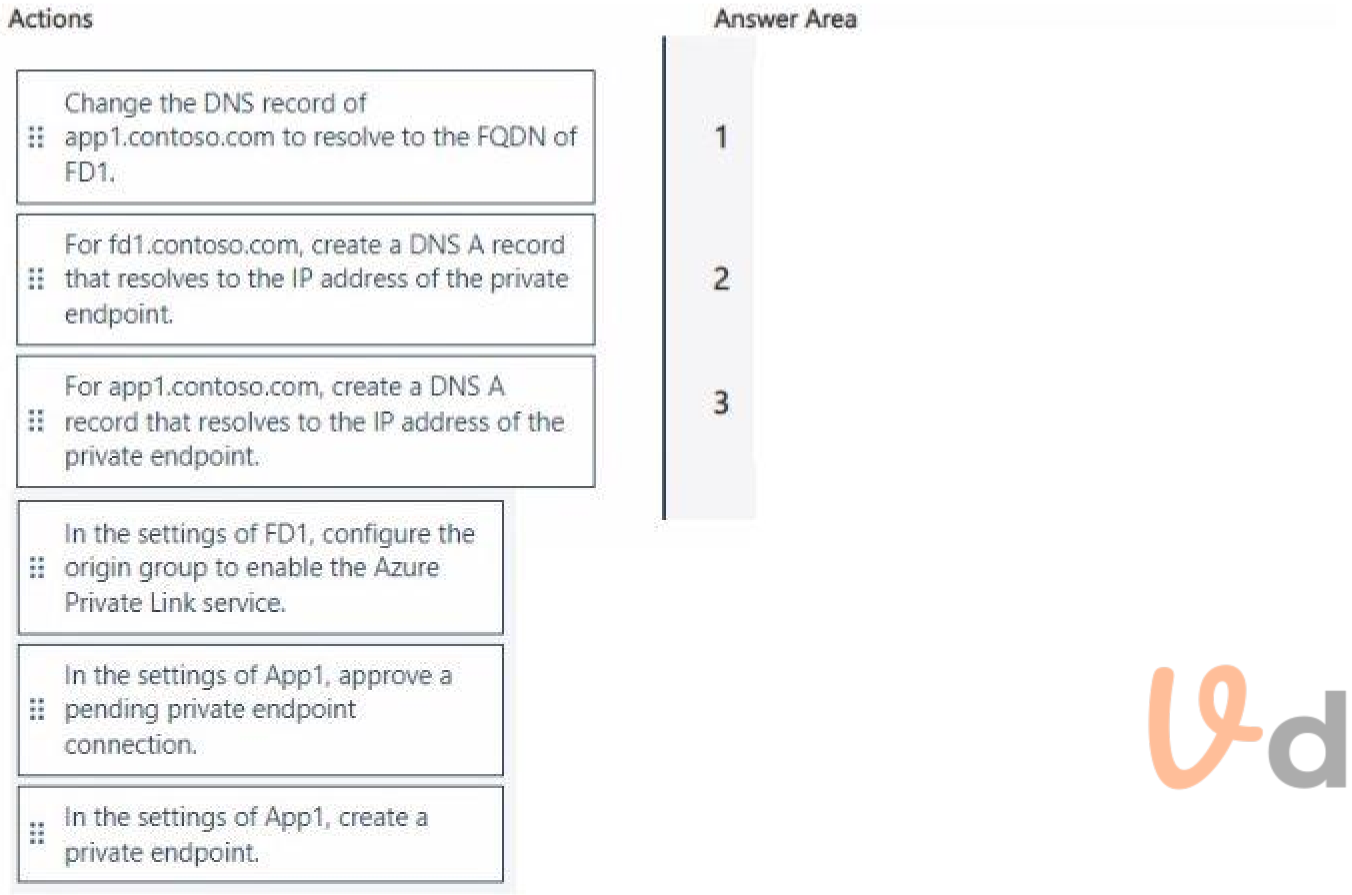
You discover that users connect directly to App1.
You need to meet The following requirements:
* Administrators must only access App1 by using a private endpoint.

* All user connections to App1 must be routed through FD1.
* The downtime of connections to App1 must be minimized.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Select and Place:



Actions

- Change the DNS record of app1.contoso.com to resolve to the FQDN of FD1.
- For fd1.contoso.com, create a DNS A record that resolves to the IP address of the private endpoint.
- For app1.contoso.com, create a DNS A record that resolves to the IP address of the private endpoint.
- In the settings of FD1, configure the origin group to enable the Azure Private Link service.
- In the settings of App1, approve a pending private endpoint connection.
- In the settings of App1, create a private endpoint.

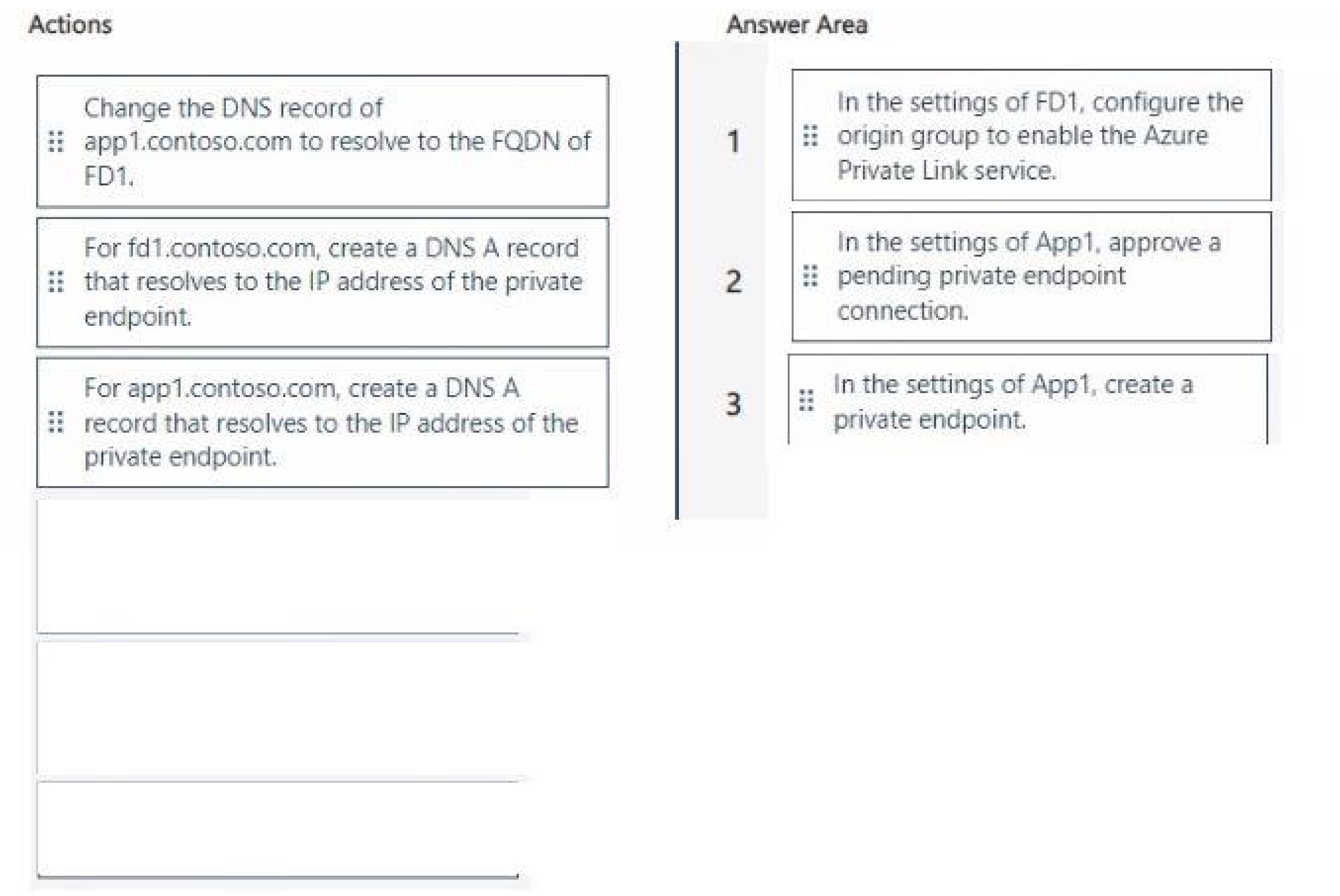
Answer Area

1

2

3

Correct Answer:



Actions

- Change the DNS record of app1.contoso.com to resolve to the FQDN of FD1.
- For fd1.contoso.com, create a DNS A record that resolves to the IP address of the private endpoint.
- For app1.contoso.com, create a DNS A record that resolves to the IP address of the private endpoint.

Answer Area

1 In the settings of FD1, configure the origin group to enable the Azure Private Link service.

2 In the settings of App1, approve a pending private endpoint connection.

3 In the settings of App1, create a private endpoint.

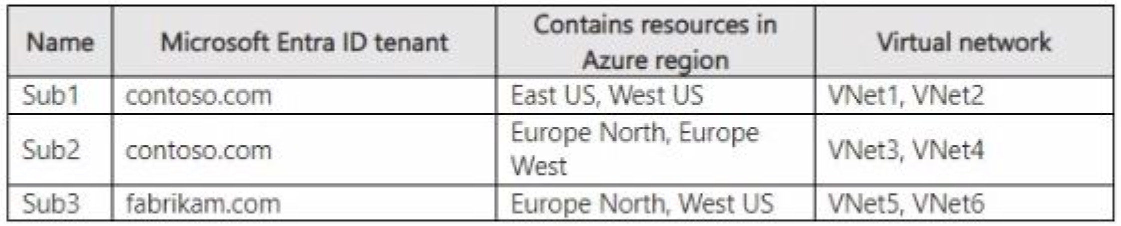
Section:
Explanation:

QUESTION 111
You have an instance of Azure Web Application Firewall (WAF) on Azure Front Door.
You plan to create a WAF rule that will block high rates of requests from a single IP address.
You need to query Log Analytics to identify the optimal threshold for the rule.
Which table should you query in Log Analytics?

A. AZFWThreatlnte1
B. AzureDiagnostics
C. SecurityDetection
D. AGWFirewallLogs

Correct Answer: B
Section:

QUESTION 112
You have the Azure subscriptions shown in the following table.



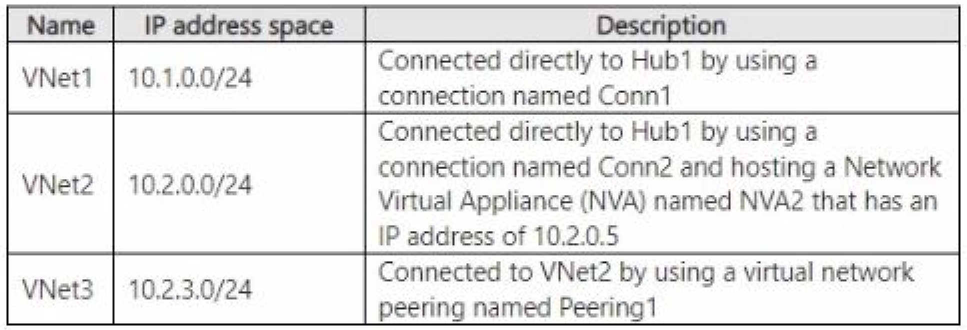
Name	Microsoft Entra ID tenant	Contains resources in Azure region	Virtual network
Sub1	contoso.com	East US, West US	VNet1, VNet2
Sub2	contoso.com	Europe North, Europe West	VNet3, VNet4
Sub3	fabrikam.com	Europe North, West US	VNet5, VNet6

Each virtual network contains 20 internet-accessible resources that are assigned public IP addresses.
You need to implement Azure DDoS Network Protection to protect the resources. The solution must minimize costs.
What is the minimum number of DDoS Network Protection plans you should deploy?

A. 1
B. 2
C. 3
D. 6

Correct Answer: B
Section:

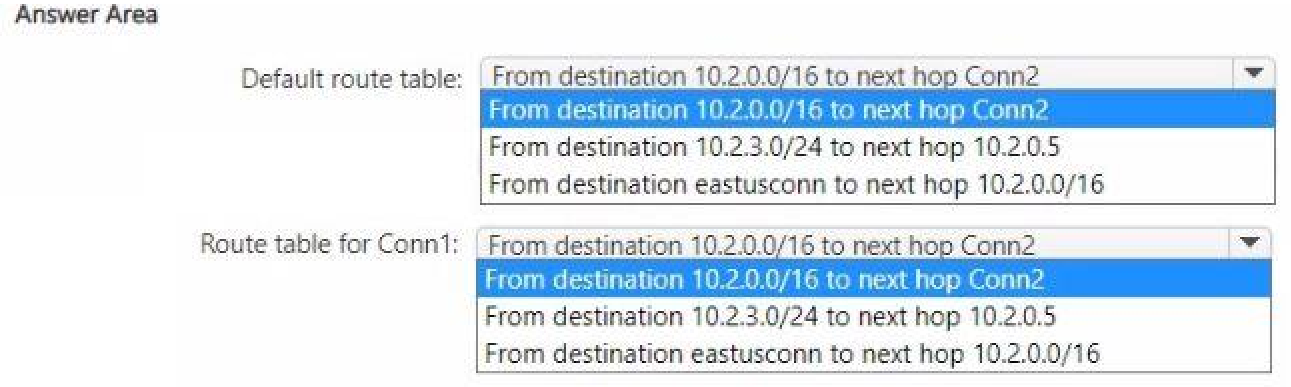
QUESTION 113
HOTSPOT
You plan to implement an Azure Virtual WAN named VWAN1 that will contain a hub named Hub1. VWAN1 will include the virtual networks shown in the following table.



Name	IP address space	Description
VNet1	10.1.0.0/24	Connected directly to Hub1 by using a connection named Conn1
VNet2	10.2.0.0/24	Connected directly to Hub1 by using a connection named Conn2 and hosting a Network Virtual Appliance (NVA) named NVA2 that has an IP address of 10.2.0.5
VNet3	10.2.3.0/24	Connected to VNet2 by using a virtual network peering named Peering1

You need to ensure that hosts connected to VNet1 can communicate with hosts connected to VNet3.
How should you configure the routing tables for VWAN1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

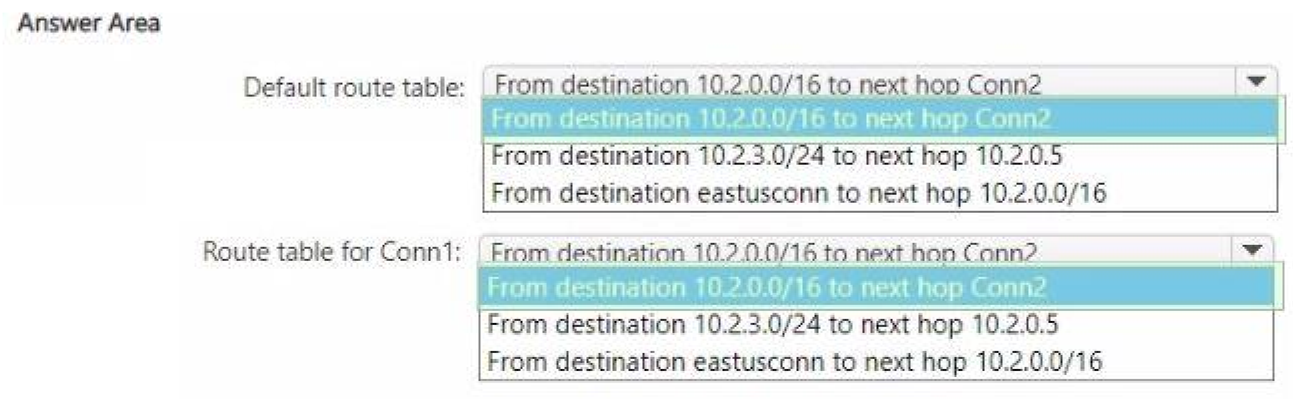


Answer Area

Default route table: From destination 10.2.0.0/16 to next hop Conn2
- From destination 10.2.0.0/16 to next hop Conn2
- From destination 10.2.3.0/24 to next hop 10.2.0.5
- From destination eastusconn to next hop 10.2.0.0/16

Route table for Conn1: From destination 10.2.0.0/16 to next hop Conn2
- From destination 10.2.0.0/16 to next hop Conn2
- From destination 10.2.3.0/24 to next hop 10.2.0.5
- From destination eastusconn to next hop 10.2.0.0/16

Answer Area:



Answer Area

Default route table: From destination 10.2.0.0/16 to next hop Conn2

[✓ From destination 10.2.0.0/16 to next hop Conn2]

From destination 10.2.3.0/24 to next hop 10.2.0.5

From destination eastusconn to next hop 10.2.0.0/16

Route table for Conn1: From destination 10.2.0.0/16 to next hop Conn2

[✓ From destination 10.2.0.0/16 to next hop Conn2]

From destination 10.2.3.0/24 to next hop 10.2.0.5

From destination eastusconn to next hop 10.2.0.0/16

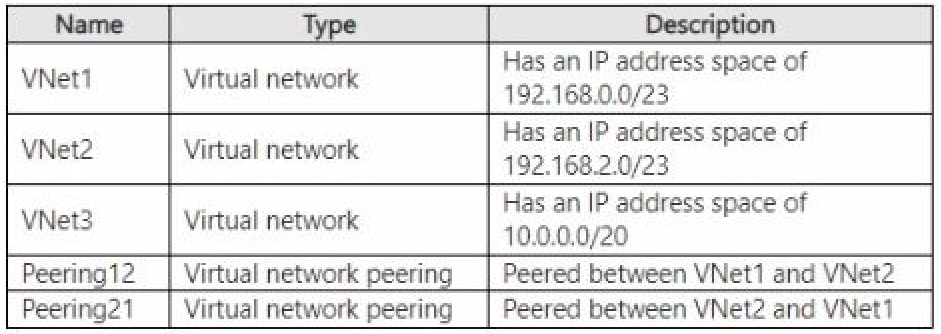
Section:

Explanation:

QUESTION 114

HOTSPOT

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



Name	Type	Description
VNet1	Virtual network	Has an IP address space of 192.168.0.0/23
VNet2	Virtual network	Has an IP address space of 192.168.2.0/23
VNet3	Virtual network	Has an IP address space of 10.0.0.0/20
Peering12	Virtual network peering	Peered between VNet1 and VNet2
Peering21	Virtual network peering	Peered between VNet2 and VNet1

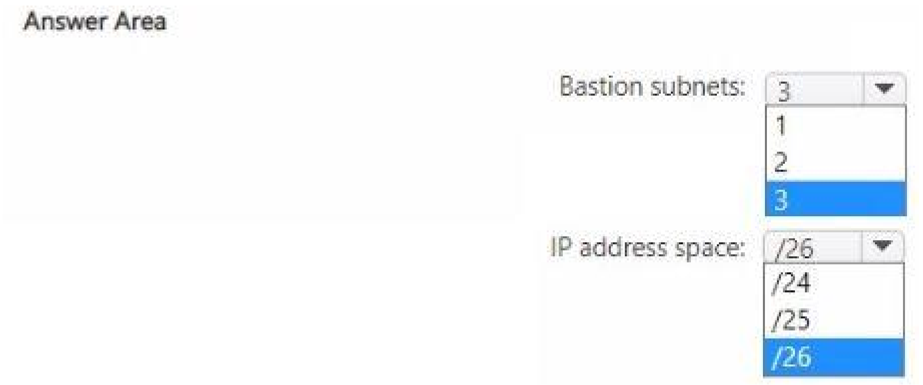
Each virtual network contains 20 virtual machines and a subnet that has an IP address space of /24.

You need to ensure that you can access the virtual machines from the internet by using Azure Bastion.

What is the minimum number of bastion subnets you should deploy, and what is the smallest supported IP address space for each bastion subnet? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Bastion subnets: 3

1

2

[✓ 3]

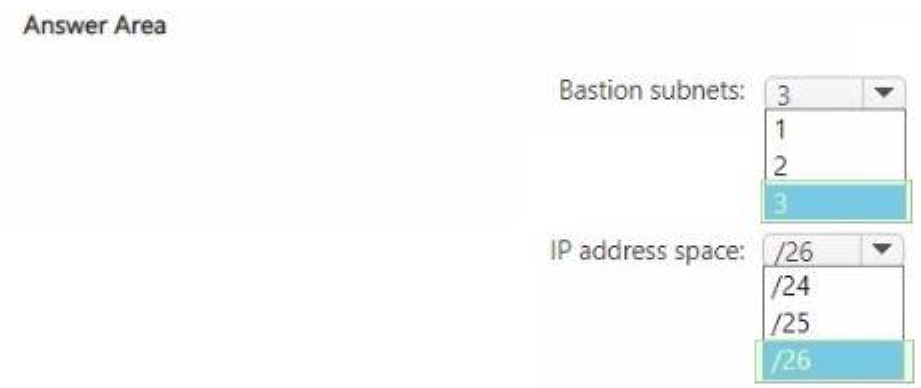
IP address space: /26

/24

/25

[✓ /26]

Answer Area:



Answer Area

Bastion subnets: 3

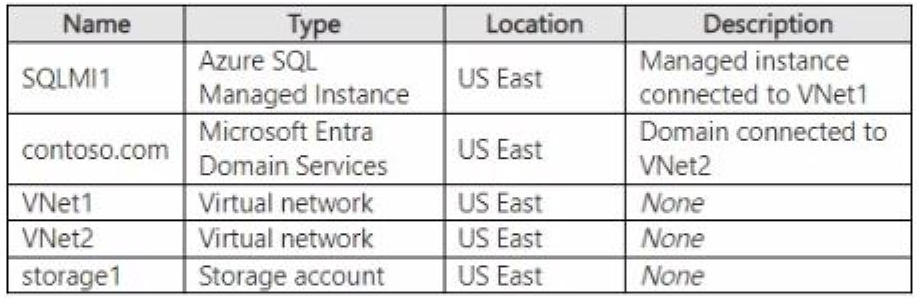
- 1
- 2
- 3

IP address space: /26

- /24
- /25
- /26

Section:
Explanation:

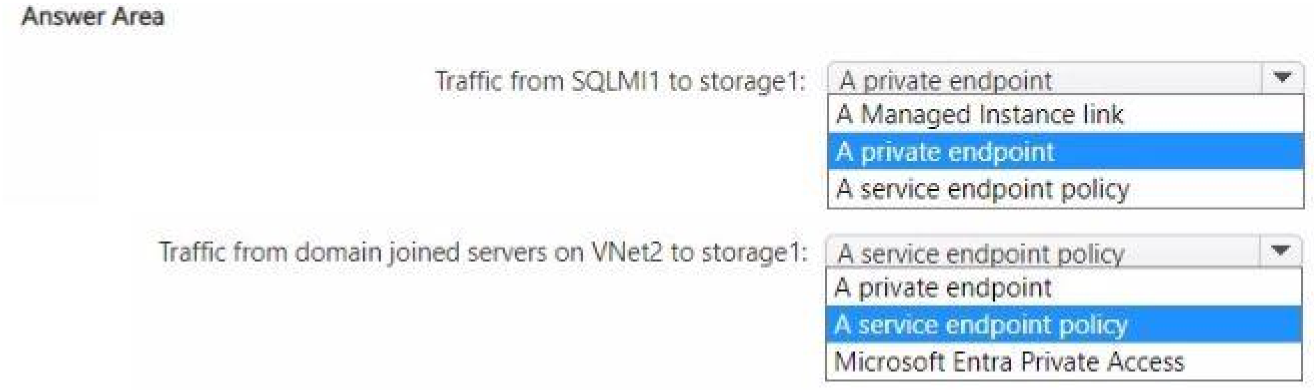
QUESTION 115
OTSPOT
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Location	Description
SQLMI1	Azure SQL Managed Instance	US East	Managed instance connected to VNet1
contoso.com	Microsoft Entra Domain Services	US East	Domain connected to VNet2
VNet1	Virtual network	US East	*None*
VNet2	Virtual network	US East	*None*
storage1	Storage account	US East	*None*

You need to ensure that network traffic is routed over the Azure backbone network for the following scenarios:
* Traffic from SQIMI1 to storage1
* Traffic from domain joined servers on VNet2 to storage1
The solution must minimize costs.
What should you configure for each scenario? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

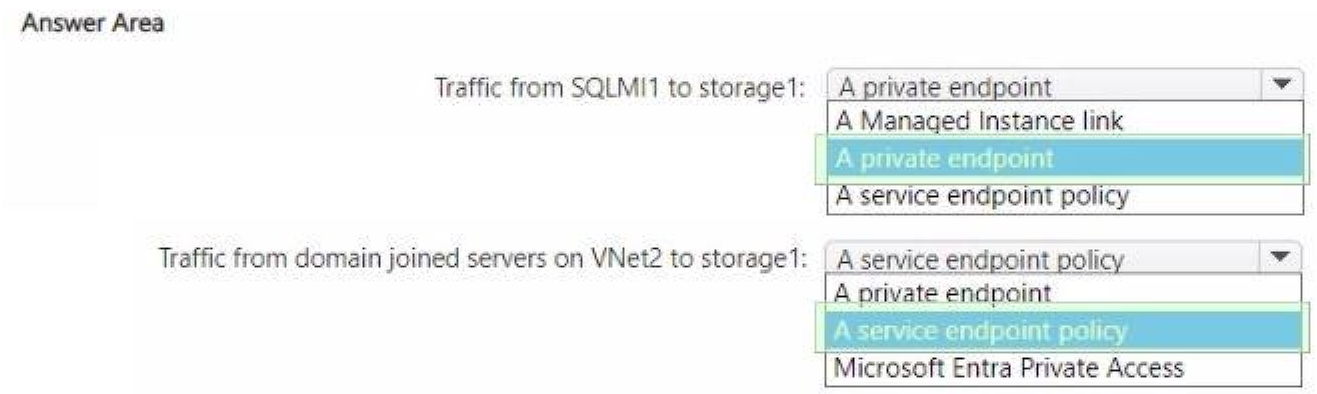
Traffic from SQLMI1 to storage1: A private endpoint

- A Managed Instance link
- A private endpoint
- A service endpoint policy

Traffic from domain joined servers on VNet2 to storage1: A service endpoint policy

- A private endpoint
- A service endpoint policy
- Microsoft Entra Private Access

Answer Area:



Answer Area

Traffic from SQLMI1 to storage1: A private endpoint

- A Managed Instance link
- A private endpoint
- A service endpoint policy

Traffic from domain joined servers on VNet2 to storage1: A service endpoint policy

- A private endpoint
- A service endpoint policy
- Microsoft Entra Private Access

Section:
Explanation:

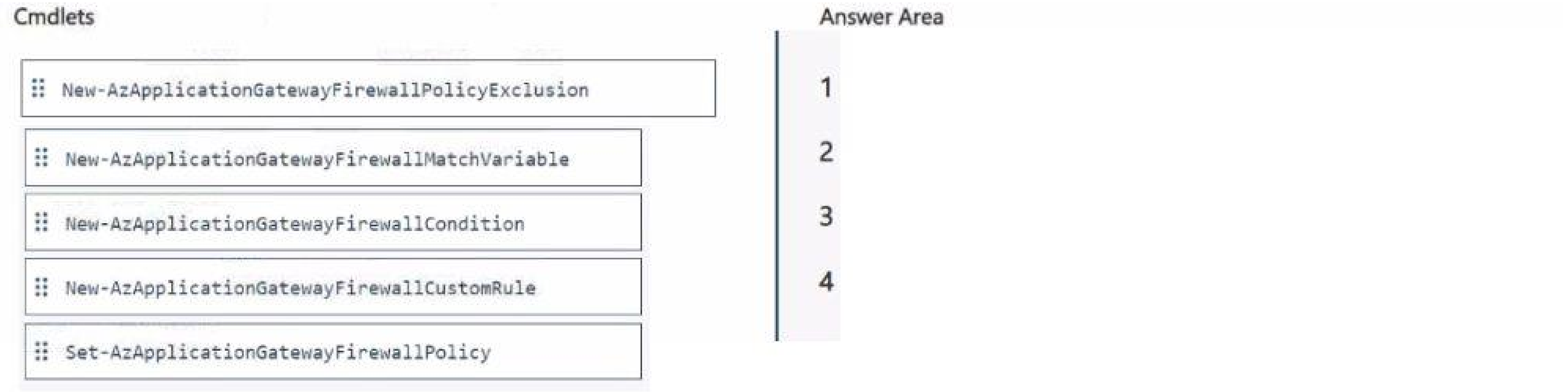
QUESTION 116
You have an on-premises network named Site1.
You have an Azure subscription that contains a storage account named storage1 and a virtual network named VNet1. VNet1 contains a subnet named Subnet1. A private endpoint for storage1 is connected to Subnet1 Site1 is connected to VNet1 by using a Site-to-Site (S2S) VPN.
You need to control access to storage1 from Site1 by using network security groups (NSGs).
What should you do first?

A. Associate a route table with Subnet1.
B. Associate a NAT gateway with Subnet1.
C. Configure a network policy for private endpoints on Subnet1.
D. Create a subnet delegation on Subnet1.

Correct Answer: A
Section:

QUESTION 117
DRAG DROP
You have an Azure Web Application Firewall (WAF) v2 tier named AG1 on an Azure application gateway. AG1 has a policy named Policy 1.
You need to add a custom rule to Policy 1. The rule must block all requests from IP addresses in a specific IP address range.
Which four PowerShell cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Select and Place:



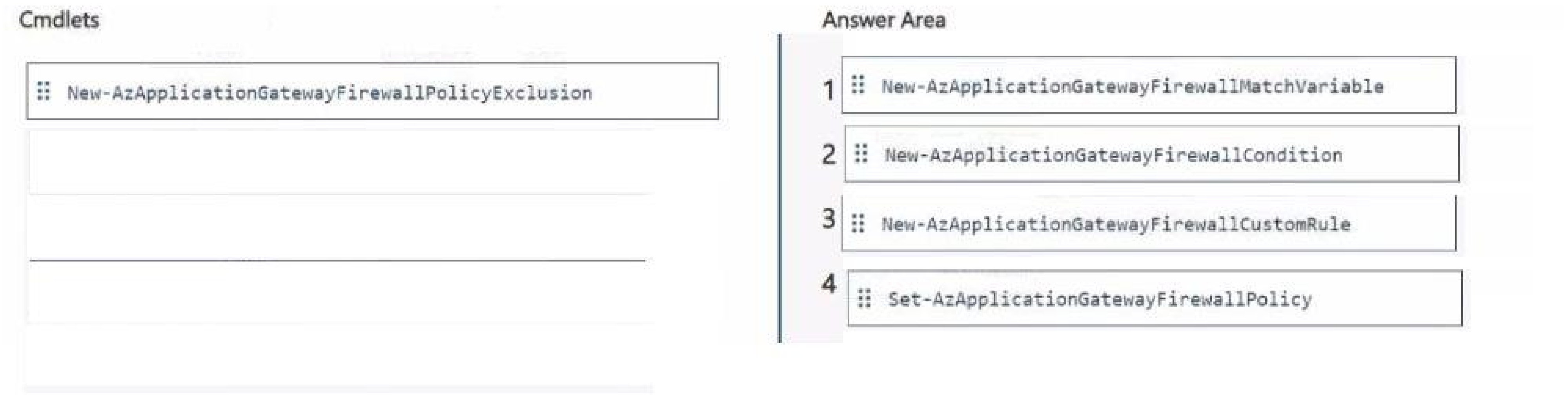
Cmdlets

- New-AzApplicationGatewayFirewallPolicyExclusion
- New-AzApplicationGatewayFirewallMatchVariable
- New-AzApplicationGatewayFirewallCondition
- New-AzApplicationGatewayFirewallCustomRule
- Set-AzApplicationGatewayFirewallPolicy

Answer Area

1
2
3
4

Correct Answer:



Cmdlets

- New-AzApplicationGatewayFirewallPolicyExclusion

Answer Area

1. New-AzApplicationGatewayFirewallMatchVariable
2. New-AzApplicationGatewayFirewallCondition
3. New-AzApplicationGatewayFirewallCustomRule
4. Set-AzApplicationGatewayFirewallPolicy

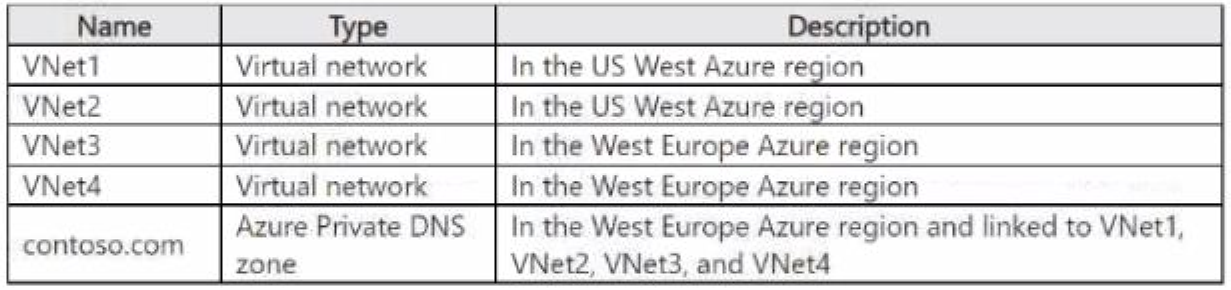
Section:
Explanation:

QUESTION 118
You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFW1. You plan to enable the following:
* TLS inspection
* Threat intelligence
* A network intrusion detection and prevention system (IDPS)
What can you enable by using AzFW1?

A. TLS inspection only
B. threat intelligence only
C. TLS inspection and the IDPS only
D. threat intelligence and the IDPS only
E. TLS inspection, threat intelligence, and the IDPS

Correct Answer: E
Section:

QUESTION 119
You have an on-premises DNS server named Server1 that hosts a primary DNS zone named fabrikam.com.
You have an Azure subscription that contains the resources shown in the following table.



Name	Type	Description
VNet1	Virtual network	In the US West Azure region
VNet2	Virtual network	In the US West Azure region
VNet3	Virtual network	In the West Europe Azure region
VNet4	Virtual network	In the West Europe Azure region
contoso.com	Azure Private DNS zone	In the West Europe Azure region and linked to VNet1, VNet2, VNet3, and VNet4

Users on the on-premises network access resources on all the virtual networks by using a Site-to-Site (S2S) VPN. You need to deploy an Azure DNS Private Resolver solution that meets the following requirements:
* Resources connected to the virtual networks must be able to resolve DNS names for fabrikam.com.
* Server1 must be able to resolve the DNS names of the resources in contoso.com.
* The solution must minimize costs and administrative effort.
What is the minimum number of resolvers you should deploy?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B
Section:

QUESTION 120

HOTSPOT

You have two Azure subscriptions.

You need to perform the following actions in the East US Azure region of each subscription:

* Deploy 50 virtual machines to availability zone 1.

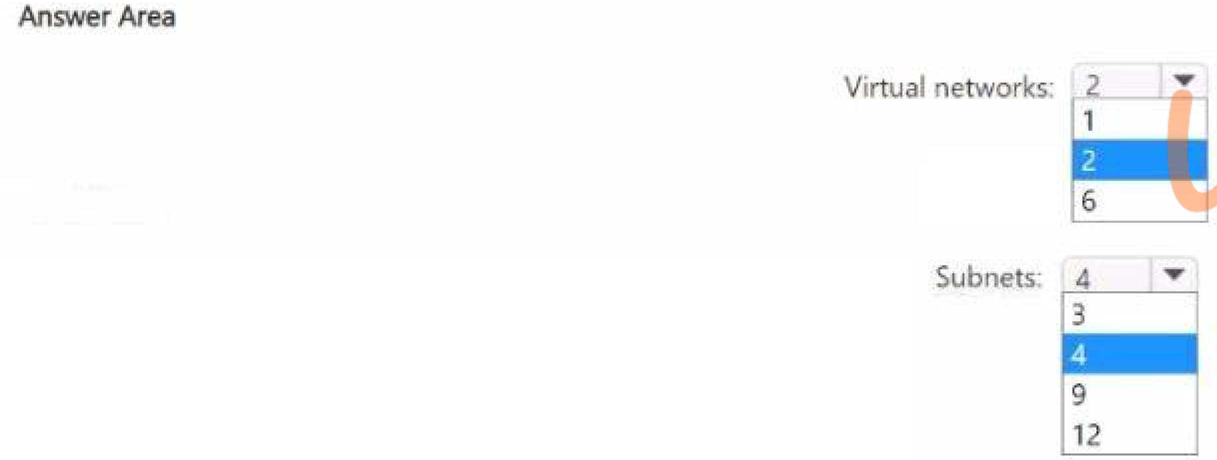
* Deploy 50 virtual machines to availability zone 2.

* Deploy 50 virtual machines to availability zone 3.

What is the minimum number of virtual networks and /25 subnets you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

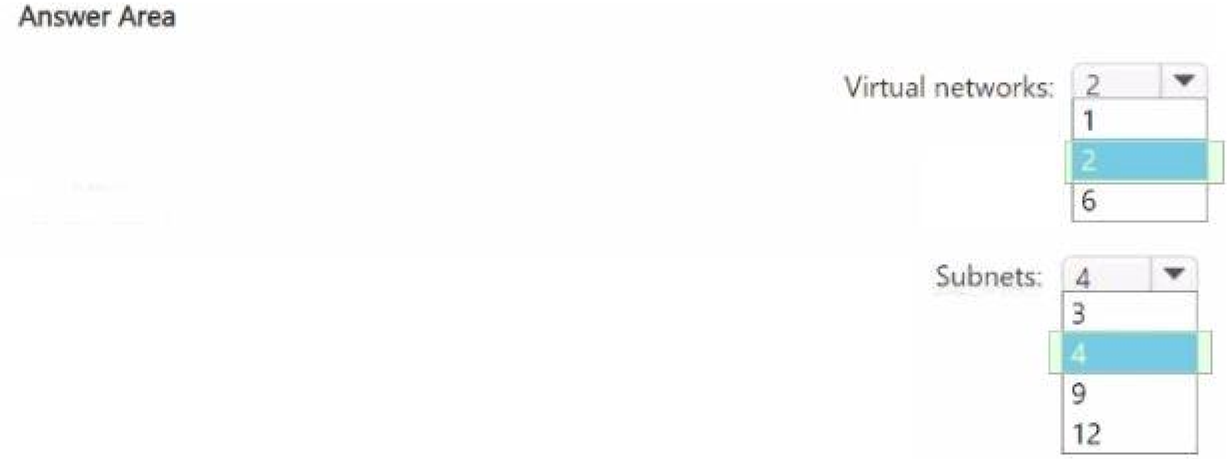


Answer Area

Virtual networks: 2 ▾
- 1
- 2
- 6

Subnets: 4 ▾
- 3
- 4
- 9
- 12

Answer Area:



Answer Area

Virtual networks: 2 ▾
- 1
- [✓ 2]
- 6

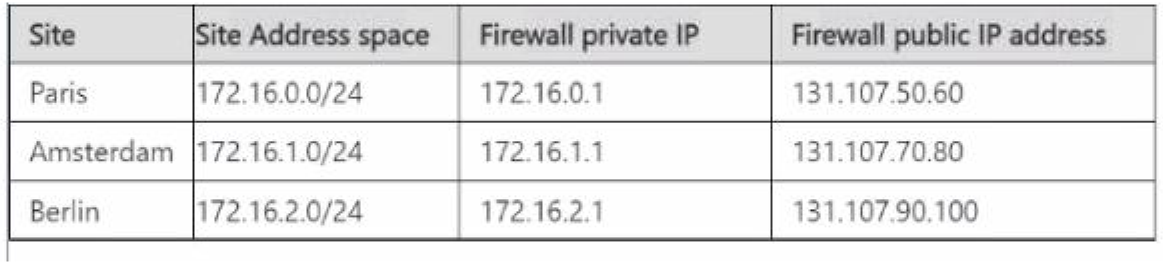
Subnets: 4 ▾
- 3
- [✓ 4]
- 9
- 12

Section:
Explanation:

QUESTION 121

HOTSPOT

You have an on-premises network that includes the sites shown in the following table.

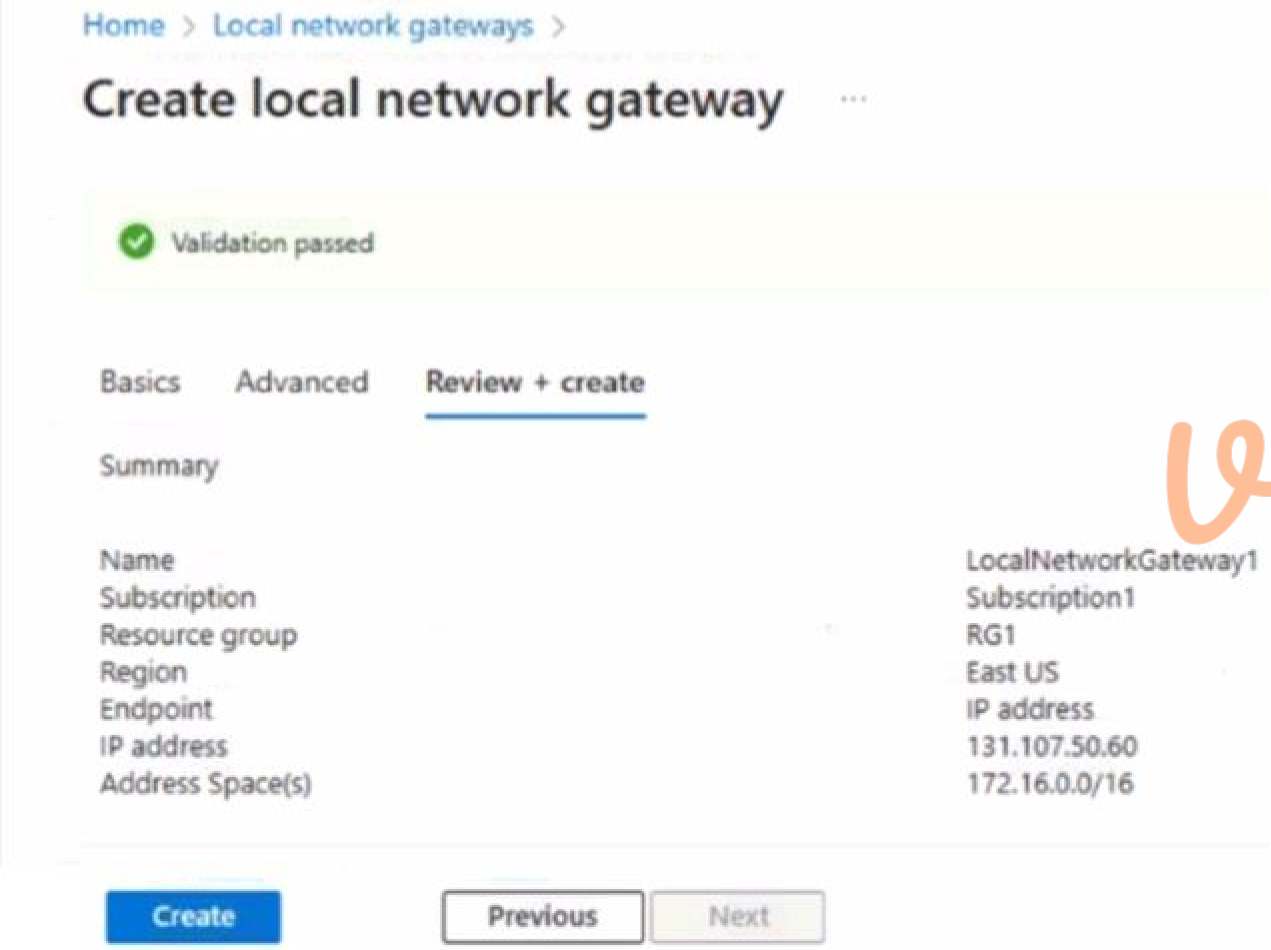


Site	Site Address space	Firewall private IP	Firewall public IP address
Paris	172.16.0.0/24	172.16.0.1	131.107.50.60
Amsterdam	172.16.1.0/24	172.16.1.1	131.107.70.80
Berlin	172.16.2.0/24	172.16.2.1	131.107.90.100

Each site is connected to the Internet by a firewall. All sites are connected to an SD-WAN. Each site is configured to propagate routes by using BGP.

You have an Azure subscription that includes a virtual network named Vnet1 that contains a Virtual Network Gateway named Gateway 1.

You create a local network gateway with the configuration shown in the gateway exhibit (Click the Gateway tab.)



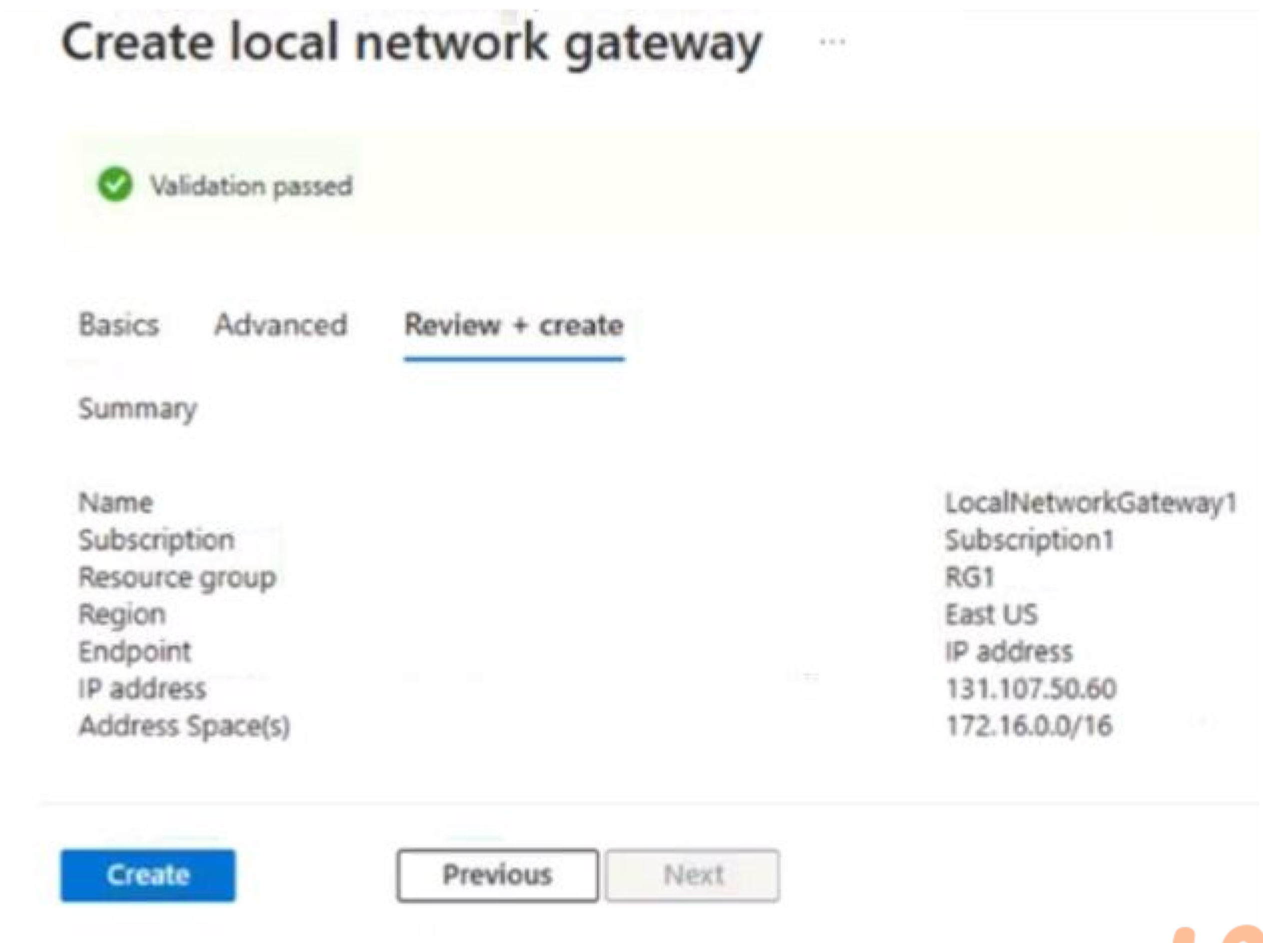
Create local network gateway

Validation passed

Summary

Name	LocalNetworkGateway1
Subscription	Subscription1
Resource group	RG1
Region	East US
Endpoint	IP address
IP address	131.107.50.60
Address Space(s)	172.16.0.0/16

You create a Site-to-Site (S2S) connection with the configuration shown in connection exhibit. (Click the Connection tab)



Create local network gateway ...

Validation passed

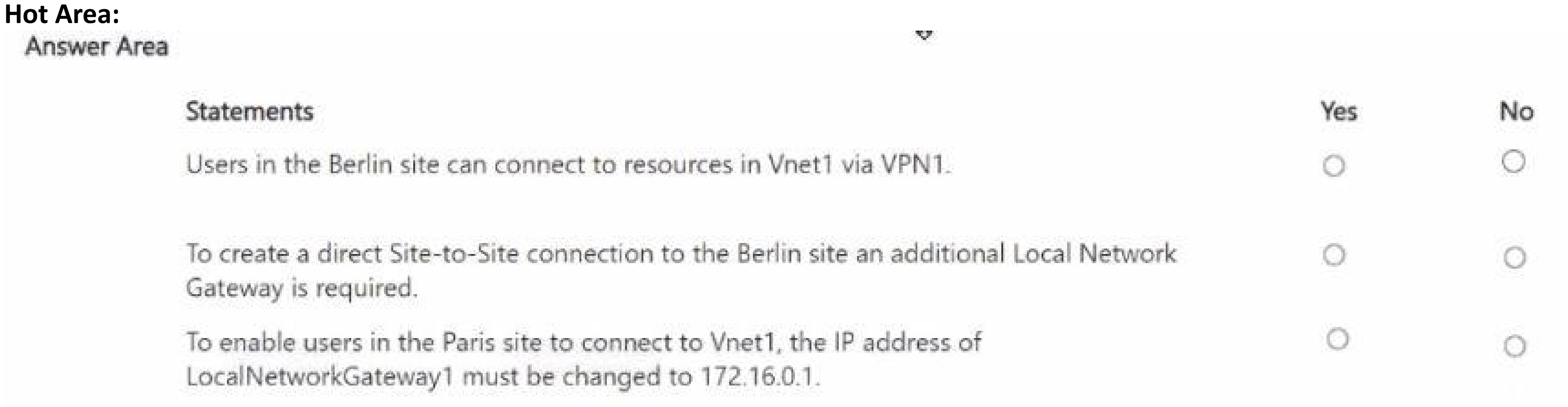
Basics Advanced Review + create

Summary

Name	LocalNetworkGateway1
Subscription	Subscription1
Resource group	RG1
Region	East US
Endpoint	IP address
IP address	131.107.50.60
Address Space(s)	172.16.0.0/16

For each of the following statements, select Yes if the statement is true Otherwise, select No.
NOTE: Each correct selection is worth one point.

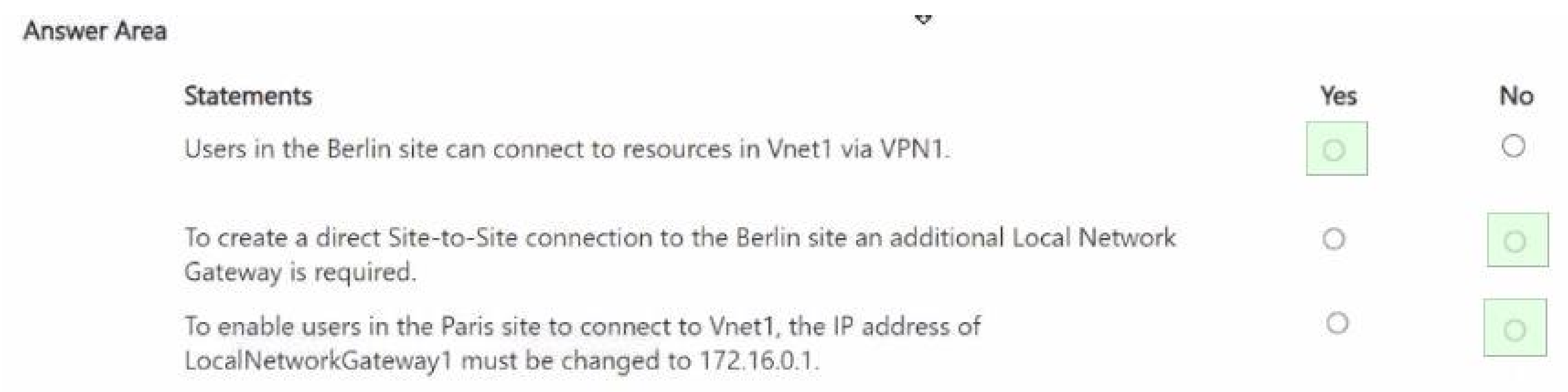
Hot Area:



Answer Area

Statements	Yes	No
Users in the Berlin site can connect to resources in Vnet1 via VPN1.	○	○
To create a direct Site-to-Site connection to the Berlin site an additional Local Network Gateway is required.	○	○
To enable users in the Paris site to connect to Vnet1, the IP address of LocalNetworkGateway1 must be changed to 172.16.0.1.	○	○

Answer Area:



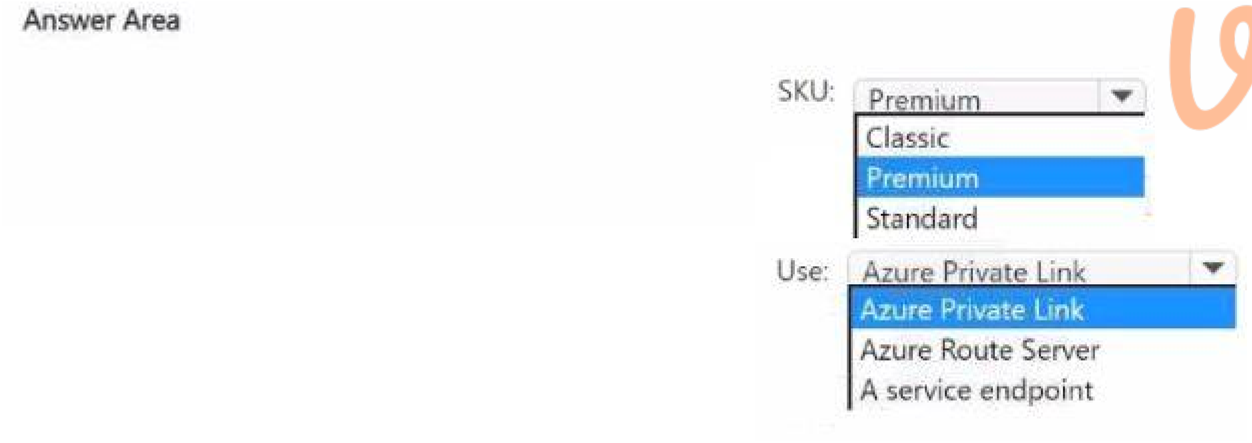
Answer Area

Statements	Yes	No
Users in the Berlin site can connect to resources in Vnet1 via VPN1.	[✓ ○]	○
To create a direct Site-to-Site connection to the Berlin site an additional Local Network Gateway is required.	○	[✓ ○]
To enable users in the Paris site to connect to Vnet1, the IP address of LocalNetworkGateway1 must be changed to 172.16.0.1.	○	[✓ ○]

Section:
Explanation:

QUESTION 122
HOTSPOT
You have an Azure subscription that contains multiple virtual machine scale sets and multiple Azure load balancers. The load balancers balance traffic across the scale sets.
You plan to deploy Azure Front Door to load balance traffic across the load balancers.
You need to identify which Front Door SKU to configure, and what to use to route the traffic to the load balancers. The solution must minimize costs.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

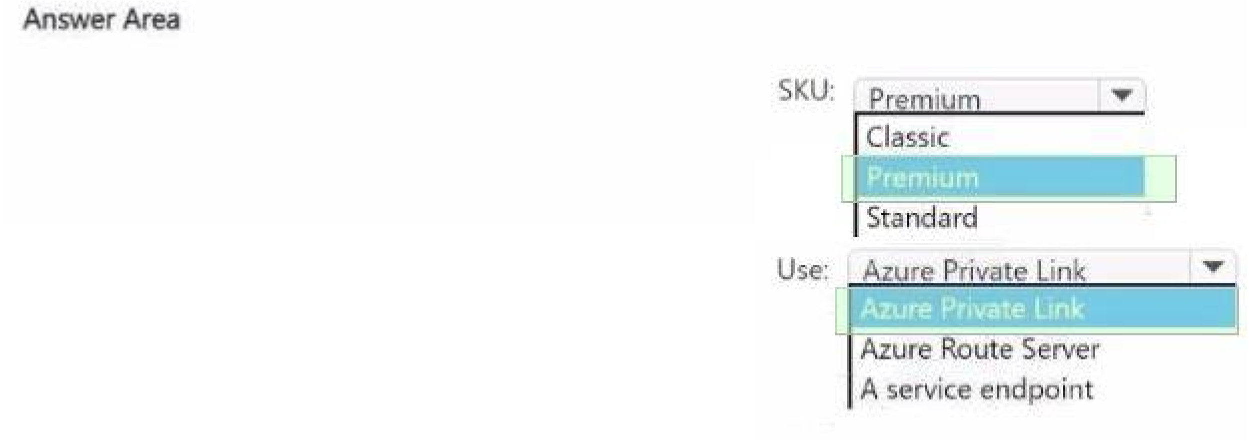


Answer Area

SKU: Premium
- Classic
- Premium
- Standard

Use: Azure Private Link
- Azure Private Link
- Azure Route Server
- A service endpoint

Answer Area:



Answer Area

SKU: Premium
- Classic
- [✓ Premium]
- Standard

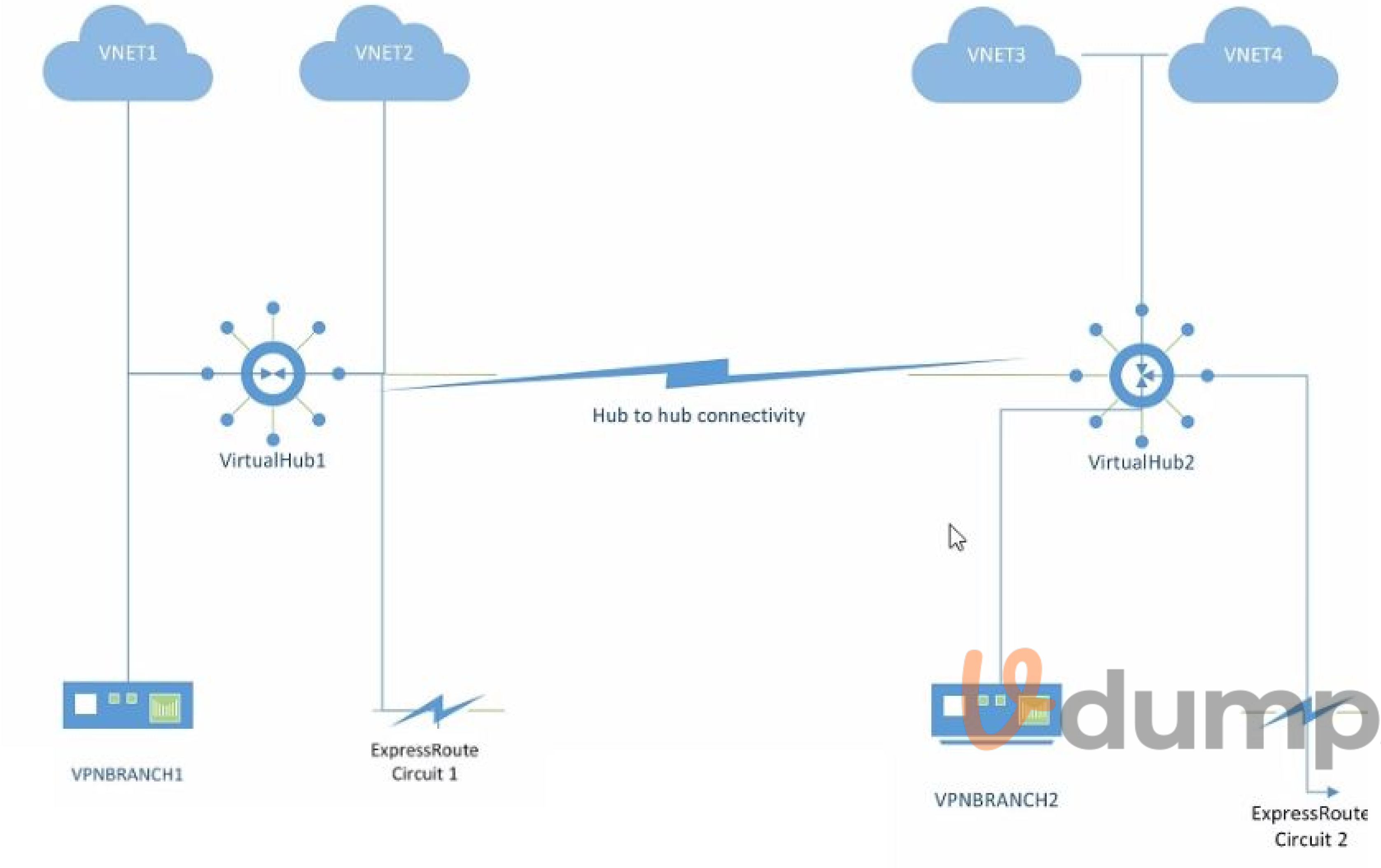
Use: Azure Private Link
- [✓ Azure Private Link]
- Azure Route Server
- A service endpoint

Section:
Explanation:

QUESTION 123

You have an Azure subscription.

You plan to implement Azure Virtual WAN as shown in the following exhibit.



What is the minimum number of route tables that you should create?

A. 1

B. 2

C. 4

D. 6

Correct Answer: B

Section:

QUESTION 124

DRAG DROP

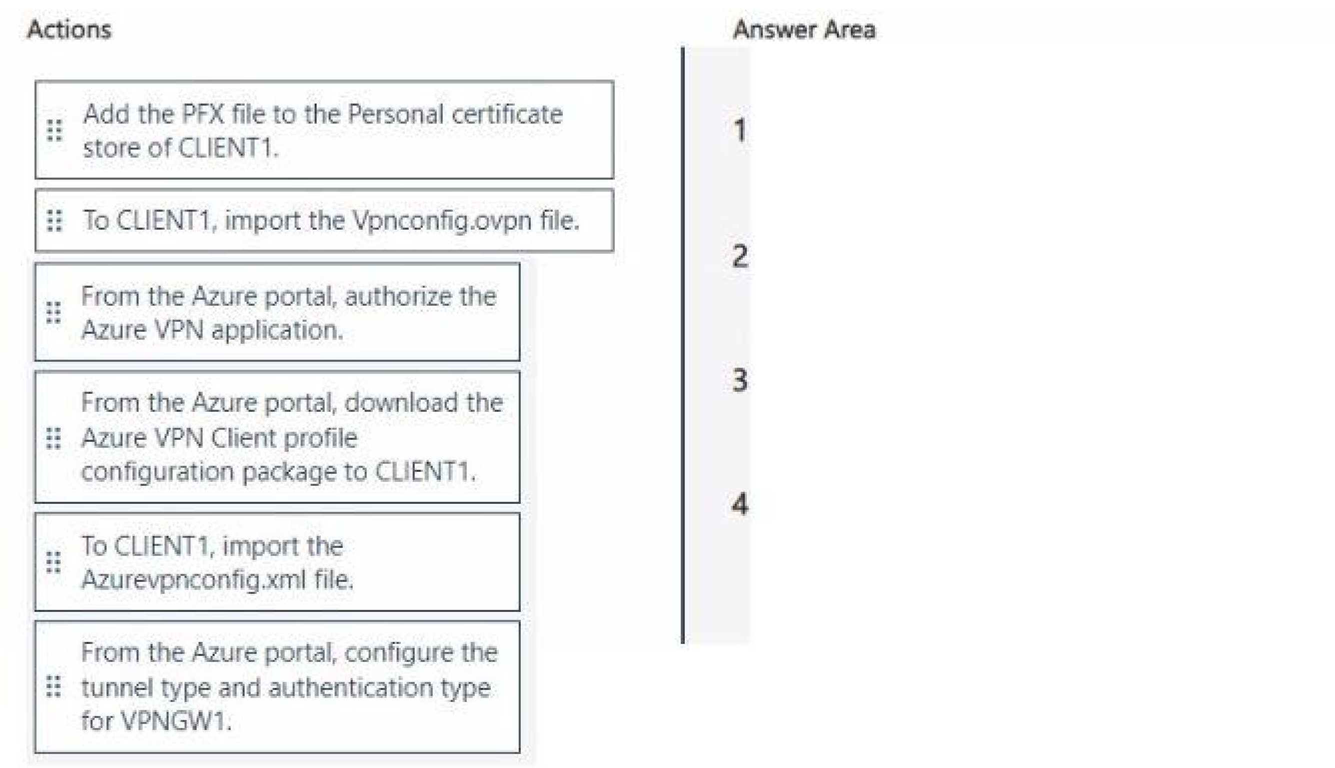
You have a computer named CLIENT! that runs Windows 11 and has the Azure VPN Client installed.

You have an Azure virtual network gateway named VPNGW1.

You need to ensure that you can connect CLIENT1 to VPNGW1. The solution must support Microsoft Entra authentication.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

- Add the PFX file to the Personal certificate store of CLIENT1.
- To CLIENT1, import the Vpnconfig.ovpn file.
- From the Azure portal, authorize the Azure VPN application.
- From the Azure portal, download the Azure VPN Client profile configuration package to CLIENT1.
- To CLIENT1, import the Azurevpnconfig.xml file.
- From the Azure portal, configure the tunnel type and authentication type for VPNGW1.

Answer Area

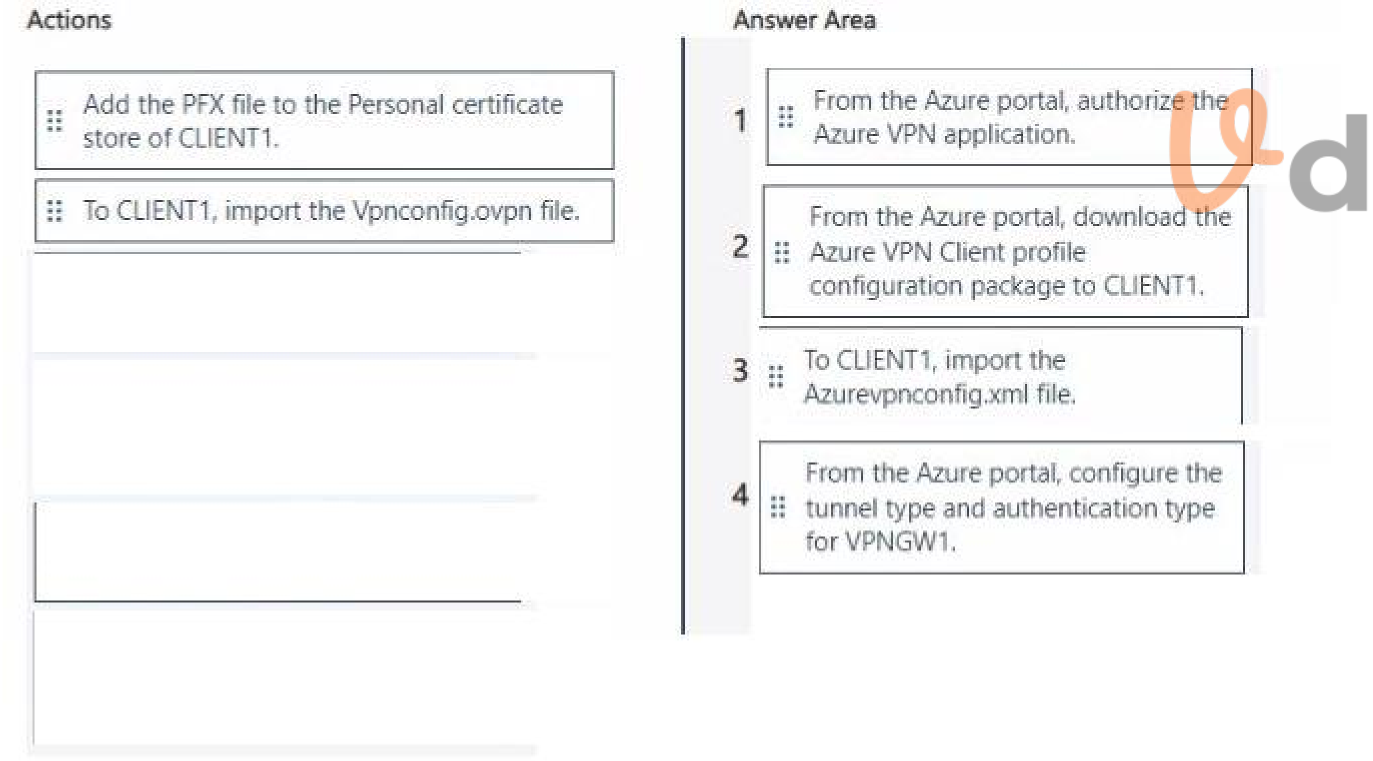
1

2

3

4

Correct Answer:



Actions

- Add the PFX file to the Personal certificate store of CLIENT1.
- To CLIENT1, import the Vpnconfig.ovpn file.

Answer Area

1 From the Azure portal, authorize the Azure VPN application.

2 From the Azure portal, download the Azure VPN Client profile configuration package to CLIENT1.

3 To CLIENT1, import the Azurevpnconfig.xml file.

4 From the Azure portal, configure the tunnel type and authentication type for VPNGW1.

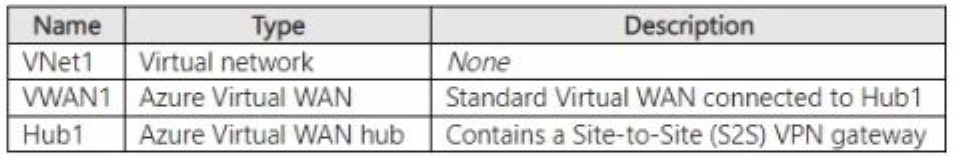
Section:

Explanation:

QUESTION 125

You have an on-premises datacenter named Site1 that contains a firewall named FW1. FW1 connects to the internet.

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



Name	Type	Description
VNet1	Virtual network	*None*
VWAN1	Azure Virtual WAN	Standard Virtual WAN connected to Hub1
Hub1	Azure Virtual WAN hub	Contains a Site-to-Site (S2S) VPN gateway

You plan to connect Site1 to Hub1 by using a site-to-site connection.
You need to configure the site-to-site connection to FW1.
What should you create in VWAN1?

A. a VPN site
B. a virtual network connection
C. a network virtual appliance (NVA)
D. a User VPN configuration

Correct Answer: A
Section:

QUESTION 126
SIMULATION
Task 1
You need to ensure that virtual machines on VNET1 and VNET2 are included automatically in a DNS zone named contoso.azure. The solution must ensure that the virtual machines on VNET1 and VNET2 can resolve the names of the virtual machines on either virtual network.

A. See the Explanation below for step by step instructions

Correct Answer: A
Section:
Explanation:
To achieve the task of ensuring that virtual machines on VNET1 and VNET2 are included automatically in a DNS zone namedcontoso.azure, and that they can resolve the names of the virtual machines on either virtual network, you can follow these steps:
Step-by-Step Solution
Step 1: Create a Private DNS Zone
Navigate to the Azure Portal.
Search for ''Private DNS zones''in the search bar and select it.
Click on ''Create''.
Enter the DNS zone nameascontoso.azure.
Select the appropriate subscriptionand resource group.
Click on ''Review + create''and then''Create''.
Step 2: Link VNET1 and VNET2 to the DNS Zone
Go to the newly created DNS zone(contoso.azure).
Select ''Virtual network links''from the left-hand menu.
Click on ''Add''.
Enter a namefor the link (e.g.,VNET1-link).
Select the subscriptionandvirtual network (VNET1).
Enable auto-registrationto ensure that VMs are automatically registered in the DNS zone.
Click on ''OK''.
Repeat the processfor VNET2.
Step 3: Configure DNS Settings for VNET1 and VNET2
Navigate to VNET1in the Azure Portal.

Select ''DNS servers''under the ''Settings'' section.
Ensure that the DNS server is set to ''Default (Azure-provided)''.
Repeat the processfor VNET2.
Step 4: Verify Name Resolution
Deploy a virtual machinein VNET1 and another in VNET2.
Connect to the virtual machinesusing Remote Desktop Protocol (RDP) or Secure Shell (SSH).
Test name resolutionby pinging the VM in VNET2 from the VM in VNET1 using its hostname (e.g.,ping <VM-name>.contoso.azure).
Explanation:
Private DNS Zone: This allows you to manage and resolve domain names in a private network without exposing them to the public internet.
Virtual Network Links: Linking VNET1 and VNET2 to the DNS zone ensures that VMs in these networks can register their DNS records automatically.
Auto-registration: This feature automatically registers the DNS records of VMs in the linked virtual networks, simplifying management.
DNS Settings: Using Azure-provided DNS ensures that the VMs can resolve each other's names without additional configuration.
By following these steps, you ensure that virtual machines on VNET1 and VNET2 are included automatically in the DNS zonecontoso.azureand can resolve each other's names seamlessly.

QUESTION 127
SIMULATION
Task 2
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 Central region are in a network segment that has an IP address range of 10.5.1.0/24.

A. See the Explanation below for step by step instructions

Correct Answer: A
Section:
Explanation:
To deploy Azure virtual machines to the France Central region and ensure they are in a network segment with an IP address range of 10.5.1.0/24, follow these steps:
Step-by-Step Solution
Step 1: Create a Virtual Network in France Central
Navigate to the Azure Portal.
Search for ''Virtual networks''in the search bar and select it.
Click on ''Create''.
Enter the following details:
Subscription: Select your subscription.
Resource Group: Select an existing resource group or create a new one.
Name: Enter a name for the virtual network (e.g.,VNet-FranceCentral).
Region: SelectFrance Central.
Click on ''Next: IP Addresses''.
Step 2: Configure the Address Space and Subnet
In the IP Addresses tab, enter the address space as10.5.1.0/24.
Click on ''Add subnet''.
Enter the following details:
Subnet name: Enter a name for the subnet (e.g.,Subnet-1).
Subnet address range: Enter10.5.1.0/24.
Click on ''Add''.
Click on ''Review + create''and then''Create''.
Step 3: Deploy Virtual Machines to the Virtual Network
Navigate to the Azure Portal.
Search for ''Virtual machines''in the search bar and select it.
Click on ''Create''and then''Azure virtual machine''.
Enter the following details:

Subscription: Select your subscription.
Resource Group: Select the same resource group used for the virtual network.
Virtual machine name: Enter a name for the VM.
Region: SelectFrance Central.
Image: Select the desired OS image.
Size: Select the appropriate VM size.
Click on ''Next: Disks'', configure the disks as needed, and then click on''Next: Networking''.
In the Networking tab, select the virtual network (VNet-FranceCentral) and subnet (Subnet-1) created earlier.
Complete the remaining configuration stepsand click on''Review + create''and then''Create''.
Explanation:
Virtual Network: A virtual network in Azure allows you to create a logically isolated network that can host your Azure resources.
Address Space: The address space10.5.1.0/24ensures that the VMs are in a specific network segment.
Subnet: Subnets allow you to segment the virtual network into smaller, manageable sections.
Region: Deploying the virtual network and VMs in the France Central region ensures that the resources are physically located in that region.
By following these steps, you can ensure that your Azure virtual machines in the France Central region are deployed within the specified IP address range of 10.5.1.0/24.