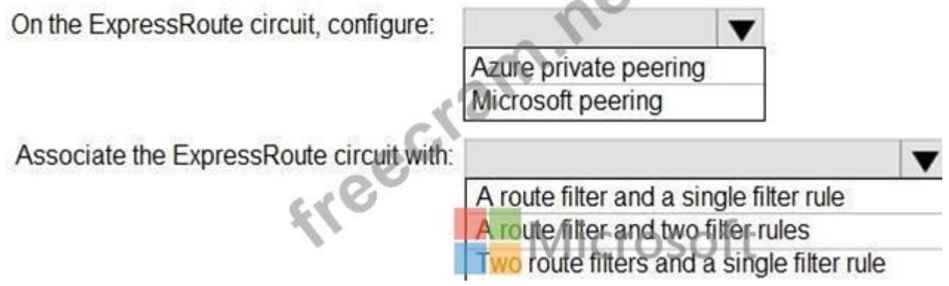
Microsoft.AZ-700.v2026-10-23.q191

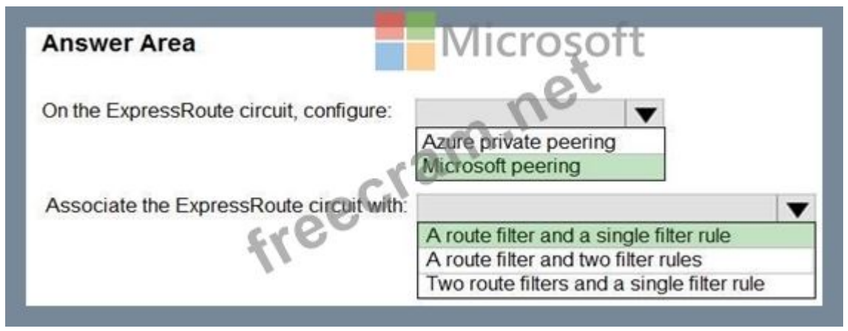
Exam Code:	AZ-700
Exam Name:	Designing and Implementing Microsoft Azure Networking Solutions
Certification Provider:	Microsoft
Free Question Number:	191
Version:	v2026-10-23
# of views:	103
# of Questions views:	1910
https://www.freecram.net/torrent/Microsoft.AZ-700.v2026-10-23.q191.html	

NEW QUESTION: 1
Hotspot Question
You create an ExpressRoute circuit named ERC1 that is enabled by your connectivity provider.
You need to ensure that the routes for Azure Backup and Azure Cosmos DB are advertised to the on-premises network via ECR1.
The solution must minimize administrative effort.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



NEW QUESTION: 2
SIMULATION



Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
- If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You need to ensure that requests for www.relecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net.
To complete this task, sign in to the Azure portal.
Answer:

Stage 1: Create an Azure private DNS zone using the Azure portal.

Step 1: On the portal search bar, type private dns zones in the search text box and press Enter.

Step 2: Select Private DNS zone.

Step 3: Select Create private dns zone.
On the Create Private DNS zone page, type or select appropriate values:

Resource group: Select Create new, enter something X, and select OK. The resource group name must be unique within the Azure subscription.
Name: Type private.relecloud.com.
Resource group location:

Step 4: Select Review + Create.

Step 5: Select Create.

Stage 2: Create a CNAME DNS record

Step 6: Open the X resource group you created earlier and select the private.relecloud.com private zone.
You can enter private.relecloud.com the Filter by name box to find it more easily.

Step 7: At the top of the DNS zone page, select + Record set.

Step 8: On the Add record set page, type or select the following values:

Name: Type www.
Type: CNAME
Record set properties: frontdoor1.azurefd.net

Step 9: Select Save at the top of the page to save your settings. Then close the page.

Reference:
https://learn.microsoft.com/en-us/azure/dns/private-dns-getstarted-portal
https://learn.microsoft.com/en-us/azure/dns/dns-operations-recordsets-portal

freecram.net

NEW QUESTION: 3

You are the system administrator. You need to create and set the IPsec/IKE policy on a site-to- site VPN connection. The following are the steps (not necessarily in the proper sequence) required to create and update the policy.
a. Create a local network gateway for the cross-premises connection.
b. Create a virtual network and a VPN gateway.
c. Create an IPsec/IKE policy with selected algorithms and parameters.
d. Create an IPSec connection with the IPsec/IKE policy.
e. Add/update/remove an IPsec/IKE policy for an existing connection.
Arrange the above steps in the proper sequence.
A. b-a-c-d-eright
B. a-b-c-d-e
C. a-b-d-c-e
D. a-c-d-e-b
E. b-a-d-c-e
Answer: (SHOW ANSWER)
Here are the steps you should follow to create and update/set the IPsec/IKE policy on a site-to- site VPN connection.

- OpenVPN® Protocol, an SSL/TLS based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. OpenVPN can be used to connect from Android, iOS (versions 11.0 and above), Windows, Linux, and Mac devices (macOS versions 10.13 and above).

- Secure Socket Tunneling Protocol (SSTP), a proprietary TLS-based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. SSTP is only supported on Windows devices. Azure supports all versions of Windows that have SSTP (Windows 7 and later).

- IKEv2 VPN, a standards-based IPsec VPN solution. IKEv2 VPN can be used to connect from Mac devices (macOS versions 10.11 and above).

Option A is correct. The given sequence is the proper sequence of steps to be followed to create and update/set the IPsec/IKE policy on a site-to-site VPN connection.
Option B is incorrect. The given sequence is not correct.
Option C is incorrect. With the given sequence of steps, you can't create or set the IPsec/IKE policy on a site-to-site VPN connection.
Option D is incorrect. The given sequence is not correct.
Option E is incorrect. The given sequence is not correct.
Reference:
https://docs.microsoft.com/en-us/azure-stack/user/azure-stack-vpn-s2s

NEW QUESTION: 4
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.corn 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. rules
B. rewrites
C. HTTP settings

D. listeners

Answer: (SHOW ANSWER)

https://docs.microsoft.com/en-us/azure/application-gateway/configuration-request-routing-rules#rule-type

NEW QUESTION: 5

Case Study 2 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment:

Azure Network Infrastructure

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	**None**

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

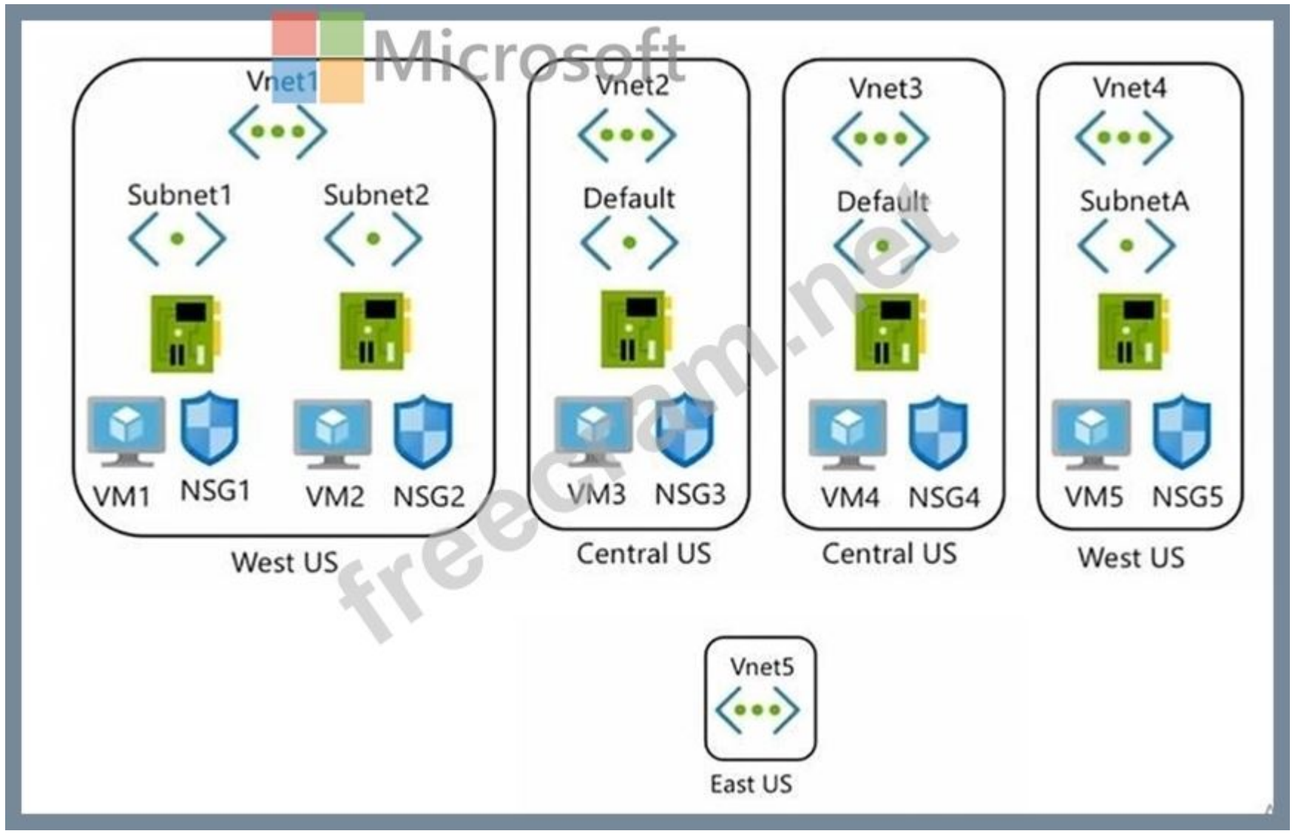
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements:
Virtual Network Requirements
Contoso has the following virtual networks requirements:
- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
Two container groups that connect to Vnet6
Three virtual machines that connect to Vnet6
Allow VPN connections to be established to Vnet6
Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over
the Microsoft backbone network
- The virtual machines in Vnet4 and Vnet5 must be able to communicate
over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-
Analyze must inspect the outbound network traffic from Subnet2 to the
internet.
Network Security Requirements
Contoso has the following network security requirements:
- Configure Azure Active Directory (Azure AD) authentication for Point- to-Site (P2S) VPN users.
- Enable NSG flow logs for NSG3 and NSG4.
- Create an NSG named NSG10 that will be associated to Vnet1/Subnet1
and will have the custom inbound security rules shown in the following
table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

- Create an NSG named NSG11 that will be associated to Vnet1/Subnet2
and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

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

Answer Area

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	○	○
VM4 has an automatic registration in zone1.contoso.com.	○	○
You can link zone2.contoso.com to Vnet3 and enable auto registration.	○	○

Microsoft
freecram.net

Answer:

Answer Area

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	○	●
VM4 has an automatic registration in zone1.contoso.com.	●	○
You can link zone2.contoso.com to Vnet3 and enable auto registration.	○	●

Explanation:
Box 1: No
Zone2.contoso.com is not linked to any virtual networks. Therefore, no VMs are able to resolve names in the zone.
Box 2: Yes
VM4 is in VNet3. Zone1.contoso.com has a link to VNet3 and auto-registration is enabled on the link.
Box3: No
VNet3 is linked to zone1.contoso.com and auto-registration is enabled on the link. A virtual network can only have one registration zone. You can link zone2.contoso.com to VNet3 but you won't be able to enable auto-registration on the link.

NEW QUESTION: 6
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. On FW1, configure a DNAT rule for port 1688
B. Deploy a NAT gateway.
C. Add an internet route to RT1 for the Azure Key Management Service (KMS).
D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

Answer: (SHOW ANSWER)

Add specific outbound rule for KMS in the FW as there is already default route points FW.
Add specific address prefix route in route table so it can by pass default route to FW.

NEW QUESTION: 7

Drag and Drop Question

Your on-premises network uses an IP address space of 10.0.0.0/20.
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
RT1	Route table	None
HubVNet	Virtual network	Uses an IP address space of 172.16.0.0/20 Peered to SpokeVNet
SpokeVNet	Virtual network	Uses an IP address space of 192.168.0.0/20

The on-premises network is connected to HubVnet by using a Site-to-Site (S2S) VPN.
You deploy an Azure firewall named AZFW1 to HubVNet.
You need to ensure that AZFW/1 can inspect all the traffic between the on-premises network and SpokeVNet.
What should you do in RT1? To answer, drag the appropriate destination to the correct route.
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.

Destinations

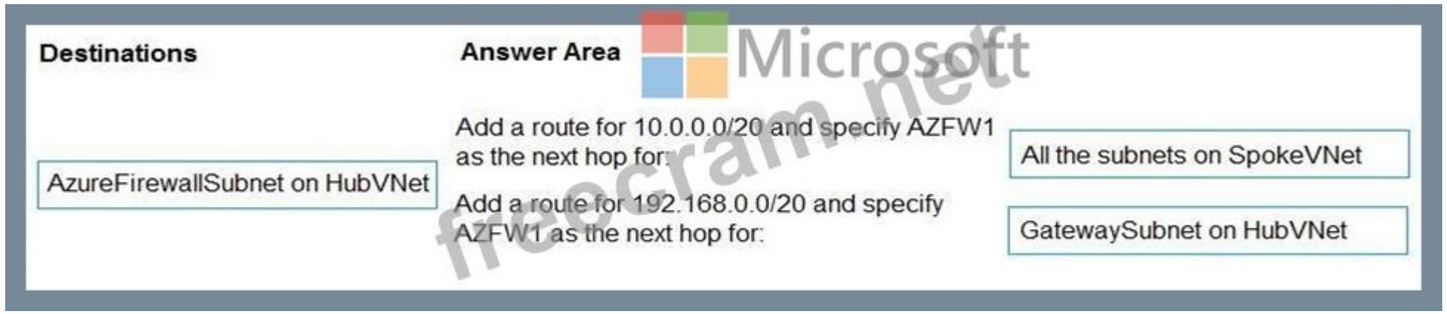
- All the subnets on SpokeVNet
- AzureFirewallSubnet on HubVNet
- GatewaySubnet on HubVNet

Answer Area

Add a route for 10.0.0.0/20 and specify AZFW1 as the next hop for: [ ]

Add a route for 192.168.0.0/20 and specify AZFW1 as the next hop for: [ ]

Answer:



NEW QUESTION: 8

Hotspot Question

Your on-premises network contains a server named DNS1 that runs Windows Server 2022.

DNS1 has the DNS server role and an IP address of 10.1.0.1. The network contains computers that use DNS1 for name resolution.

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

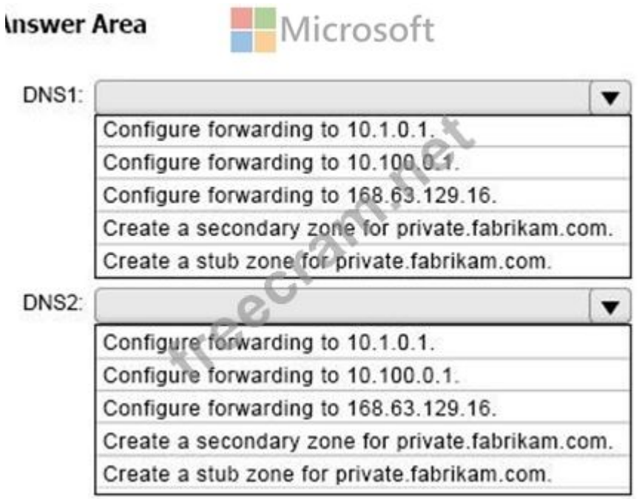
Name	Type	Description
private.fabrikam.com	Azure Private DNS zone	Linked to Vnet1
Vnet1	Virtual network	*None*
SQL1	Azure SQL Database	Has a private endpoint in Vnet1 that is registered in private.fabrikam.com
DNS2	Server that runs Windows Server 2022	Has the DNS server role and an IP address of 10.100.0.1

The on-premises network connects to Vnet1 by using a Site-to-Site VPN.

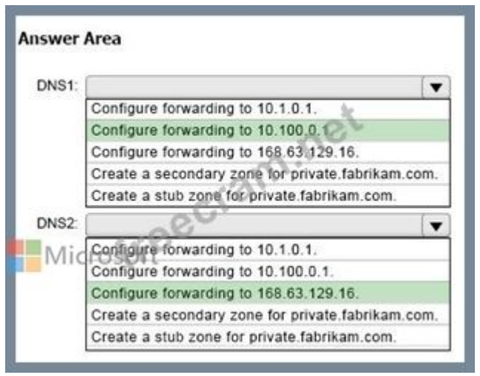
You need to ensure that the computers on the on-premises network can resolve the IP address for sql1.private.fabrikam.com.

What should you do on DNS1 and DNS2? To answer, drag the appropriate actions to the correct servers. Each action 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.



Answer:



Explanation:

On-prem DNS server DNS1 should be configured have conditional forwarder to forward traffic to AZ DNS server on IP 10.100.0.1 which acts as Azure DNS forwarder The Azure DNS server DNS2 - then forwards the DNS traffic to Azure recursive resolvers (IP

168.63.129.16) which in turn resolves the request to the on-prem client As NOTE: As of now and onwards - MS Azure no longer uses this method for name resolution to and from on-Prem - they have service called Azure DNS private resolver with inbound-outbound Endpoints with rule in place see link below - pay attention to the diagram

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#virtual-network-and-on- premises-workloads-using-a-dns-forwarder

https://learn.microsoft.com/en-us/azure/virtual-network/what-is-ip-address-168-63-129-16

NEW QUESTION: 9

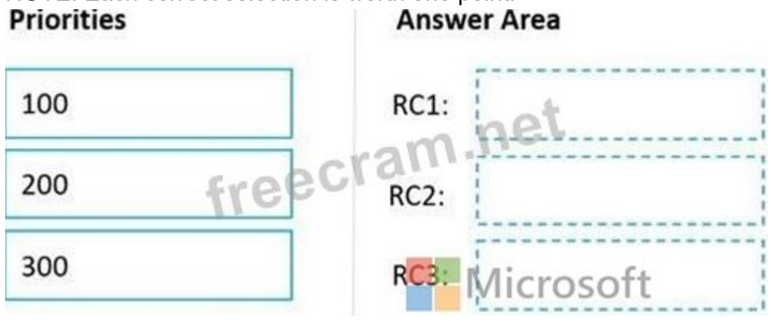
Drag and Drop Question You have an Azure subscription that contains an Azure Firewall Premium policy named FWP1.

To FWP1, you plan to add the rule collections shown in the following table.

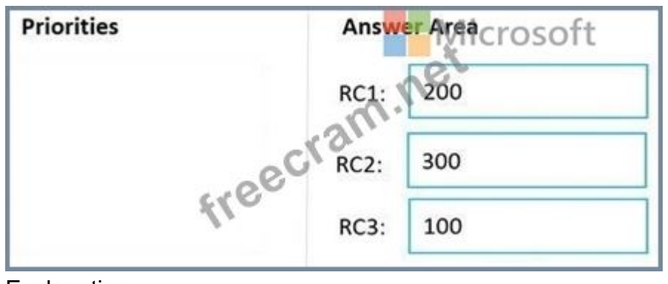
Name	Type
RC1	Network
RC2	Application
RC3	DNAT

Which priority should you assign to each rule collection? To answer, drag the appropriate priority values to the correct rule collections. Each value 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.



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets#rule-collection-groups

NEW QUESTION: 10
Hotspot Question
You have an Azure subscription that contains the resources shown in the following table:

Name	Type	Description
VNet1	Virtual network	Contains Subnet1 and Subnet2
Subnet1	Subnet	Has an IP address space of 10.0.1.0/24
Subnet2	Subnet	Dedicated subnet for virtual machines that host an app named App1 Has an IP address space of 10.1.0.0/16
NSG1	Network security group (NSG)	Associated to Subnet1 Denies traffic between Subnet 1 and Subnet2
SQL1	SQL Server on Azure Virtual Machines	Connected to Subnet1
SQL2	SQL Server on Azure Virtual Machines	Connected to Subnet1
SQL3	SQL Server on Azure Virtual Machines	Connected to Subnet1
ASG1	Application security group	Contains SQL1 and SQL2
ASG2	Application security group	Contains SQL1, SQL2, and SQL2

Each quarter, you deploy five new virtual machines to host App1.
You need to add a rule to NSG1 to ensure that the virtual machines that host App1 can connect to SQL1 and SQL2. The solution must follow the principle of least privilege and minimize administrative effort.
How should you configure the source property and the destination property for the rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



NEW QUESTION: 11

You have an Azure Front Door instance that has a single frontend named Frontend1 and an Azure Web Application Firewall (WAF) policy named Policy1.

Policy1 redirects requests that have a header containing "string1" to https://www.contoso.com/redirect1. Policy1 is associated to Frontend1.

You need to configure additional redirection settings.

Requests to Frontend1 that have a header containing "string2" must be redirected to https://www.contoso.com/redirect2.

Which three actions should you perform? Each correct answer presents part of the solution.

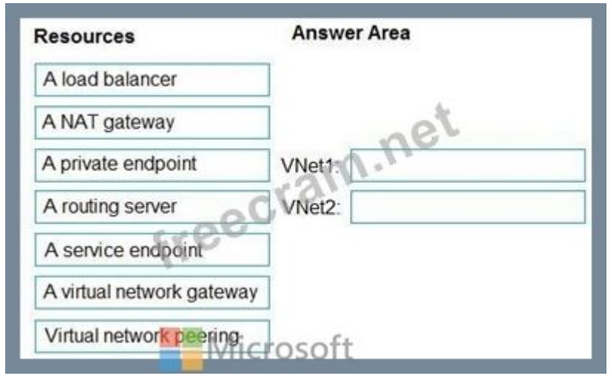
NOTE: Each correct selection is worth one point.

A. Create a custom rule.
B. Configure a managed rule.
C. Create a frontend host.
D. Create a policy.
E. Create an association.
F. Add a custom rule to Policy1.
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-create-portal

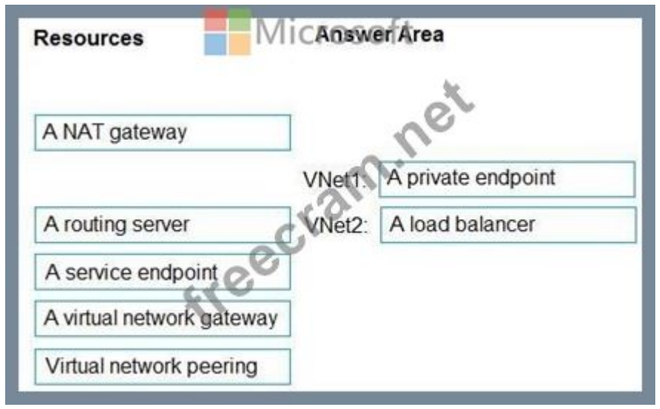
NEW QUESTION: 12
Drag and Drop Question
You have two Azure subscriptions named Sub1 and Sub2 that contain the resources shown in the following table.

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.

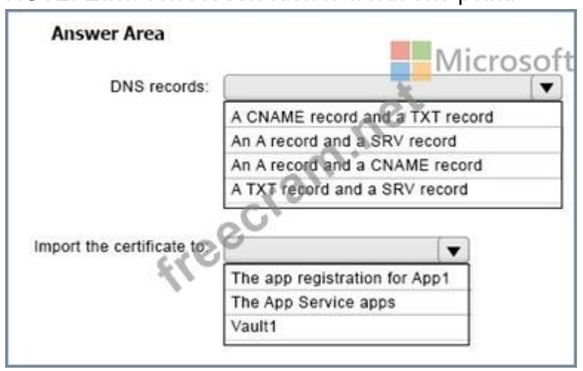


Answer:



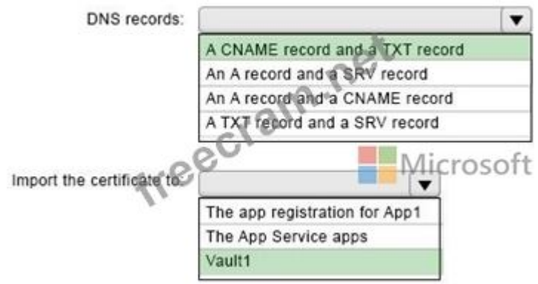
Explanation:
https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview#workflow

NEW QUESTION: 13
Hotspot Question
You have an Azure subscription that contains an Azure key vault named Vault1 and an app registration for an Azure AD app named App1.
You have a DNS domain named contoso.com that is hosted by a third-party DNS provider.
You plan to deploy App1 by using Azure App Service. App1 will have the following configurations:
- App1 will be hosted across five App Service apps.
- Users will access App1 by using a URL of https://app1.contoso.com.
- The user traffic of App1 will be managed by using Azure Front Door.
- The traffic between Front Door and the App Service apps will be sent by using HTTP.
- App1 will be secured by using an SSL certificate from a third-party certificate authority (CA).
You need to support the Front Door deployment.
Which two DNS records should you create, and to where should you import the SSL certificate for App1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Answer Area



NEW QUESTION: 14

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

Answer: (SHOW ANSWER)

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

NEW QUESTION: 15

SIMULATION



Username and password

Use the following login credentials as needed:

- To enter your username, place your cursor in the Sign in box and click on the username below.

- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

- Lab Instance: 12345678

You have two servers that are each hosted by a separate service provider in New York and California. The server hosted in New York is accessible by using a host name of ny.contoso.com.

The server hosted in California is accessible by using a host name of ca.contoso.com.

You need to implement an Azure solution to route users to the server that has the lowest latency.

The solution must minimize costs.

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

Answer:

Azure front Door route lowest latency

Set up Azure Front Door to route user traffic based on the lowest latency between the two web app servers. Start by adding a frontend host for Azure Front Door.

If there is already an Azure Front Door available, select it and skip phase 1. Start with phase 2.
If there is already an Azure Front Door and a backpool available, select them and skip phase 1 and phase 2. Start with phase 3.

Phase 1: Setup an Azure Front Door

Step 1: From the home page or the Azure menu, select + Create a resource. Select Networking > Front Door and CDN profiles.

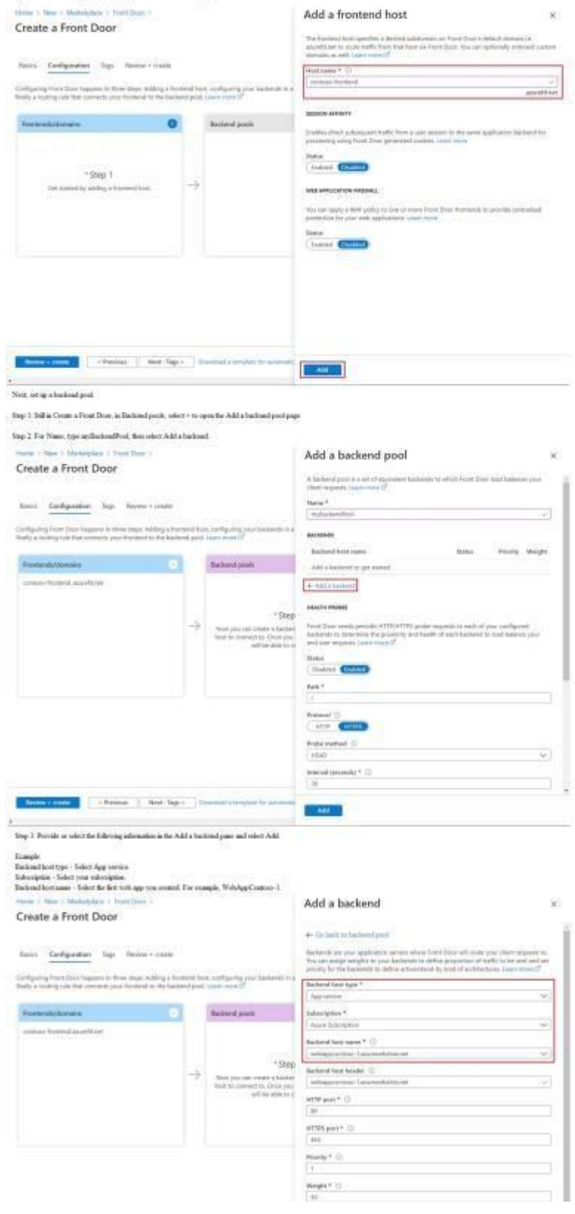
Step 2: On the Compare offerings page, select Explore other offerings. Then select Azure Front Door (classic). Then select Continue.

Step 3: In the Basics tab of Create a Front Door page, provide or select the following information, and then select Next: Configuration.

Example:
Subscription - Select your subscription.
Resource group - Select Create new and type FrontDoorQS_rg0 in the text box.
Resource group location - Select Central US.

Step 4: In Frontends/domains, select + to open Add a frontend host page.

Step 5: For Host name, type a globally unique hostname. For example, contoso-frontend. Select Add.



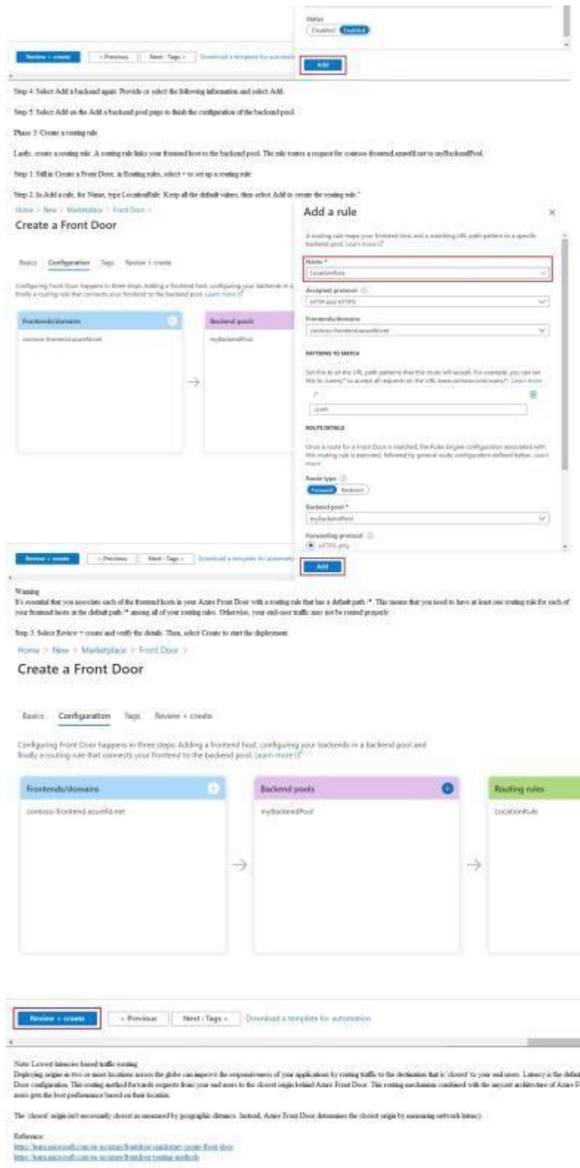
Next, set up a backend pool.

Step 1: Still in Create a Front Door, in Backend pools, select + to open the Add a backend pool page.

Step 2: For Name, type myBackendPool, then select Add a backend.

Step 3: Provide or select the following information in the Add a backend pane and select Add.

Example:
Backend host type - Select App service.
Subscription - Select your subscription.
Backend host name - Select the first web app you created. For example, WebAppContoso-1.



NEW QUESTION: 16

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.
Answer: (SHOW ANSWER)
You need a backend for VMSS2, a listener for the site adatum.com and a rule to redirect the request from the listener to backend VMSS2
https://docs.microsoft.com/en-us/azure/application-gateway/configuration-overview

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
You have an Azure subscription. The subscription contains a locally-redundant storage (LRS) account named storage1 that is deployed to the US East Azure region and has a Microsoft.Storage service endpoint.
You set Redundancy for storage1 to Read-access geo-redundant storage (RA-GRS).
You need to ensure that the contents of storage1 will be accessible by using a service endpoint in a paired region. The solution must minimize administrative effort.
What should you do first?
A. Create an object replication rule for storage.
B. Delete the existing service endpoint.
C. From storage1, select Secure transfer required.
D. Create a service endpoint policy.
Answer: (SHOW ANSWER)
When Service Endpoint policies are applied on a subnet, the Azure Storage Service Endpoint scope gets upgraded from regional to global. This process means that all the traffic to Azure Storage is secured over service endpoint thereafter. The Service endpoint policies are also applicable globally. Any storage accounts that aren't explicitly allowed are denied access.
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview

NEW QUESTION: 18


Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.

- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

- Lab Instance: 12345678

You are planning security for Azure Front Door.

You need to create a rule that can be applied to Front Door hosts. The rule must prevent hosts in Japan from making more than 50 requests per minute. You do NOT need to associate the rule to a Front Door instance to complete this task.

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

Answer:

Configure a Web Application Firewall rate-limit rule

The Azure Web Application Firewall rate-limit rule for Azure Front Door controls the number of requests allowed from a particular source IP address to the application during a rate-limit duration.

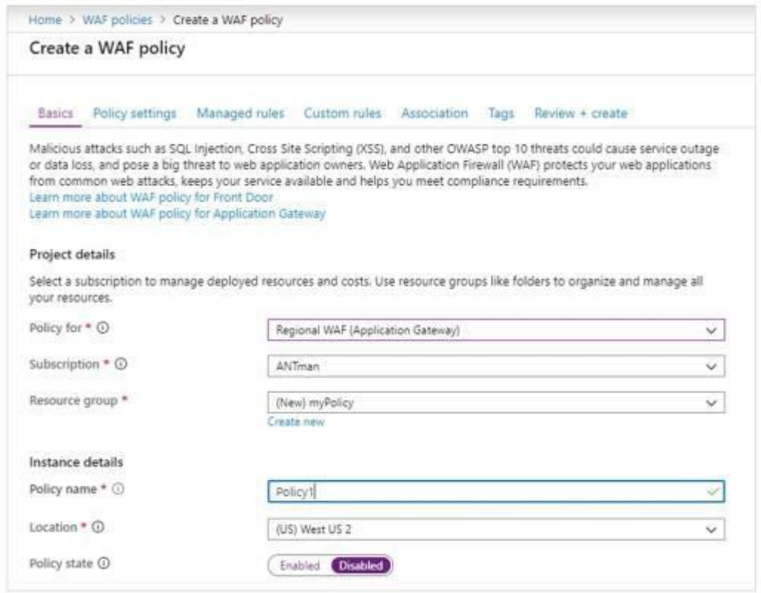
Stage 1: Create a policy

First, create a basic WAF policy

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

Step 2: On Create a WAF policy page, Basics tab, enter

Step 3: Select Review + create, then select Create.



Stage 2: Create a rate-limit rule

Step 1: Select Custom rules > Add custom rule.





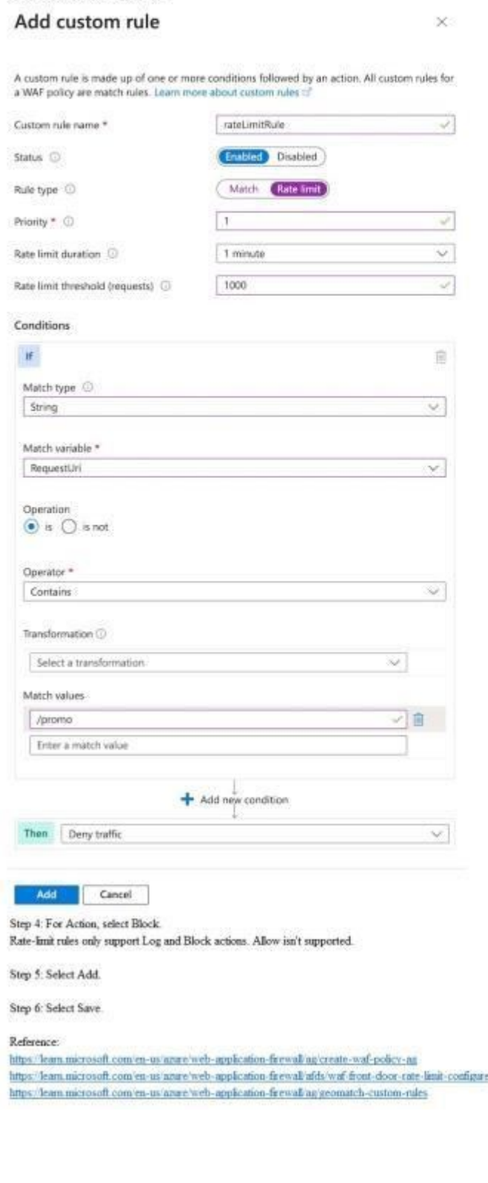
Step 2: Enter the information required to create a rate-limit rule:

Custom rule name: Enter the name of the custom rule, such as rateLimitRule.
Rule type: Select Rate limit.
Priority: Enter the priority of the rule, such as 1.
Rate limit duration: Select 1 minute.
Rate limit threshold (requests): Enter 50

Step 3: In Conditions, enter the information required to specify a match condition to identify requests. For Match type, select Geo location, for Value select JP (for Japan).

Match type: Geo Location.
Operation: Select is.
Match values: JP

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



Step 4: For Action, select Block.
Rate-limit rules only support Log and Block actions. Allow isn't supported.

Step 5: Select Add.

Step 6: Select Save.

Reference:
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag
https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-configure
https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/geomatch-custom-rules

NEW QUESTION: 19
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 Azure Standard Load Balancer that has an outbound NAT rule.
B. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
C. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.
D. Deploy a NAT gateway.
Answer: (SHOW ANSWER)

NEW QUESTION: 20
SIMULATION



Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You need to restrict access to the storage35433841 storage account to ensure that only subnet1-2 can access the account.
To complete this task, sign in to the Azure portal.

Restrict network access to a subnet
By default, storage accounts accept network connections from clients in any network, including the internet. You can restrict network access from the internet, and all other subnets in all virtual networks (except the subnet-private subnet in the vnet-1 virtual network.)

To restrict network access to a subnet:

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

Step 2: Select your storage account storage35433841

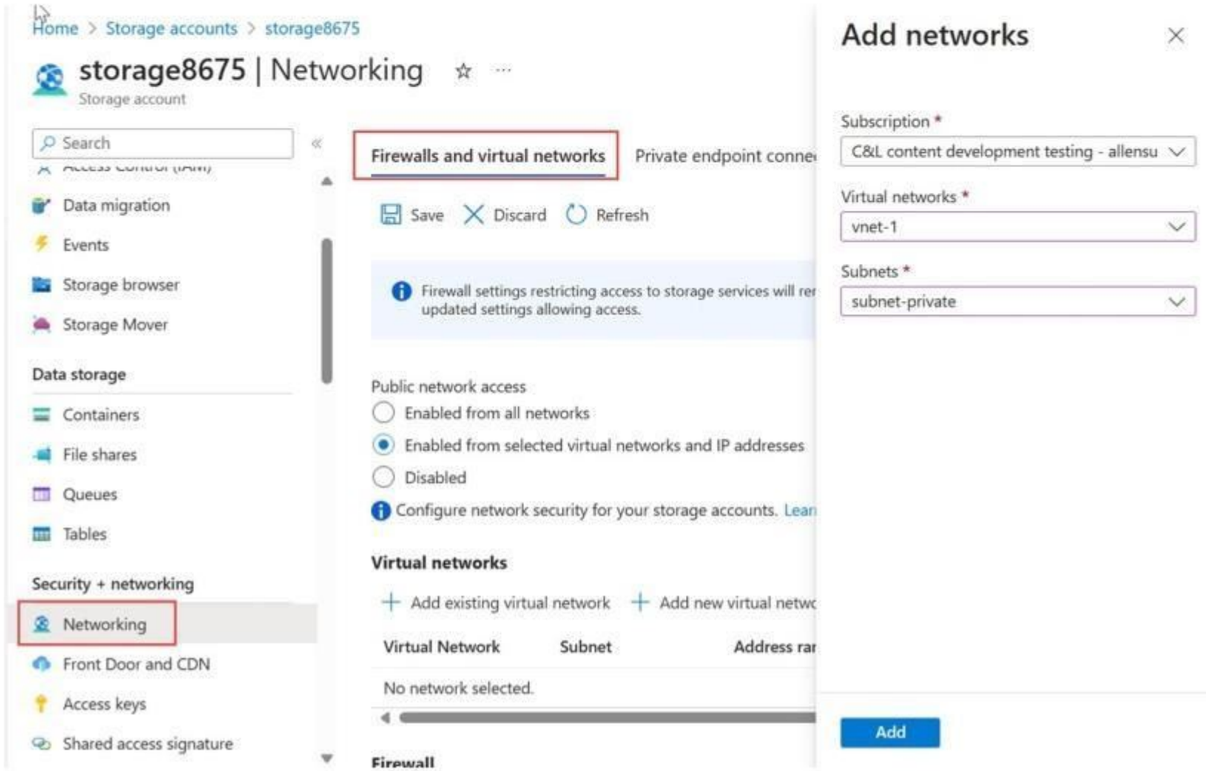
Step 3: In Security + networking, select Networking.

Step 4: In the Firewalls and virtual networks tab, select Enabled from selected virtual networks and IP addresses in Public network access.

Step 5: In Virtual networks, select + Add existing virtual network.

Step 6: In Add networks, enter or select the following information:

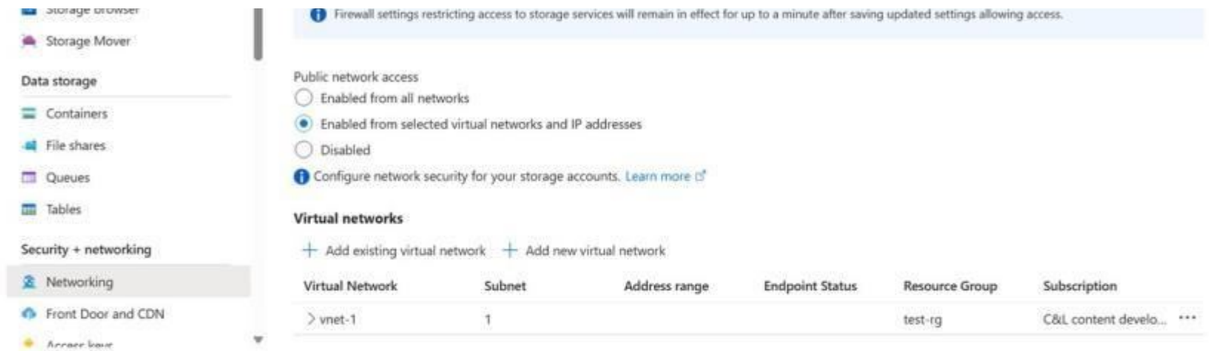
Setting - Value
Subscription: Select your subscription.
Virtual networks: Select the available virtual network
Subnets: Select subnet1-2.



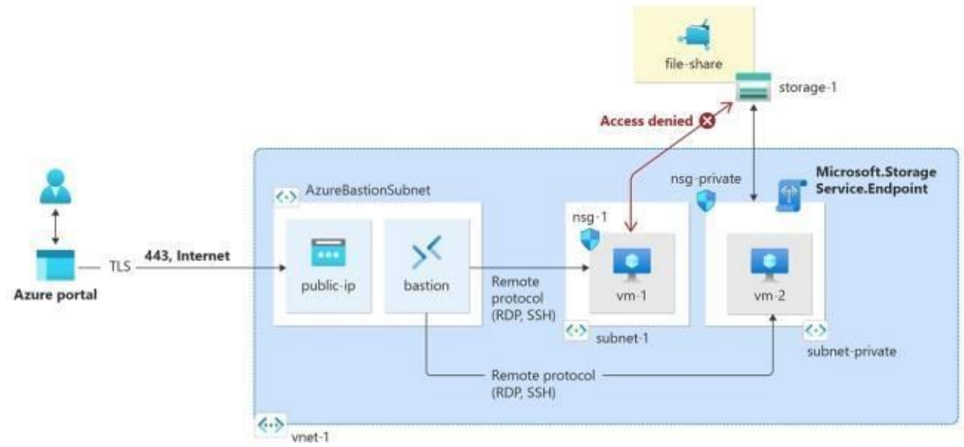
Step 7: Select Add.

Step 8: Select Save to save the virtual network configurations.





Note: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
Note: Virtual network service endpoints enable you to limit network access to some Azure service resources to a virtual network subnet. You can also remove internet access to the resources. Service endpoints provide direct connection from your virtual network to supported Azure services, allowing you to use your virtual network's private address space to access the Azure services. Traffic destined to Azure resources through service endpoints always stays on the Microsoft Azure backbone network.



Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources

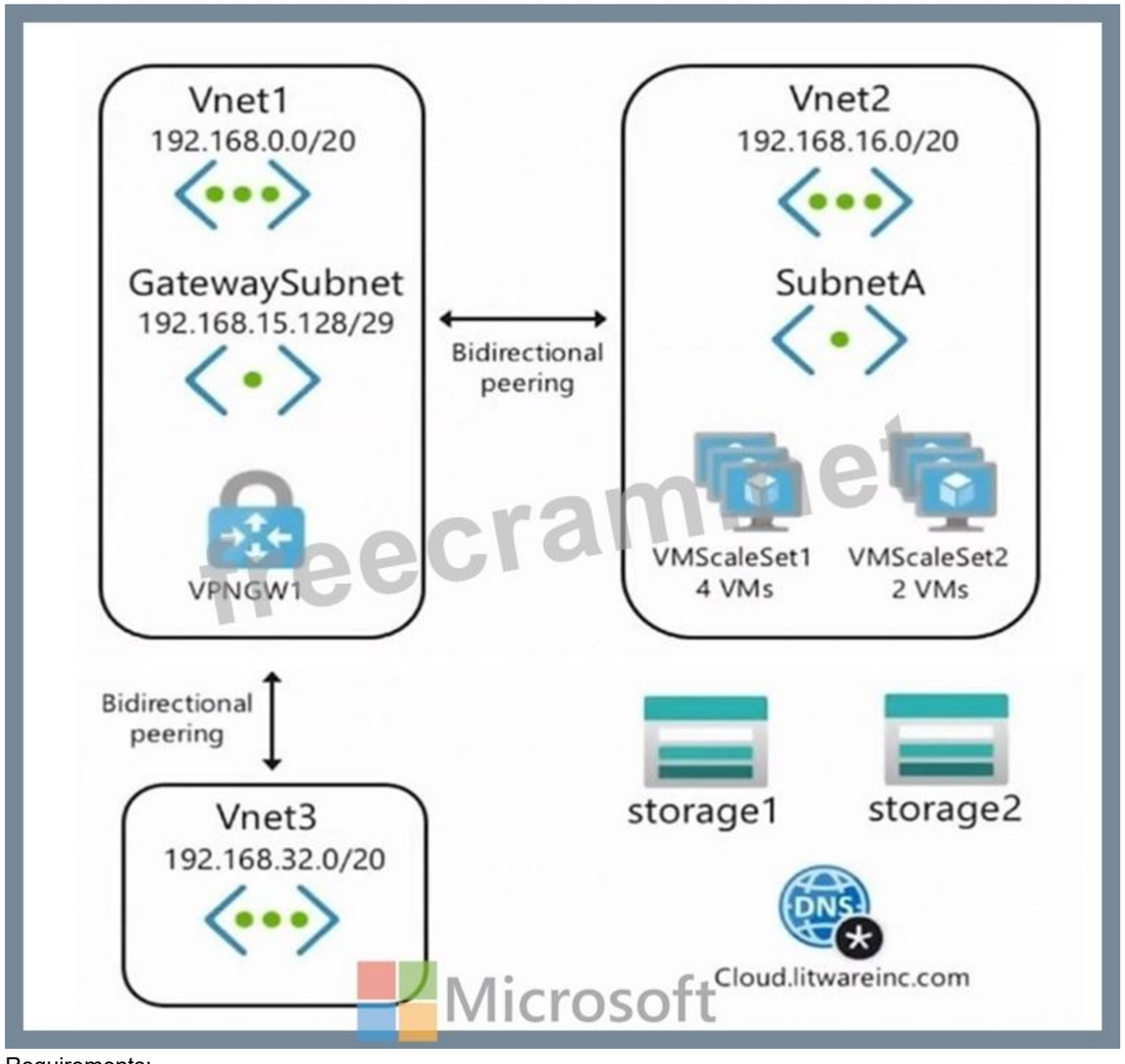
NEW QUESTION: 21
Case Study 1 - Litware. Inc
Overview
Litware. Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.
Existing Environment:
Hybrid Environment
The on-prernises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by usinq Azure AD Connect.
All the offices connect to a virtual network named Vnetl 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.

freecram.net



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 zone 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):

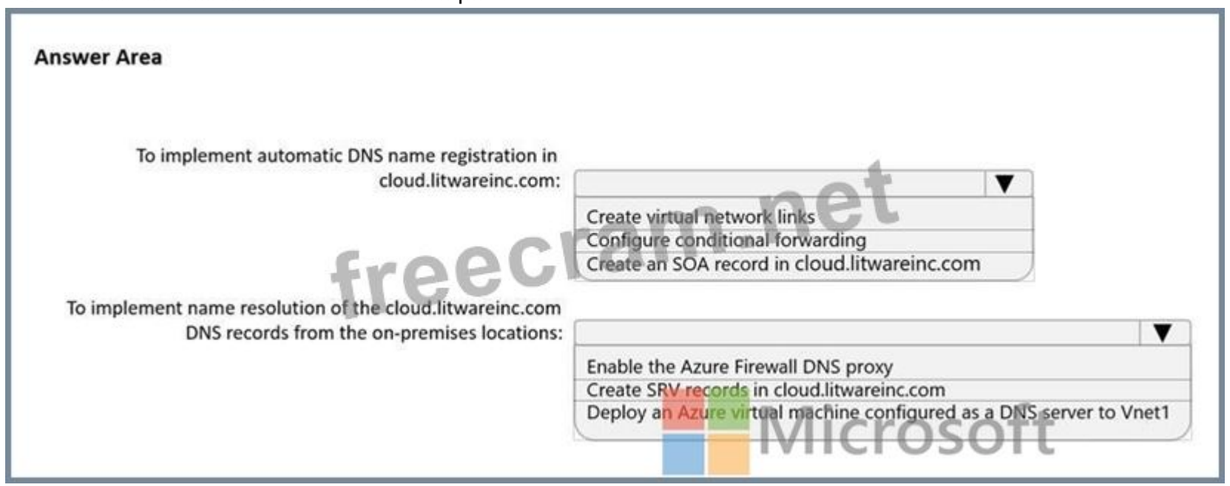
- The storage1 account must be accessible from all on-premises
locations without exposing the public endpoint of storage1.
- The storage2 account must be accessible from Vnet2 and Vnet3 without
exposing the public endpoint of storage2.

Hotspot Question

You need to implement name resolution for the cloud.litwareinc.com. The solution must meet the networking requirements.

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

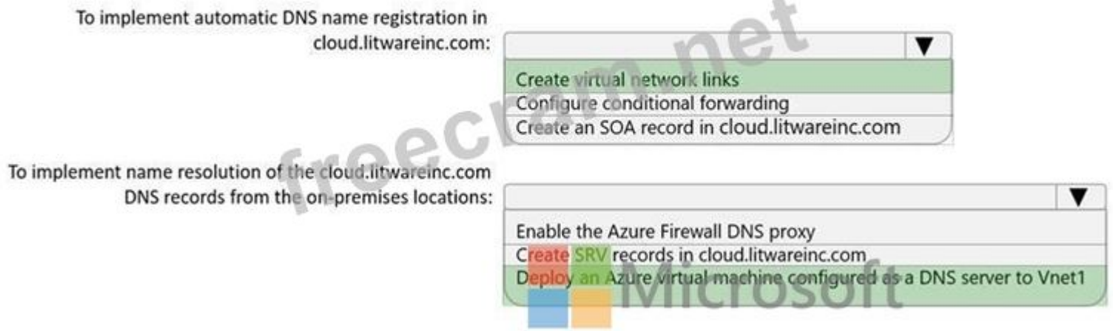
NOTE: Each correct selection is worth one point.



freecram.net
Microsoft

Answer:

Answer Area



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

NEW QUESTION: 22
You have an Azure subscription that contains a web app named App1 and an Azure Web Application Firewall (WAF) on Azure Front Door instance named FD1. FD1 manages traffic for App1.
You need to ensure that if an IP address sends abnormally high levels of traffic to App1, the traffic is detected and blocked automatically. The solution must minimize administrative effort.
What should you include in the solution?
A. an IP restriction rule
B. a WAF exclusion list
C. a bot protection rule set
D. a rate limiting rule
Answer: D (LEAVE A REPLY)
To ensure that abnormally high levels of traffic from a specific IP address are automatically detected and blocked, you must configure Rate Limiting via Azure WAF Custom Rules. This feature tracks requests from individual source IP addresses and automatically denies traffic once a defined threshold is reached Implementation Steps
1. Switch to Prevention Mode: Ensure your WAF policy is set to Prevention mode rather than Detection. In Detection mode, high traffic will only be logged, not blocked.
2. Create a Rate Limit Rule: In the Azure Portal, navigate to your WAF policy and select Custom rules > Add custom rule.
2.1 Rule Type: Select Rate limit.
2.2 Duration: Choose either 1 minute or 5 minutes as the window for counting requests.
2.3 Threshold: Set the maximum number of allowed requests (e.g., 1,000) within that duration.
3 Define Match Conditions:
3.1 To apply the limit to all incoming traffic, use a condition that is always true, such as checking if the RemoteAddr is Any or using a wildcard (*) for the IP address.
3.2 Alternatively, target specific high-risk paths (e.g., /api/login) by matching the RequestUri.
Reference:
https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit

NEW QUESTION: 23
You are planning an Azure Point-to-Site (P2S) VPN that will use OpenVPN. Users will authenticate by using an on premises Active Directory domain.

Which additional service should you deploy to support the VPN authentication?

A. a certification authority (CA)

B. a RADIUS server

C. an Azure key vault

D. Azure Active Directory (Azure AD) Application Proxy

Answer: (SHOW ANSWER)

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

NEW QUESTION: 24

Hotspot Question

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

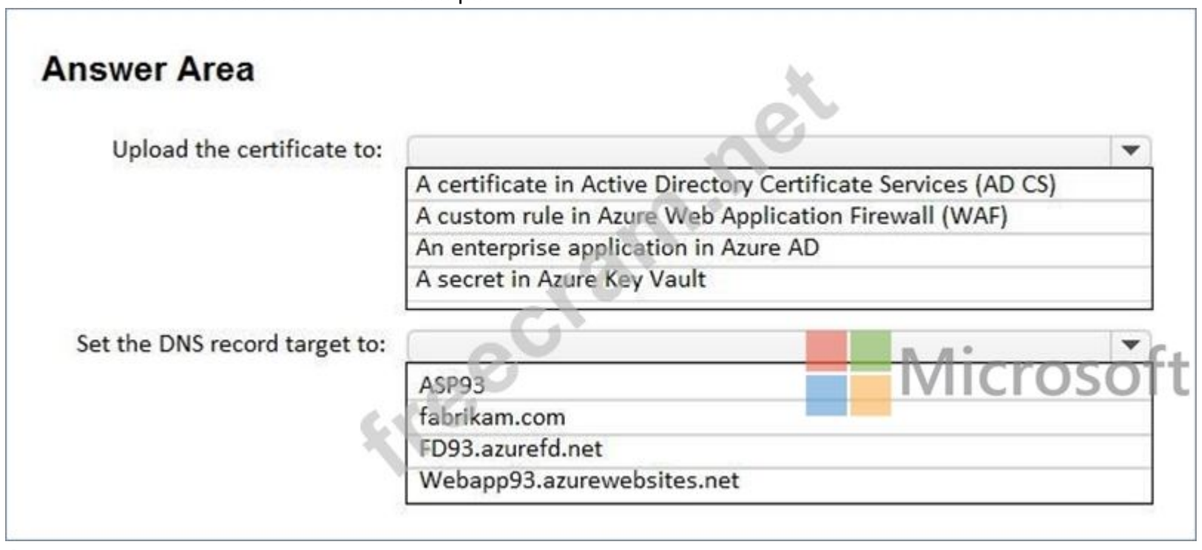
Users will connect to the App Service through Front Door by using a URL of https://www.fabrikam.com.

You obtain a certificate for the host name of www.fabrikam.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.



Answer:



Explanation:

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https

NEW QUESTION: 25

Hotspot Question

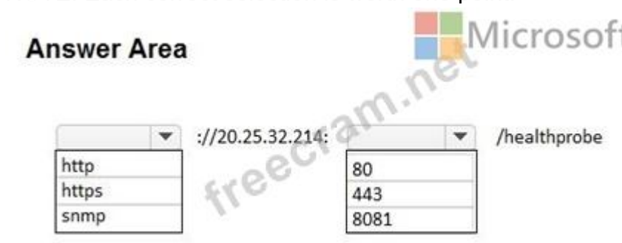
You have an Azure subscription that contains a virtual network gateway named VNetGwy1.

VNetGwy1 has a public IP address of 20.25.32.214.

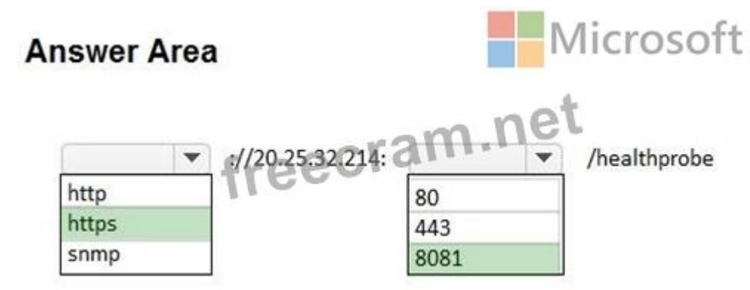
You need to query the health probe of VNetGwy1.

How should you complete the URI? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



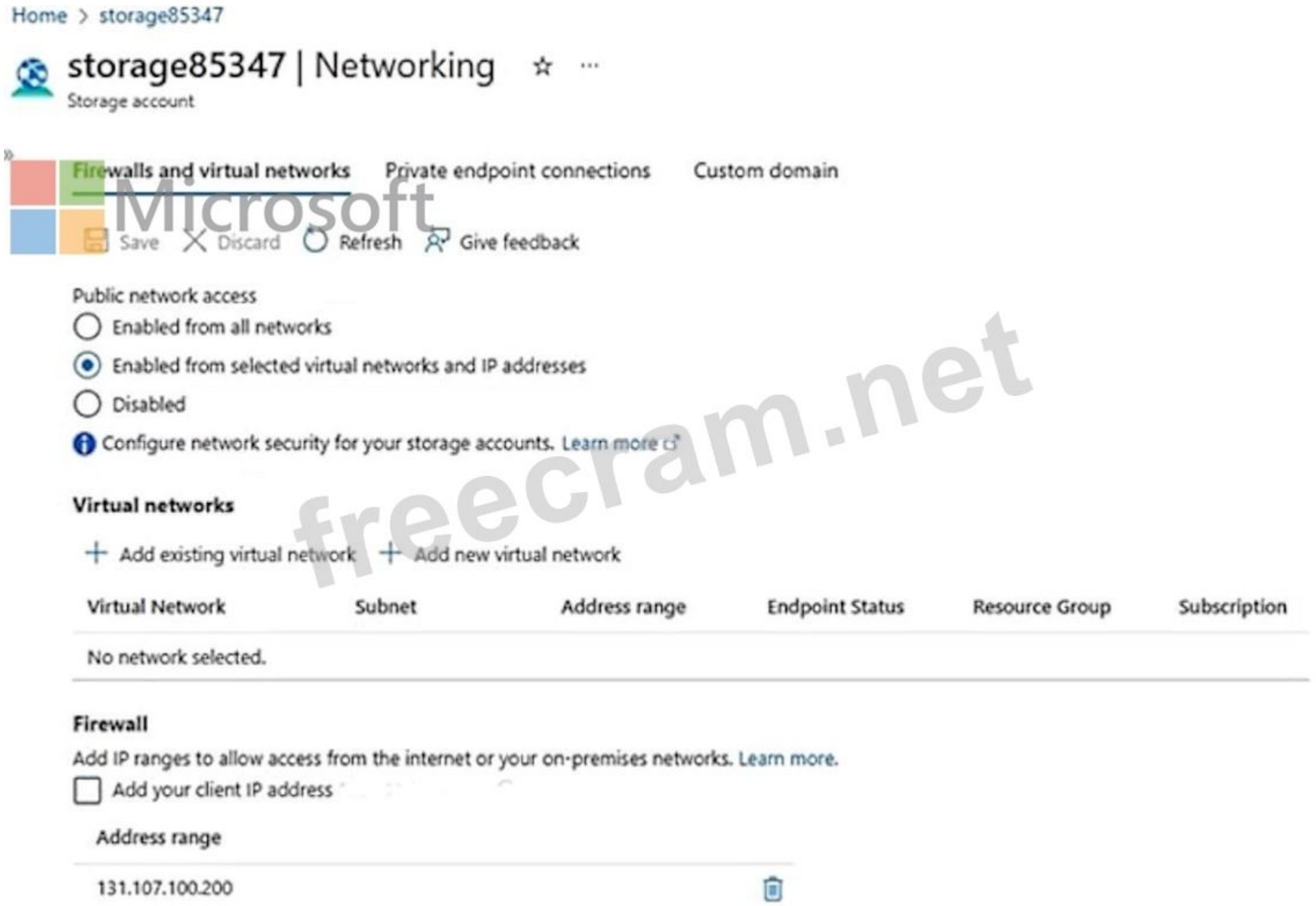
Explanation:
https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-troubleshoot-site-to-site-cannot-connect#step-7-verify-the-azure-gateway-health-probe

NEW QUESTION: 26
Hotspot Question
You have an on-premises server named Server that is assigned a public IP address of 131.107.100.200.
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
storage85347	Storage account	Accessible from anywhere
VNet1	Virtual network	Contains two subnets named Subnet1 and Subnet2
Subnet1	Subnet	Contains 50 Azure virtual machines
Subnet2	Subnet	Contains 50 Azure virtual machines

freecram.net Microsoft

storage85347 has the Networking settings configured as shown in the following exhibit.



From the Firewalls and virtual networks tab, you add Subnet1 to storage85347.

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

NOTE: Each correct selection is worth one point.

Microsoft
freecram.net

Answer Area

Statements	Yes	No
A service endpoint is created on VNet1.	○	○
All the virtual machines can access storage85347.	○	○
An additional route is created automatically in the route table of Subnet1.	○	○

freecram.net

Answer:

Answer Area

Statements	Yes	No
A service endpoint is created on VNet1.	○	○
All the virtual machines can access storage85347.	○	○
An additional route is created automatically in the route table of Subnet1.	○	○

Microsoft
freecram.net

NEW QUESTION: 27

Drag and Drop Question

You have deployed various applications using Azure Virtual Machines (VMs) in your company's Azure environment. You are seeing some suspicious activities happening on the VMs. You already use a Network Security Group (NSG) to restrict access to some of the VMs.

To identify suspicious network traffic, you have decided to enable NSG flow logs to gather more information.

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

Enable NSG flow log.

Create a storage account.

Register the Microsoft.Insights provider.

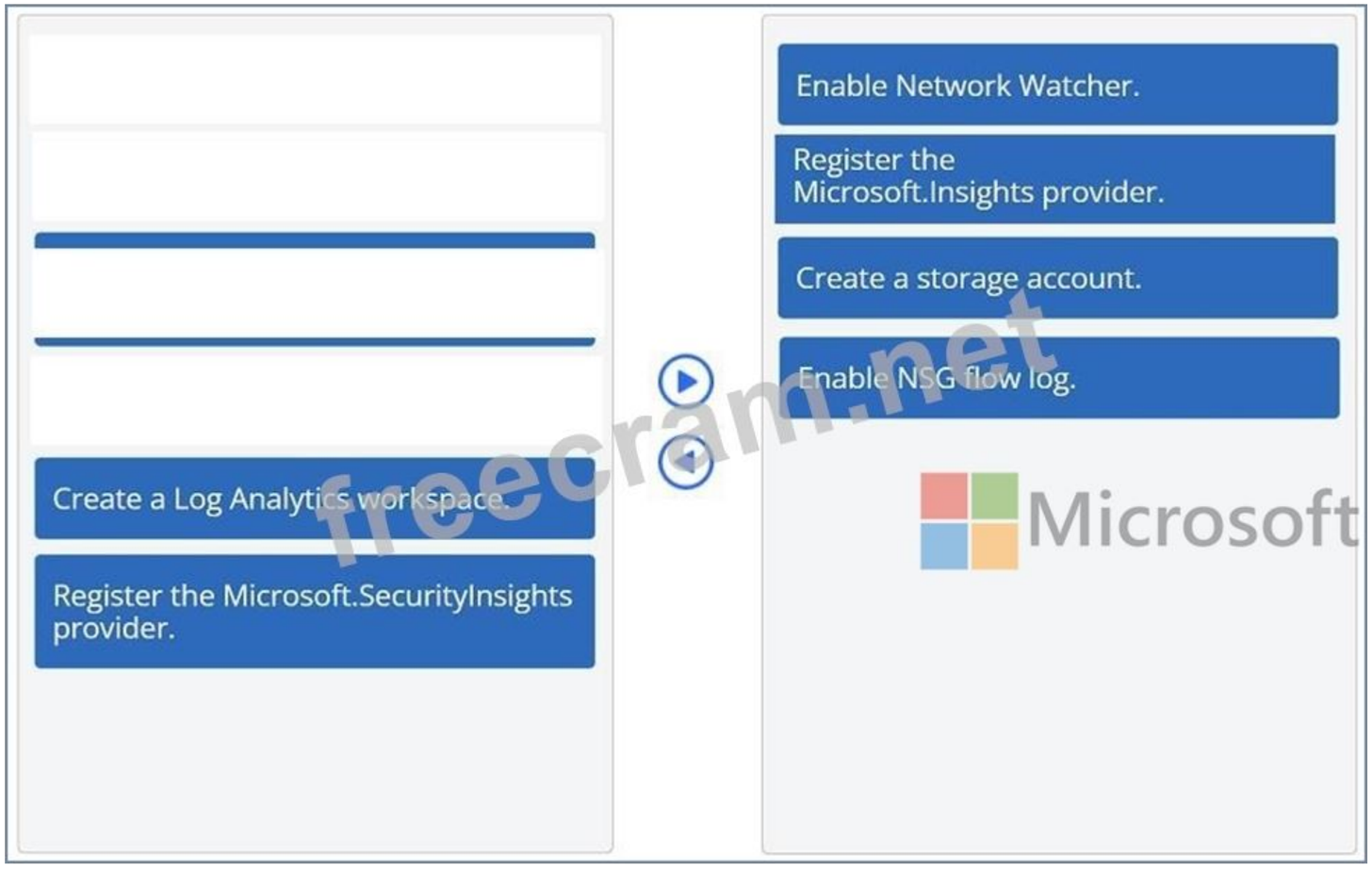
Enable Network Watcher.

Create a Log Analytics workspace.

Register the Microsoft.SecurityInsights provider.

freecram.net

Answer:



Explanation:

To enable NSG flow logs, you should enable Network Watcher in the region where your VMs are deployed. Network Watcher provides tools to monitor and collect metrics and logs from your Azure resources deployed inside a Virtual Network. Currently, Network Watcher only supports IaaS (Infrastructure as a Service) and is not intended to be used with PaaS (Platform as a Service) resources.

You should register the Microsoft.Insights provider. NSG flow logs use Azure Monitor internally to collect the logs and metrics. You should enable the Microsoft.Insights provider for the subscription where the resources are deployed.

To store the flow logs, you should create a storage account. This storage account should be in the same region and all the logs collected from NSG will be shipped to the storage account. The logs are stored in JSON format and can be viewed by downloading the files locally or shipping the files to a Security Information and Event Management system (SIEM) or an Intrusion Detection System (IDS).

You should also enable NSG flow logs. Once the flow logs are enabled, you can go and check the logs in the insights-logs-networksecuritygroupflowevent container in your storage account. In the container, navigate the folder hierarchy to find the JSON file. It follows the following naming convention for the folder hierarchy:

https://{storageAccountName}.blob.core.windows.net/insights-logs-networksecuritygroupflowevent/resourceId=/SUBSCRIPTIONS/{subscriptionID}/RESOURCEGR OUPS/{resourceGroupName}/PROVIDERS/MICROSOFT.NETWORK/NETWORKSECURITYGR OUPS/{nsgName}/y={year}/m={month}/d={day}/h={hour}/m=00/macAddress={macAddress}/PT1H.json

You should not create a Log Analytics workspace. There is another Azure service called Azure Traffic Analytics that uses Network Watcher NSG flow logs from Log Analytics to provide insights on the traffic flow. NSG flow logs can be simultaneously shipped to Log Analytics and a storage account.

You should not register the Microsoft.SecurityInsights provider. This provider is used by Microsoft Sentinel (formerly, Azure Sentinel), which is a cloud-based SIEM managed by Azure.

NEW QUESTION: 28
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
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal#site

NEW QUESTION: 29
Case Study 3 - Contoso, Ltd
Overview
Proseware, Inc. is a financial services company that has a main office in New York City and a branch office in San Francisco.
Existing Environment. Hybrid Environment
Proseware has an on-premises Active Directory Domain Services (AD DS) forest named corp.proseware.com that syncs with a Microsoft Entra tenant named proseware.com.
Proseware has an Azure subscription that is linked to proseware.com.
Proseware has an internal certification authority (CA).
Existing Environment. Network Infrastructure
The offices contain the resources shown in the following table.

Name	Type	Office	Description
NYCNet	On-premises network	New York City	IP address space of 192.168.0.0/22
SFONet	On-premises network	San Francisco	IP address space of 192.168.100.0/22
NYCDNS1	Server	New York City	DNS server that runs Windows Server 2019 and has an IP address of 192.168.0.100

NYCNet connects to Azure by using an ExpressRoute circuit.
SFONet connects to Azure by using a Site-to-Site (S2S) VPN.
Existing Environment. Azure Resources
The Azure subscription contains the virtual networks and subnets shown in the following table.

Name	Type	Location	Description
HubVNet	Virtual network	East US Azure region	IP address space of 10.0.0.0/20 peered to SpokeVNet
SpokeVNet	Virtual network	East US Azure region	IP address space of 10.0.16.0/20 peered to HubVNet
VPNGW1	Virtual network gateway	HubVNet	Active-passive resiliency, in the Generation 2, VpnGw3 SKU that has the default ASN connected to SFONet
SUBNET-PE	Subnet	HubVNet	Used for private endpoints
SUBNET-JUMPHOSTS	Subnet	HubVNet	Used for jump hosts
SUBNET-APPGW1	Subnet	SpokeVNet	Contains an Azure application gateway named APPGW1

The subscription contains four virtual machines named VM1, VM2, VM3, and VM4. VM1 and VM2 host an app named App1.

VM3 and VM4 host a web app named App2 that is accessed by using a FQDN of app2.proseware.com. Users access app2.proseware.com by using HTTP or HTTPS.

VM1, VM2, and VM4 are connected to SpokeVNet.

The subscription contains Application Gateway resources shown in the following table.

Name	Type	Location	Description
APPGW1	Application Gateway	SpokeVNet	In the Azure Web Application Firewall (WAF) V2 SKU Terminates HTTPS connections to a backend pool that contains VM3 and VM4
APPGW1-NSG1	Network security group (NSG)	East US region	Associated with SUBNET-APPGW1
APPGW1-WAFPolicy	Azure Web Application Firewall (WAF) policy	East US region	Applied to APPGW1

The subscription contains an Azure Front Door Standard profile named FD1. FD1 contains a single origin group that targets APPGW1 by using the default endpoint name.

HubVNet connects to NYCNet by using an ExpressRoute gateway named ERGW1.

Planned Changes and Requirements. Planned Changes

Proseware plans to implement the following changes:

- Deploy an Azure Private DNS Resolver named PRDNS1 to HubVNet and link PRDNS1 to SpokeVNet.
- Create a DNS forwarding ruleset named DNSRS1 and associate DNSRS1 with PRDNS1.
- Deploy Azure Virtual Network Manager and implement the following rules:
- Allow inbound connections on TCP port 3389 from the on-premises networks to SUBNET- JUMPHOSTS.
- Block inbound connections on TCP port 80 from the internet to SpokeVNet.
- Ensure that Azure Virtual Network Manager rules take precedence over conflicting NSG rules.
- Deploy two network virtual appliances (NVAs) named NVA1 and NVA2 to HubVNet.
- Deploy a gateway load balancer named LBGW1 to HubVNet.
- Configure LBGW1 to inspect traffic on TCP ports 443, 1433, and 1434 from LBS1 by using NVA1 and NVA2.
- Ensure that all the traffic to App2 is processed by using FD1.

Planned Changes and Requirements. Connectivity requirements

Proseware identifies the following connectivity requirements:

- Minimize the complexity of the Azure Virtual Network Manager deployment.
- Route traffic between NYCNet and SFONet via the ExpressRoute circuit and the S2S VPN.
- Ensure that remote users on Windows 11 devices can connect to HubVNet by using a Point-to- Site (P2S) VPN and their proseware.com credentials.

Planned Changes and Requirements. Security requirements

Proseware identifies the following security requirements:

- Whenever possible, use the internal CA.
- Ensure that all connections routed via APPGW1 use end-to-end encryption.
- Ensure that user connections to Azure-hosted apps use end-to-end encryption.
- Ensure that all inbound internet traffic to app2.proseware.com is routed via FD1.
- Prevent devices that connect to NYCNet from accessing Azure services that use private endpoints.
- Enable the virtual machines that connect to HubVNet and SpokeVNet to access Azure services that use private endpoints.

Planned Changes and Requirements. General requirements

Proseware identifies the following general requirements:

- Minimize the IP address space required to deploy platform-managed resources to the virtual networks.
- From SpokeVNet, resolve name resolution requests for the azure.proseware.com namespace and the corp.proseware.com namespace by using PRDNS1.
- Whenever possible, minimize administrative effort.

You need to configure APPGW1 to support end-to-end encryption. The solution must meet the security requirements.

What should you do?

A. From the Backend settings, upload the internal root CA certificate.

B. From the SSL settings, upload a TLS client certificate that is issued by the internal root CA.

C. From the Backend settings, upload a wildcard TLS certificate that has a private key issued by the internal root CA.

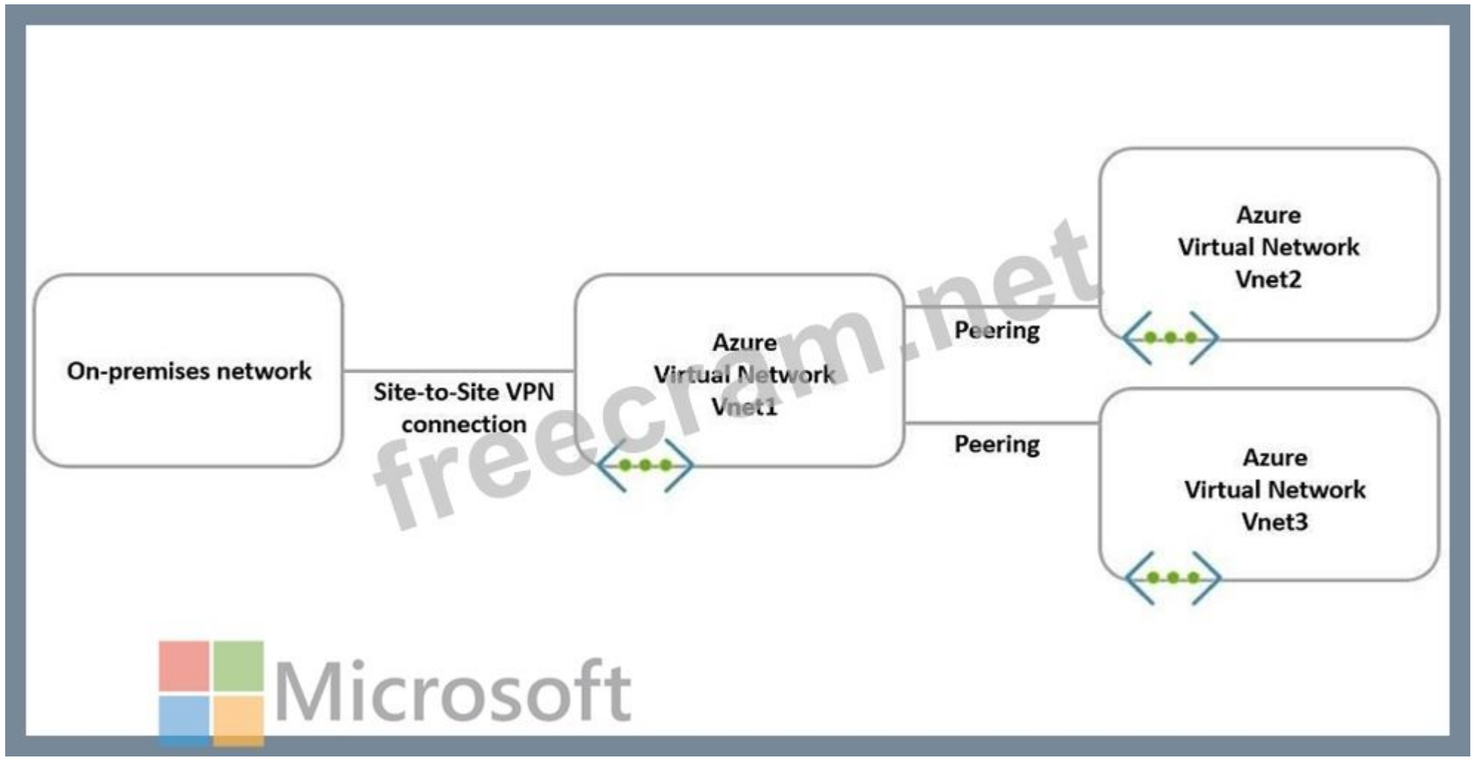
D. From the SSL settings, upload a TLS client certificate that is issued by the internal root CA and includes the full certificate chain.

Answer: (SHOW ANSWER)

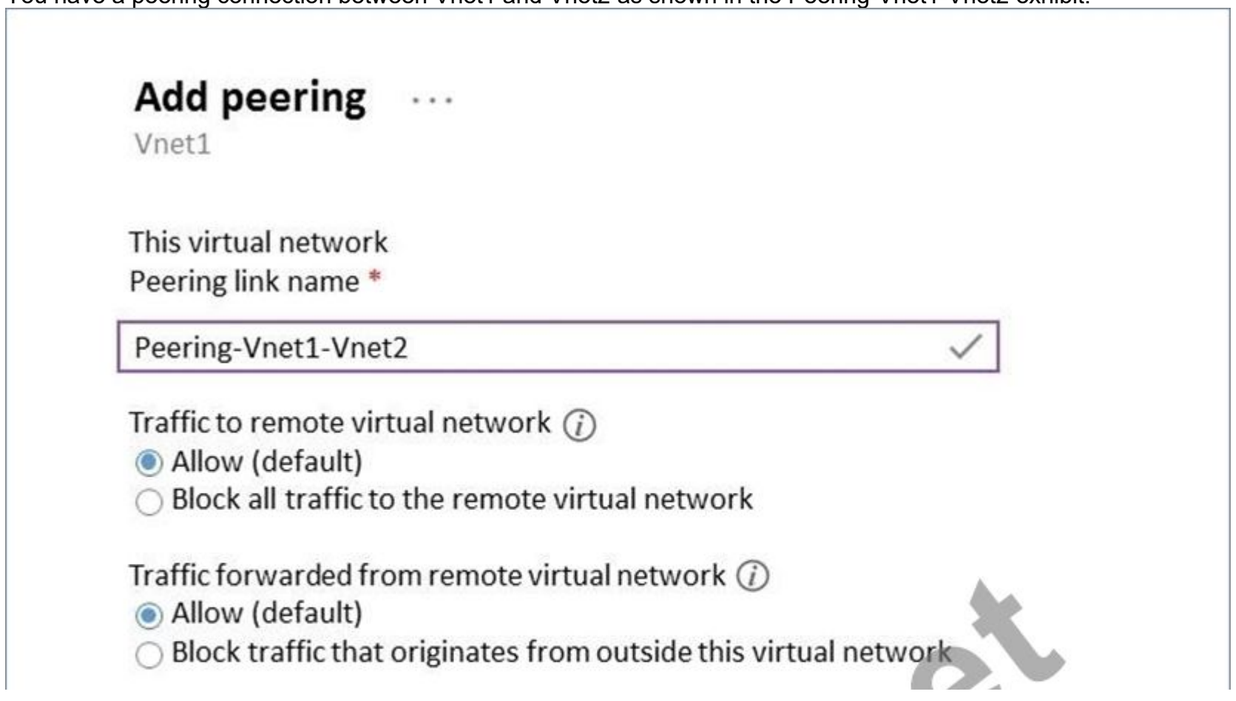
NEW QUESTION: 30

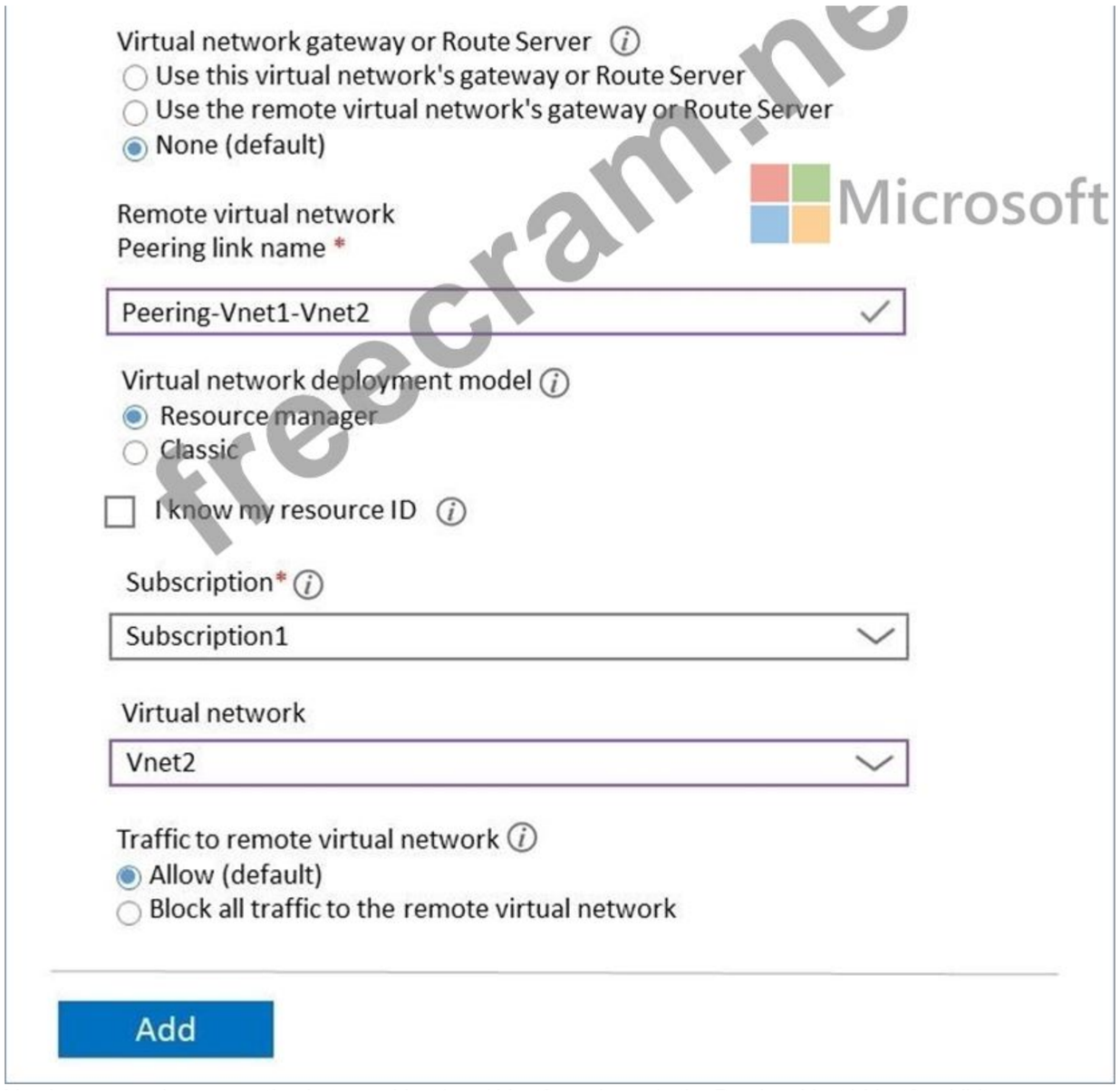
Hotspot Question

You have the hybrid network shown in the Network Diagram exhibit.



You have a peering connection between Vnet1 and Vnet2 as shown in the Peering-Vnet1-Vnet2 exhibit.





freecram.net
Microsoft

You have a peering connection between Vnet1 and Vnet3 as shown in the Peering -Vnet1-Vnet3 exhibit.



Traffic to remote virtual network ⓘ
- (•) Allow (default)
- ( ) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
- (•) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ
- ( ) Use this virtual network's gateway or Route Server
- ( ) Use the remote virtual network's gateway or Route Server
- (•) None (default)

Remote virtual network
Peering link name *

Peering-Vnet1-Vnet3

Virtual network deployment model ⓘ
- (•) Resource manager
- ( ) Classic

[ ] I know my resource ID ⓘ

Subscription* ⓘ

Subscription1

Virtual network

Vnet1

Traffic to remote virtual network ⓘ
- (•) Allow (default)
- ( ) Block all traffic to the remote virtual network

Traffic to remote virtual network
- (•) Allow (default)
- ( ) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network
- (•) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server
- ( ) Use this virtual network's gateway or Route Server
- ( ) Use the remote virtual network's gateway or Route Server
- (•) None (default)

freecram.net
Microsoft

Add

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

NOTE: Each correct selection is worth one point.

Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	○	○
The resources in Vnet2 can communicate with the resources in Vnet3.	○	○
The resources in Vnet2 can communicate with the resources in the on-premises network.	○	○

freecram.net
Microsoft

Answer:

Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	○	○
The resources in Vnet2 can communicate with the resources in Vnet3.	○	○
The resources in Vnet2 can communicate with the resources in the on-premises network.	○	○

freecram.net
Microsoft

Explanation:

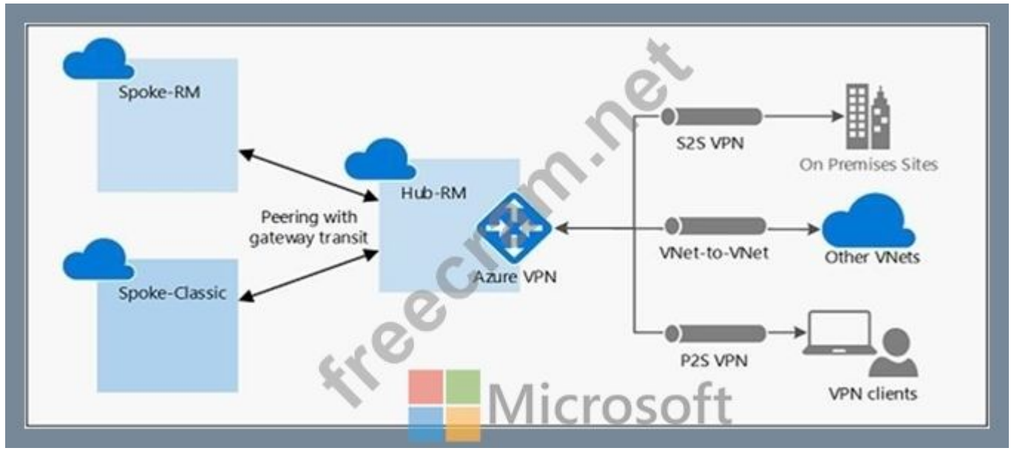
Box 1: Yes

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes.

Box 2: No

No Virtual Gateway is used.

Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity. The following diagram shows how gateway transit works with virtual network peering.



In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual networks.

Box 3: No

No Virtual Gateway is used.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

NEW QUESTION: 31

SIMULATION



Username and password

Use the following login credentials as needed:

- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com

- Azure Password: xxxxxxxxxx

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:

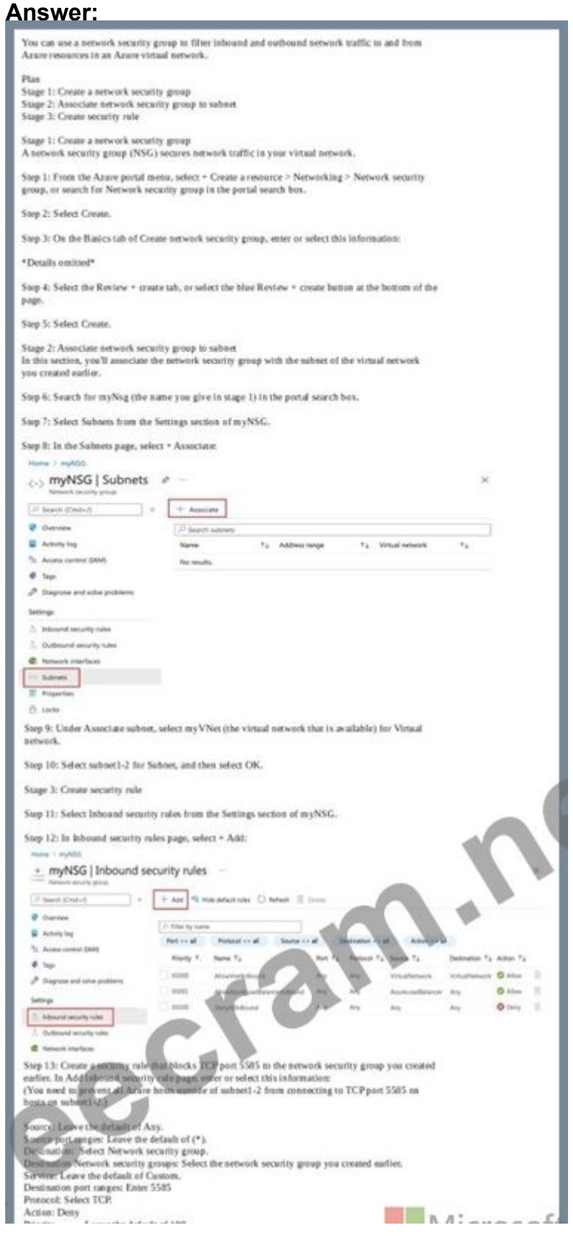
- Lab Instance: 12345678

You plan to deploy several virtual machines to subnet1-2.

You need to prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts on subnet1-2. The solution must minimize administrative effort.

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

Answer:



You can use a network security group to filter inbound and outbound network traffic to and from Azure resources in an Azure virtual network.

Plan
Stage 1: Create a network security group
Stage 2: Associate network security group to subnet
Stage 3: Create security rule

Stage 1: Create a network security group
A network security group (NSG) secures network traffic in your virtual network.

Step 1: From the Azure portal menu, select + Create a resource > Networking > Network security group, or search for Network security group in the portal search box.

Step 2: Select Create.

Step 3: On the Basics tab of Create network security group, enter or select this information:

Details omitted

Step 4: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 5: Select Create.

Stage 2: Associate network security group to subnet
In this section, you'll associate the network security group with the subnet of the virtual network you created earlier.

Step 6: Search for myNsg (the name you give in stage 1) in the portal search box.

Step 7: Select Subnets from the Settings section of myNSG.

Step 8: In the Subnets page, select + Associate.

Step 9: Under Associate subnet, select myVNet (the virtual network that is available) for Virtual network.

Step 10: Select subnet1-2 for Subnet, and then select OK.

Stage 3: Create security rule

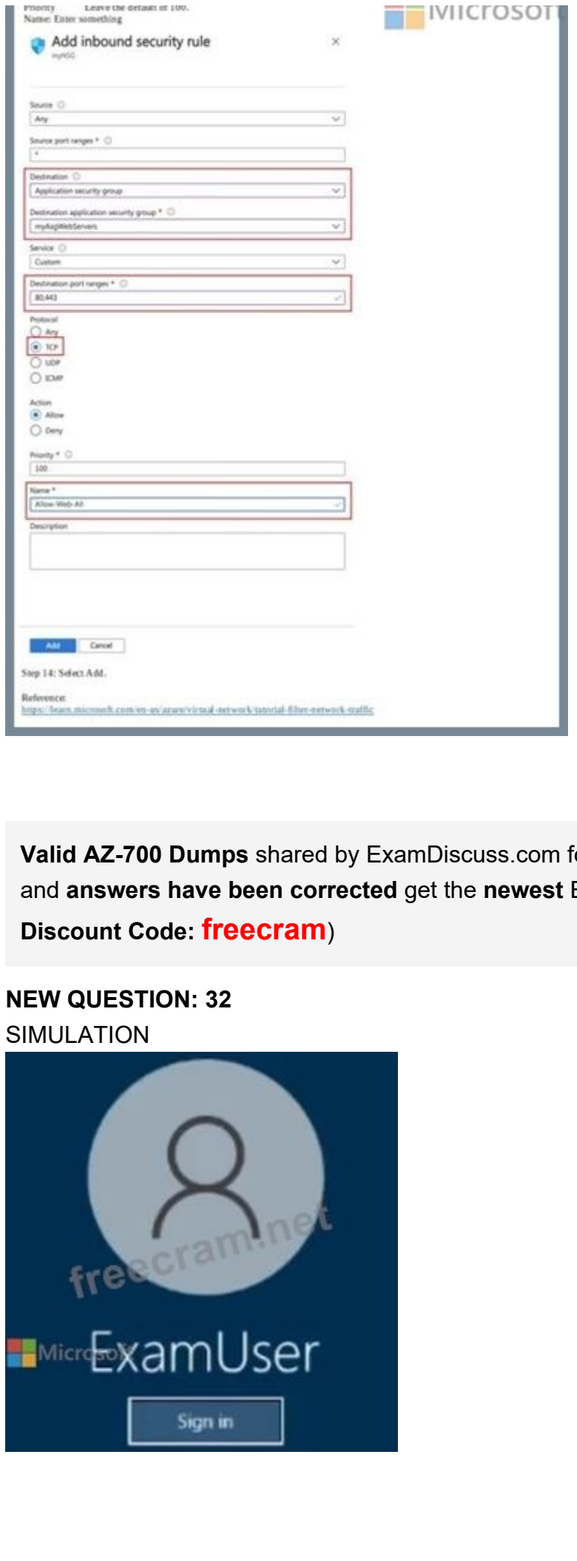
Step 11: Select Inbound security rules from the Settings section of myNSG.

Step 12: In Inbound security rules page, select + Add.

Step 13: Create a security rule that blocks TCP port 5585 to the network security group you created earlier. In Add inbound security rule page, enter or select this information:
(You need to prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts on subnet1-2.)

Source: Leave the default of Any.
Source port ranges: Leave the default of (*).
Destination: Select Network security group.
Destination Network security groups: Select the network security group you created earlier.
Service: Leave the default of Custom.
Destination port ranges: Enter 5585
Protocol: Select TCP.
Action: Deny

ecram.n



Step 14: Select Add.

Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
SIMULATION

Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
- If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You need to ensure that the storage12345678 storage account will only accept connections from the hosts on VNET1.

Azure storage account accepts connections from Virtual network.

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

Link the private endpoint to the existing storage account
Step 1: In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.

Step 2: Select or Search&find storage account storage12345678

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

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

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

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

Step 7: Select Next: Resource.

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

Step 9: Select Next: Virtual Network.

Step 10: In Virtual Network, enter or select:
* Virtual network: VNET1.

Microsoft
freecram.net

Step 11: Select Next: DNS.

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

Step 13: Select Create.

Back in the setting of settings of the Storage Account.

Step 14: Save.

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

NEW QUESTION: 33
You have an Azure subscription that contains the virtual networks shown in the following table.

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

speecram.net
Microsoft

You plan to deploy an Azure firewall named AF1 to RG1 in the West US Azure region.
To which virtual networks can you deploy AF1?
A. Vnet1 only
B. Vnet1 and Vnet2 only
C. Vnet1, Vnet2, and Vnet4 only
D. Vnet1 and Vnet4 only
E. Vnet1, Vnet2. Vnet3, and Vnet4
Answer: (SHOW ANSWER)
Azure Firewall operates in a single VNET.
Azure Firewall is a regional service.
Yes. Vnet1: Same VNET and same region.
No. Vnet2: Same Resource Group but different VNET and different region. Must be in the same region.
No. Vnet3: Different VNET, different region. Must be in the same region.
No. Vnet4: Different VNET, same region.
Reference:
https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-framework-azure-firewall

NEW QUESTION: 34

Case Study 1 - Litware. Inc

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-prernises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by usinq Azure AD Connect.

All the offices connect to a virtual network named Vnetl by using a Site-to-Site VPN connection.

Azure Environment

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

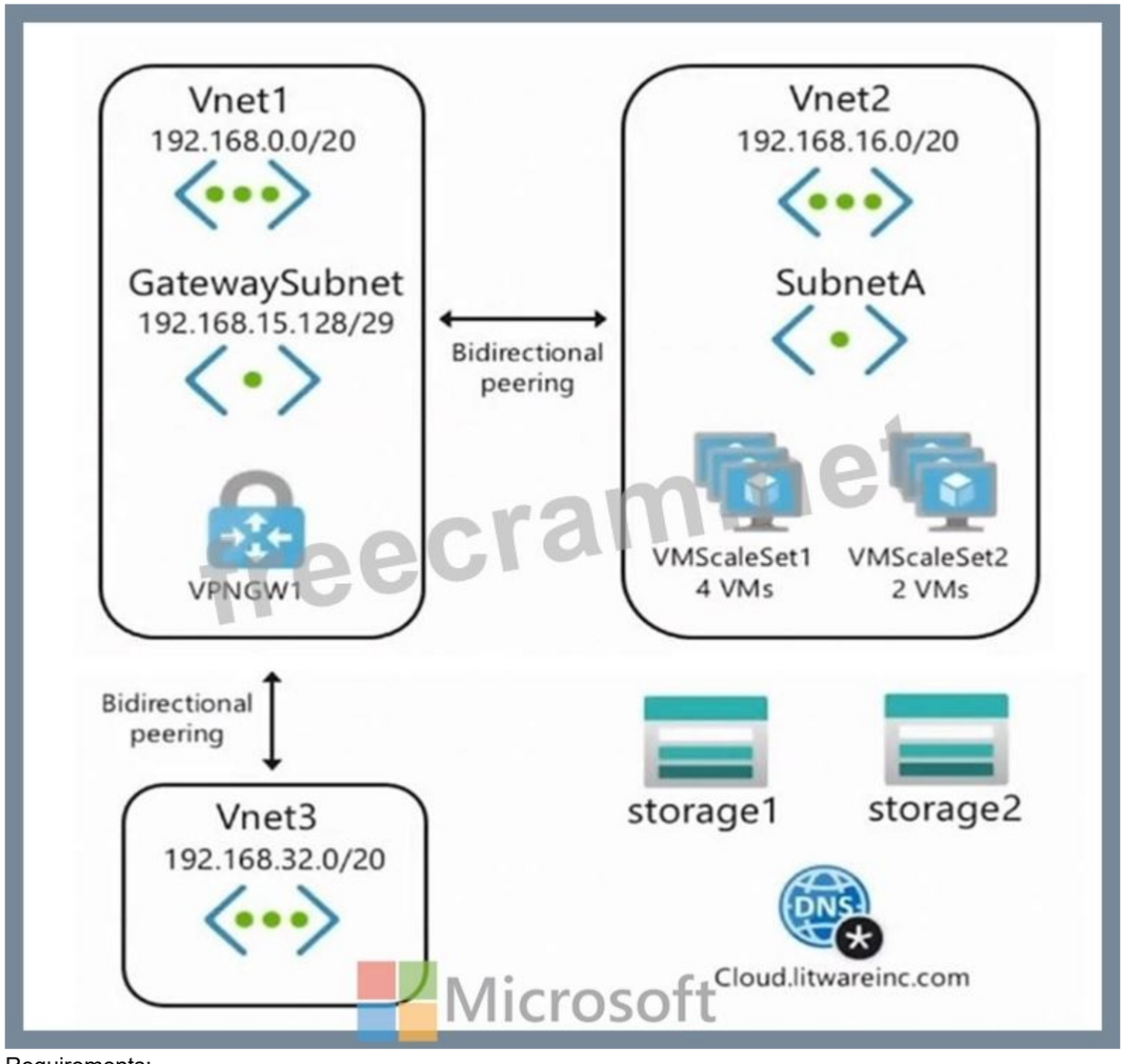
ces in the East US Azure region as shown in the following table.

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

freecram.net Microsoft



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 zone 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):

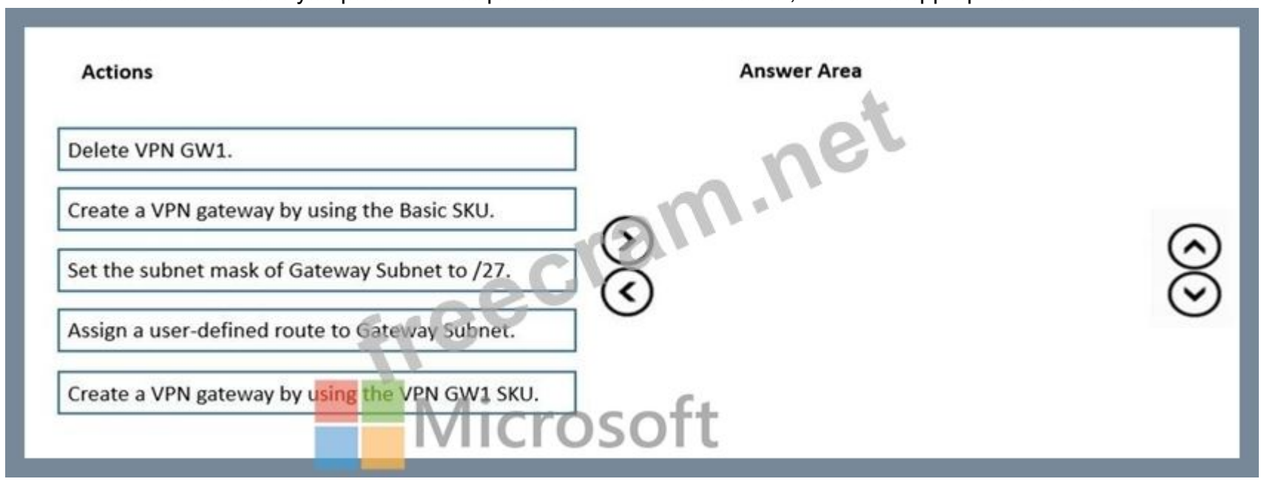
- The storage1 account must be accessible from all on-premises
locations without exposing the public endpoint of storage1.
- The storage2 account must be accessible from Vnet2 and Vnet3 without
exposing the public endpoint of storage2.

Drag and Drop Question

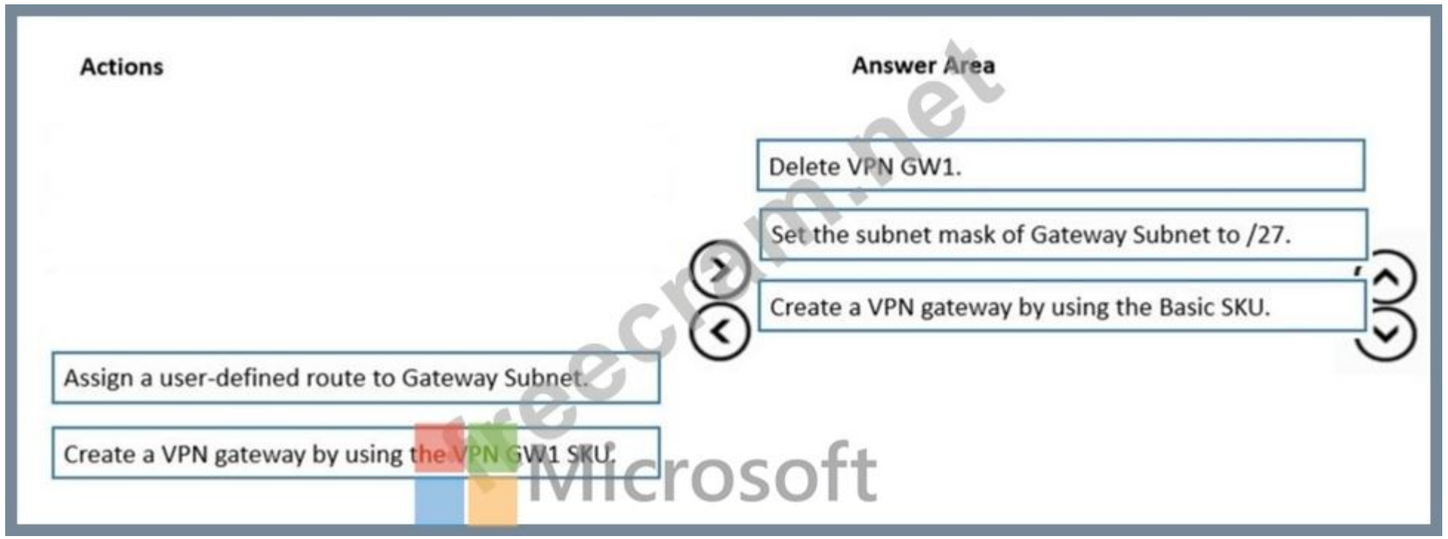
You need to prepare Vnet1 for the deployment of an ExpressRoute gateway.

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.



Answer:



Explanation:

Step 1: Delete the VPN GW1.

The existing VPN GW1 GatewaySubnet is too small with /29.

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.

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

Step 2: Set the subnet mask of Gateway Subnet to /27.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We [Microsoft] recommend that you create a gateway subnet that uses a /27 or /28.

It's best to specify /27 or larger (/26,/25 etc.). This allows enough IP addresses for future changes, such as adding an ExpressRoute gateway.

Step 3: Create a VPN gateway by using Basic SKU.

Basic SKU is good enough.

Note:

The Basic gateway SKU does not support IKEv2 or RADIUS authentication. If you plan on having Mac clients connect to your virtual network, do not use the Basic SKU.

Reference:

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

NEW QUESTION: 35

Case Study 1 - Litware. Inc

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-prernises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by usinq Azure AD Connect.

All the offices connect to a virtual network named Vnetl 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.

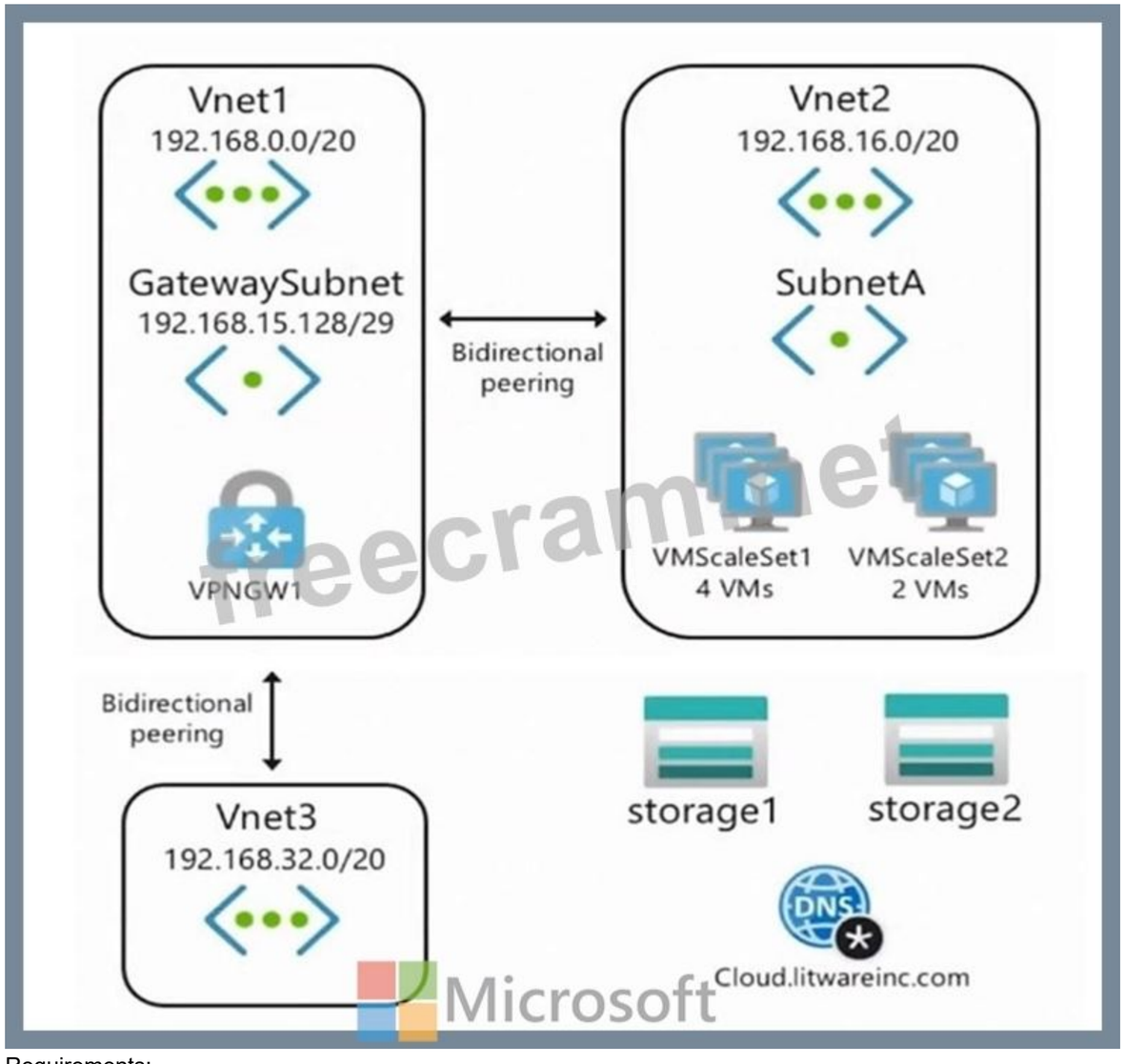
Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	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

freecram.net



Requirements:

Business Requirements

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

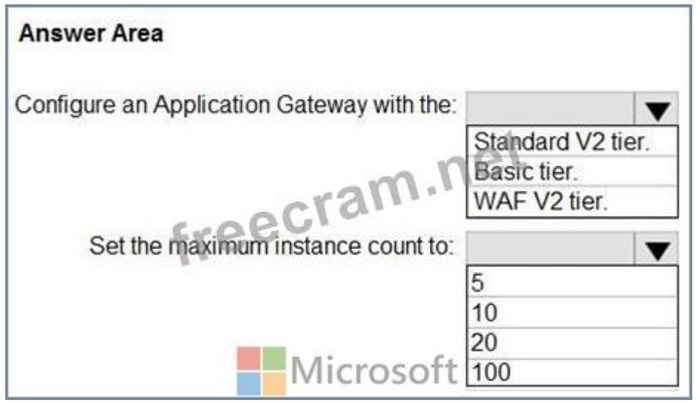
Virtual Networking Requirements

Litware identifies the following virtual networking requirements:

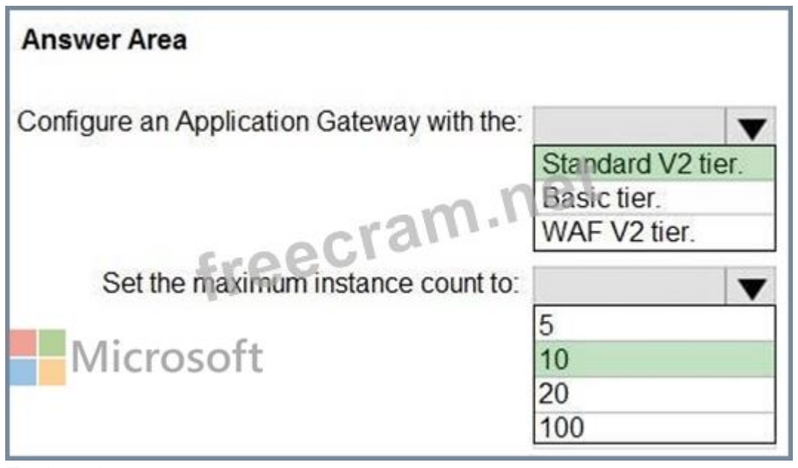
- Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.
- Ensure that the records in the cloud.litwareinc.com zone can be resolved from the on-premises locations.
- Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com 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.
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
Answer: (SHOW ANSWER)
Azure Service Endpoint provides secure and direct connectivity to Azure PaaS services over an optimized route over the Azure backbone network.
Traffic still left your VNet and hit the public endpoint of PaaS service. ==> Then it can't meet the goal because of the public IP.
Azure Private Link (or Private Endpoint) allows you to access Azure PaaS services over Private IP address within the VNet.

NEW QUESTION: 36
Hotspot Question
You have an Azure subscription.
You plan to deploy an app named App1 that will be accessed by using Azure Application Gateway.
You need to deploy the application gateway for App1. The solution must meet the following requirements:
- Support autoscaling to 100 capacity units.
- Minimize costs.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:

Box 1: Standard V2 tier

The Azure Application Gateway Standard_v2 and WAF_v2 tiers support autoscaling and can scale up to 125 capacity units. Each capacity unit can handle a certain number of persistent connections, and additional capacity units are added as limits are reached.

The Azure Application Gateway Standard_v2 tier is generally the cheaper option compared to the WAF_v2 tier. While both tiers have a base cost per hour, the WAF_v2 tier includes additional features for web application firewalling, which is reflected in its higher hourly cost.

Box 2: 10

You must specify a minimum and optionally maximum instance count. Minimum capacity ensures that Application Gateway and WAF v2 don't fall below the minimum instance count specified, even without traffic. The minimum instance count can range from 0 to 100. Each instance is roughly equivalent to 10 more reserved Capacity Units.

Reference:

https://learn.microsoft.com/en-us/azure/application-gateway/application-gateway-autoscaling-zone-redundant

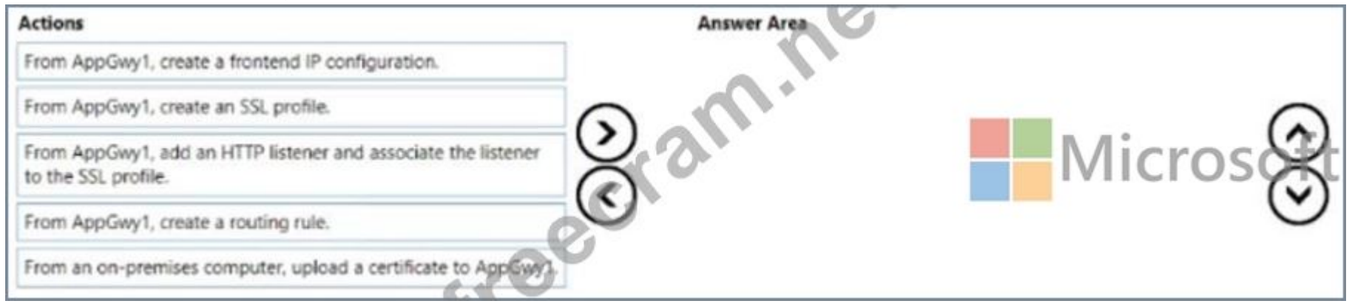
NEW QUESTION: 37

Drag and Drop Question

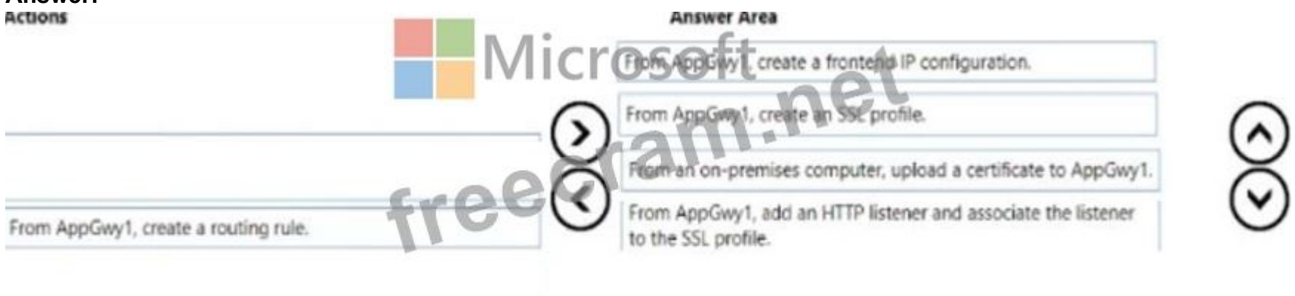
Your on-premises network contains an Active Directory Domain Services (AD DS) domain named contoso.com that has an internal certification authority (CA).

You have an Azure subscription.

You deploy an Azure application gateway named AppGwy1 and perform the following actions:
- Configure an HTTP listener
- Associate a routing rule with the listener
You need to configure AppGwy1 to perform mutual authentication for requests from domain- joined computers to contoso.com.
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.



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal

NEW QUESTION: 38
You have an Azure subscription that contains an Azure App Service web app named WebApp1 and an Azure Front Door profile named FDProfile1. FDProfile1 forwards requests addressed to https://www.contoso.com to WebApp1.
You need to ensure that only requests addressed to https://www.contoso.com/users/* are forwarded to WebApp1.
What should you modify in FDProfile1?
A. the routes
B. the origin group
C. the endpoint
D. the domain
Answer: A (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-route-matching?pivots=front-door- standard-premium

NEW QUESTION: 39
Case Study 2 - Contoso, Ltd
Overview
Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment:

Azure Network Infrastructure

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	**None**

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

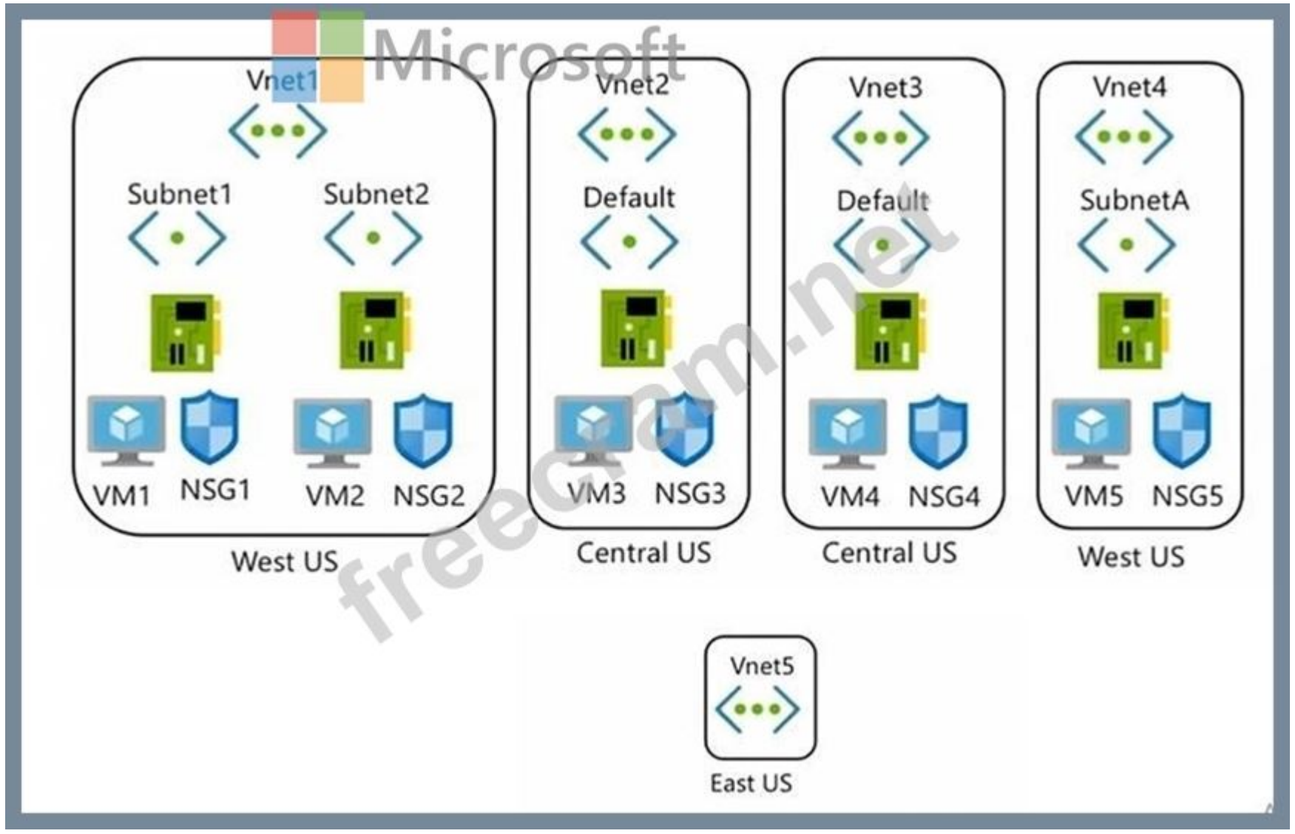
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements:

Virtual Network Requirements

Contoso has the following virtual networks requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

Two container groups that connect to Vnet6

Three virtual machines that connect to Vnet6

Allow VPN connections to be established to Vnet6

Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network

- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements

Contoso has the following network security requirements:

- Configure Azure Active Directory (Azure AD) authentication for Point- to-Site (P2S) VPN users.
- Enable NSG flow logs for NSG3 and NSG4.
- Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

- Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Hotspot Question

You create NSG10 and NSG11 to meet the network security requirements.

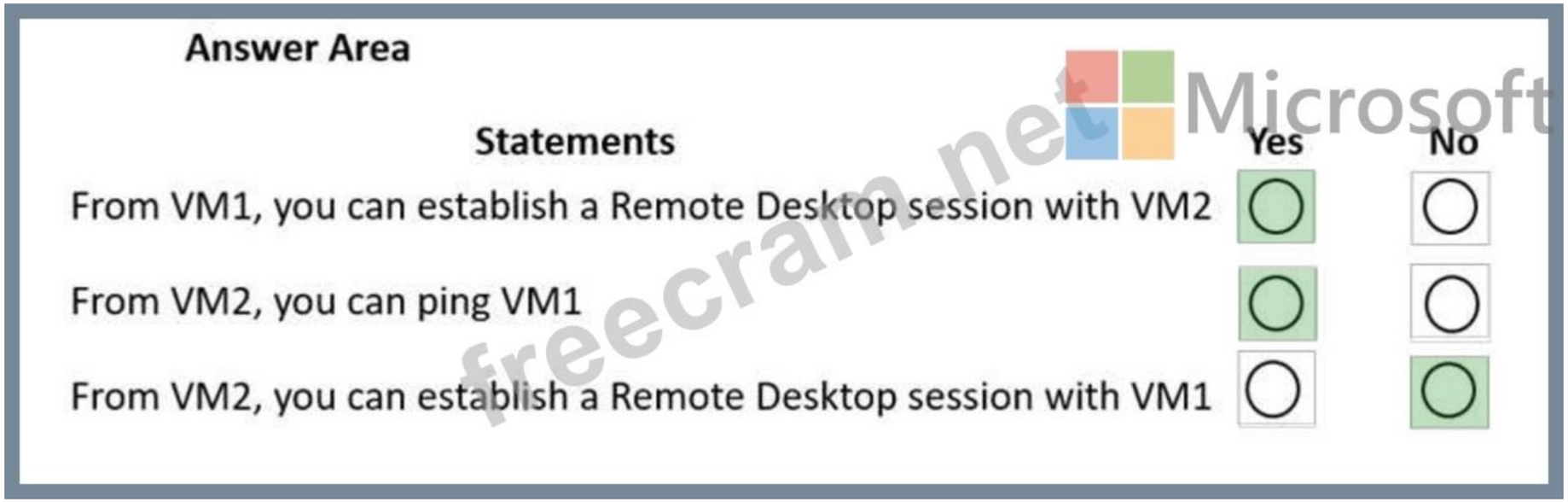
For each of the following statements, select Yes of the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

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:



Explanation:
Box 1: Yes
VM1 can establish a RDP session to VM as the filtering is set to inbound even if the rule would have matched (it would have required outbound) Box 2: Yes NSG10 blocks ICMP from VNet4 (source 10.10.0.0/16) but it is not blocked from VM2's subnet (VNet1/ Subnet2).
Box 3: 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.

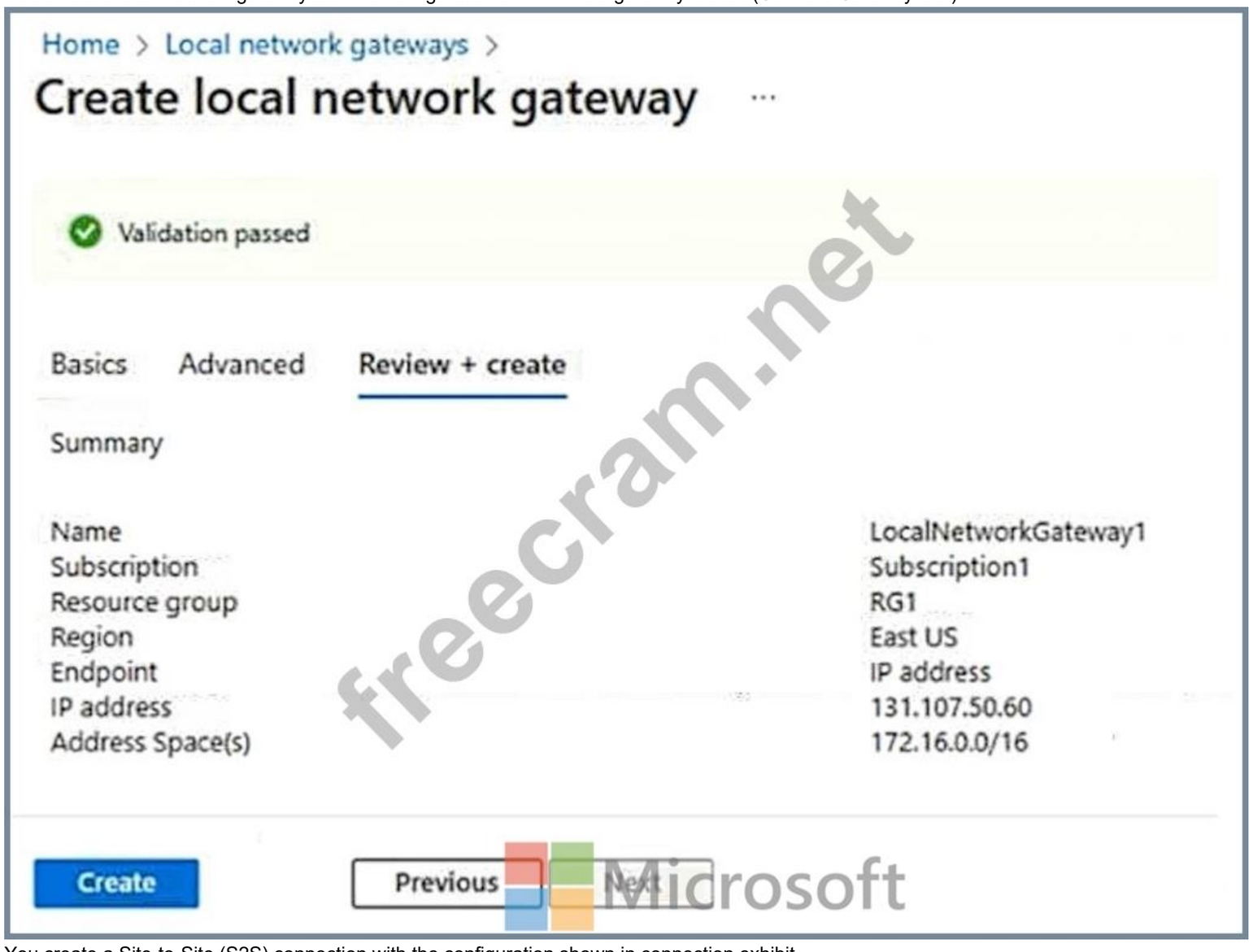
NEW QUESTION: 40
Hotspot Question
You have an on-premises network that includes the sites shown in the following table.

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 Gateway1.

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



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

(Click the Connection tab.)

Create connection ...

Validation passed

Basics Settings Tags **Review + create**

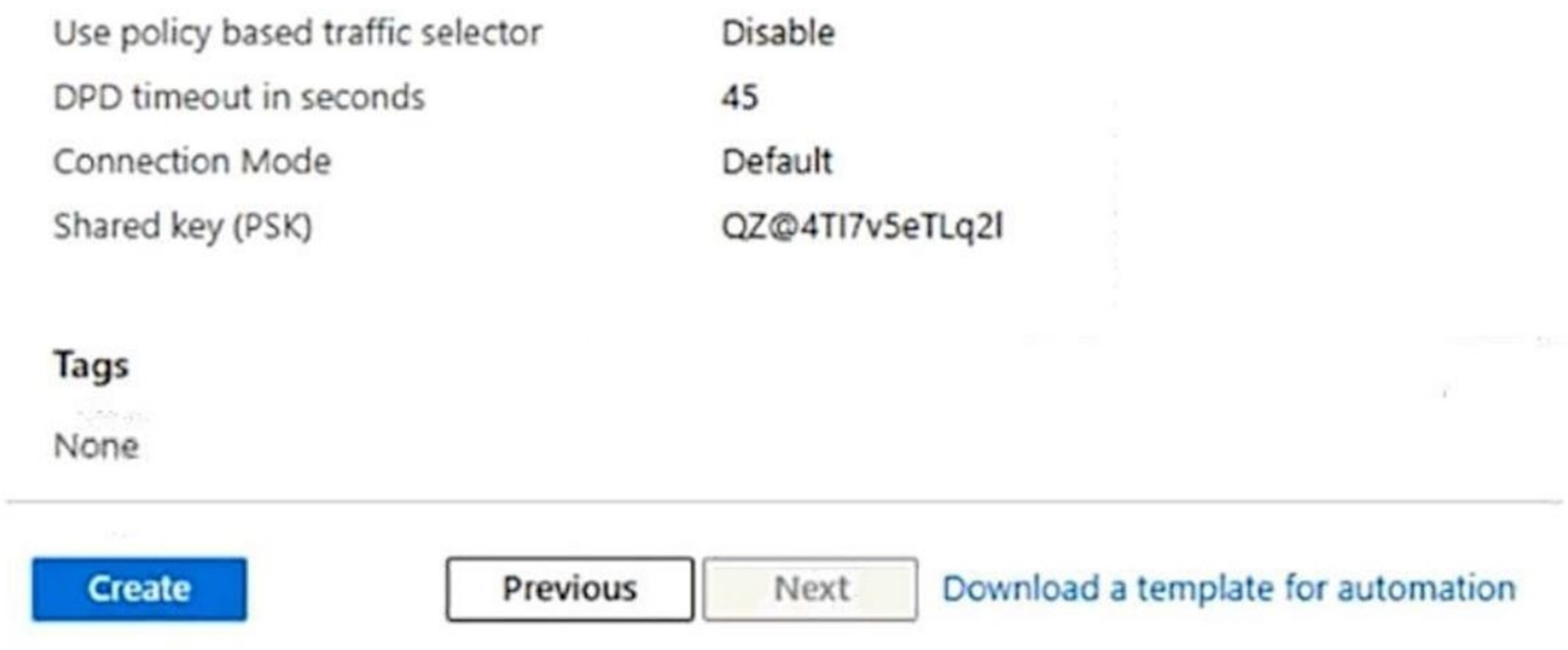
Basics

Subscription	Subscription1
Resource group	RG1
Region	East US
Connection type	Site-to-site (IPsec)
Connection name	VPN1

Settings

Virtual network gateway	Gateway1
Local network gateway	LocalNetworkGateway1
IKE Protocol	IKEv2
IPsec / IKE policy	Default

Microsoft
freecram.net



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

NOTE: Each correct selection is worth one point.

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.	○	○

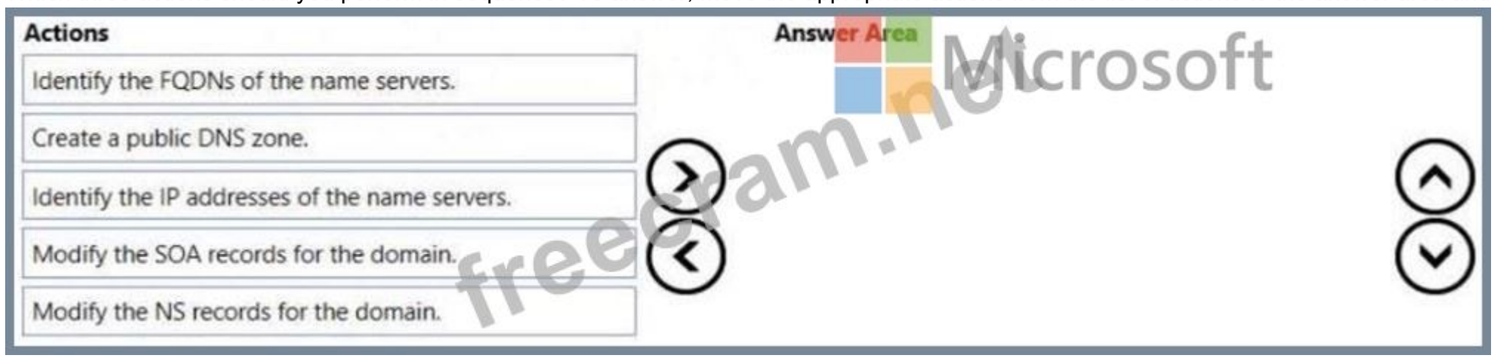
Microsoft
freecram.net

Answer:

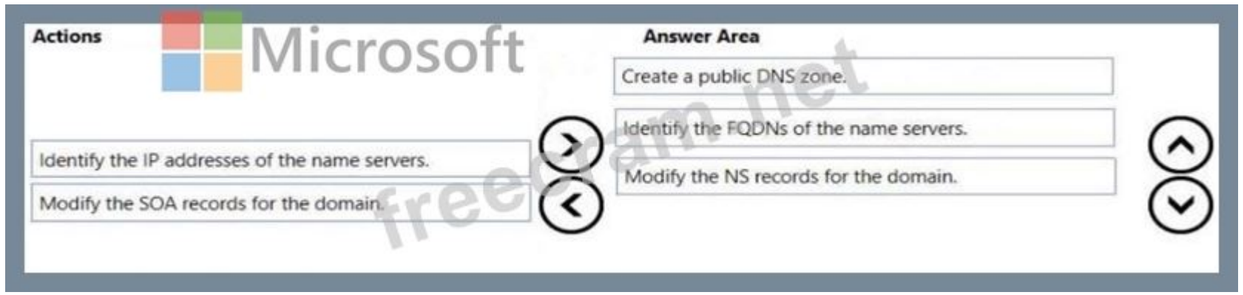


NEW QUESTION: 41
You are configuring two network virtual appliances (NVAs) in an Azure virtual network. The NVAs will be used to inspect all the traffic within the virtual network.
You need to provide high availability for the NVAs. The solution must minimize administrative effort.
What should you include in the solution?
A. Azure Standard Load Balancer
B. Azure Traffic Manager
C. Azure Application Gateway
D. Azure Front Door
Answer: A (LEAVE A REPLY)
This design uses two Azure Load Balancers to expose a cluster of NVAs to the rest of the network.
https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha?tabs=cli

NEW QUESTION: 42
Drag and Drop Question
You register a DNS domain with a third-party registrar.
You need to host the DNS zone on Azure.
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.



Answer:

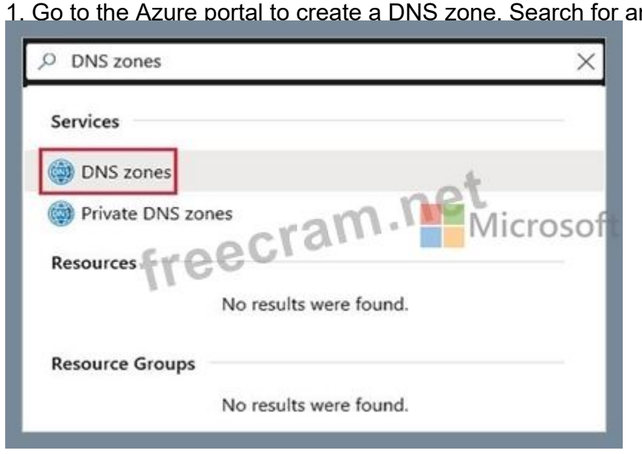


Explanation:

Step 1: Create a public DNS zone.

Create a DNS zone

1. Go to the Azure portal to create a DNS zone. Search for and select DNS zones.



2. Select Create DNS zone.

3. On the Create DNS zone page, enter the following values, and then select Create.

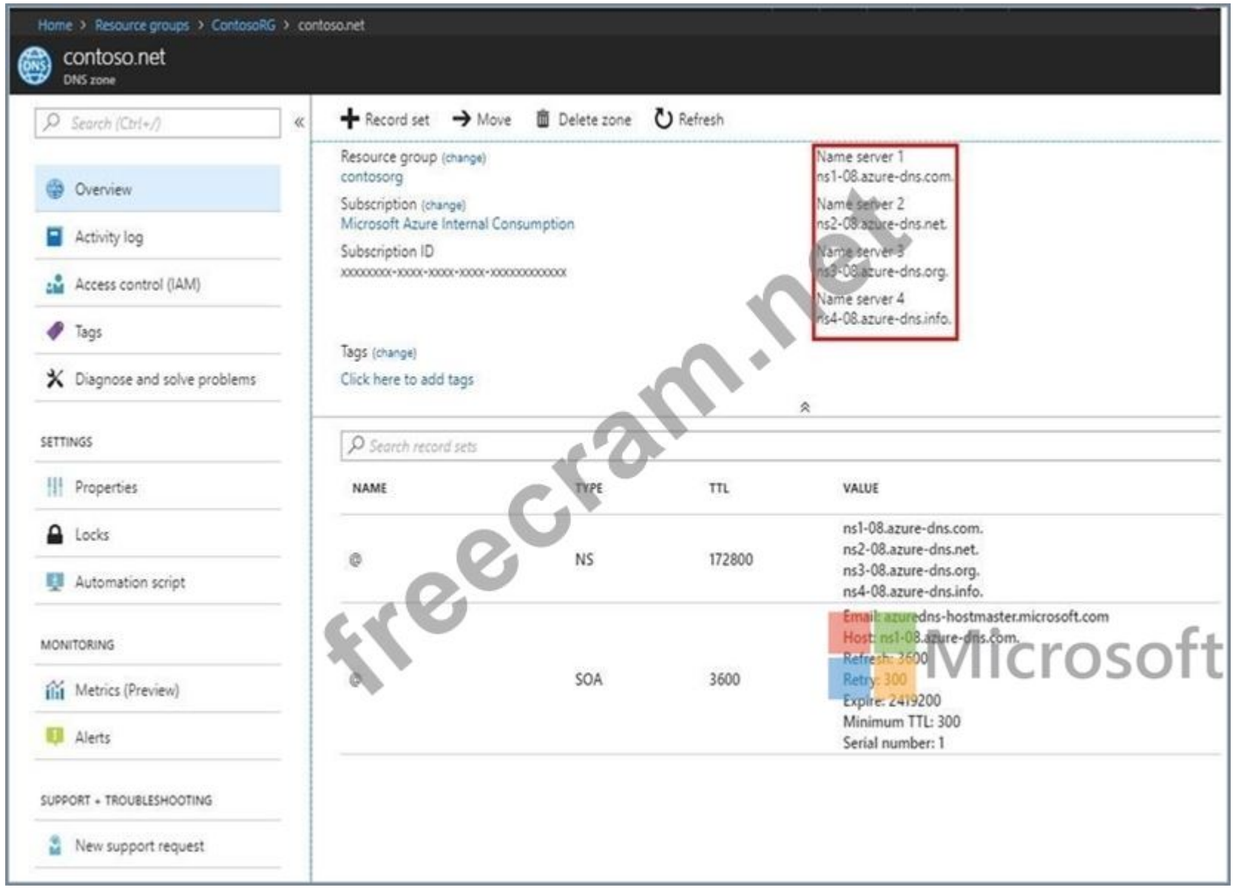
Step 2: Identify the FQDNs of the name servers.

Retrieve name servers.

Before you can delegate your DNS zone to Azure DNS, you need to know the name servers for your zone. Azure DNS gives name servers from a pool each time a zone is created.

With the DNS zone created, in the Azure portal Favorites pane, select All resources. On the All resources page, select your DNS zone. If the subscription you've selected already has several resources in it, you can enter your domain name in the Filter by name box to easily access the application gateway.

Retrieve the name servers from the DNS zone page. In this example, the zone contoso.net has been assigned name servers ns1-01.azure-dns.com, ns2-01.azure-dns.net, *ns3-01.azure-dns.org, and ns4-01.azure-dns.info:



Azure DNS automatically creates authoritative NS records in your zone for the assigned name servers.

Step 3: Modify the NS records for the domain.

Delegate the domain -

Once the DNS zone gets created and you have the name servers, you'll need to update the parent domain with the Azure DNS name servers.

Each registrar has its own DNS management tools to change the name server records for a domain.

1. In the registrar's DNS management page, edit the NS records and replace the NS records with the Azure DNS name servers.

2. When you delegate a domain to Azure DNS, you must use the name servers that Azure DNS provides. Use all four name servers, regardless of the name of your domain. Domain delegation doesn't require a name server to use the same top-level domain as your domain.

Reference:

https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns

NEW QUESTION: 43

Hotspot Question

You have an Azure subscription that contains a virtual network named VNet1.

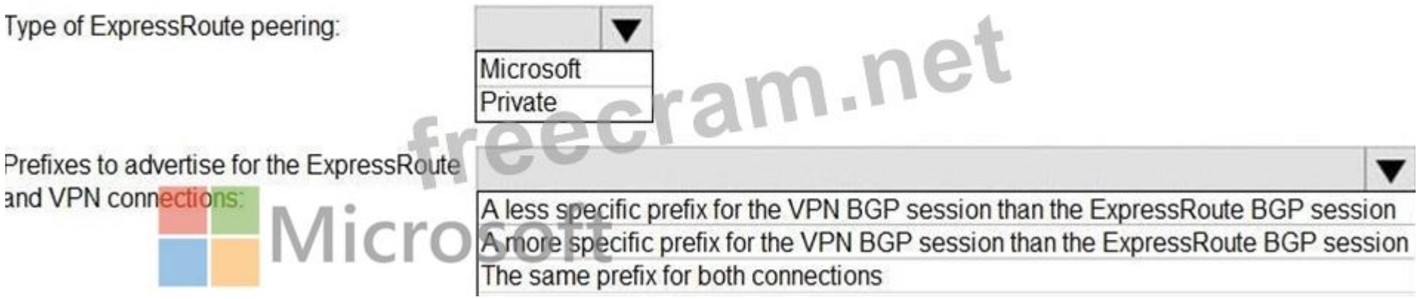
You need to implement hybrid connectivity between an on-premises network and VNet1. The solution must meet the following requirements:

- All cross-premises network traffic must traverse an ExpressRoute

freecram.net Microsoft

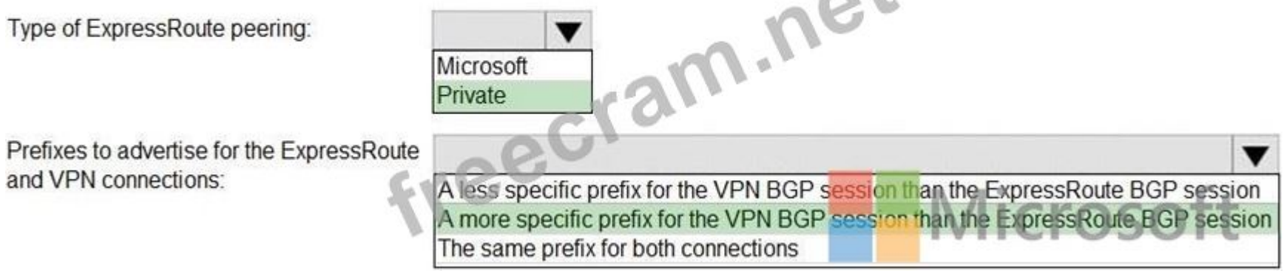
circuit.
- All cross-premises network traffic must be encrypted by using a Site- to-Site (S2S) VPN.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



NEW QUESTION: 44
An ExpressRoute circuit denotes the logical connectivity between MS cloud services and on- premises infrastructure via a connectivity provider. Which of the following statement(s) is/are true about the ExpressRoute circuits?
A. ExpressRoute circuits don't map to a physical entity
B. An ExpressRoute circuit can be uniquely recognized by a service key (s-key)
C. An ExpressRoute circuit can have one or a maximum of two peerings enabled per ExpressRoute circuit
D. There exists 1:1 mapping between ExpressRoute circuits and routing domains
E. There exists 1:1 mapping between ExpressRoute circuits and the S keys
Answer: (SHOW ANSWER)
It is possible to order several ExpressRoute circuits. Each circuit can exist in different or same regions which could be associated with various other connectivity providers.
Option A is correct. It is true that ExpressRoute circuits don't map to a physical entity.
Option B is correct. It is true that an express route circuit can be uniquely recognized as an s-key, i.e., service key.
Option C is incorrect. There can be one, two, or all three peerings enabled for each ExpressRoute circuit.
Option D is incorrect. There exists 1:N mapping (where1 <= N <= 3) between routing domains and ExpressRoute circuits.
Option E is correct. It is true that there exists a 1:1 mapping between ExpressRoute circuits and the s-key.
Reference:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings?WT.mc_id=modinfra-33046-thmaure

NEW QUESTION: 45
You have an 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	Has read-access geo-replicated storage (RA-GRS) redundancy to the paired region
storage2	Storage account	East US	Has read-access geo-replicated storage (RA-GRS) redundancy to the paired region
VM1	Virtual machine	East US	Connected to Subnet1

Microsoft
freecram.net

You create a service endpoint policy that has the following settings:
- Associated subnets: Subnet1
- Service: Microsoft.Storage
- Scope: Single account
- Resource: storage1
Which resources can VM1 access?
A. storage1 in the East US Azure region and its replica in the paired region
B. storage1 in the East US Azure region only
C. storage1 and storage2 in the East US Azure region only
D. storage1 and storage2 in the East US Azure region and their replicas in the paired region
Answer: (SHOW ANSWER)
RA-GRS secondary access is automatically allowed if the primary account is listed.
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview

NEW QUESTION: 46
You have an Azure subscription.
You plan to deploy an app named App1 that will be accessed by using Azure Application Gateway.
You need to deploy the application gateway for App1.
What should you create first?
A. a user-assigned managed identity
B. a subnet
C. an X.509 certificate
D. an Azure Web Application Firewall (WAF) policy

Answer: (SHOW ANSWER)
When deploying an Azure Application Gateway for an application, the first resource that should be created is the virtual network and its subnets, specifically a subnet dedicated to the application gateway itself and another for the backend servers. This is because the application gateway needs a network to operate within, and it requires separate subnets for its own instances and for the resources it will be routing traffic to.
Reference:
https://learn.microsoft.com/sv-se/azure/app-service/overview-app-gateway-integration

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
Case Study 2 - Contoso, Ltd
Overview
Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.
Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.
Existing Environment:
Azure Network Infrastructure
Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	**None**

freecram.net

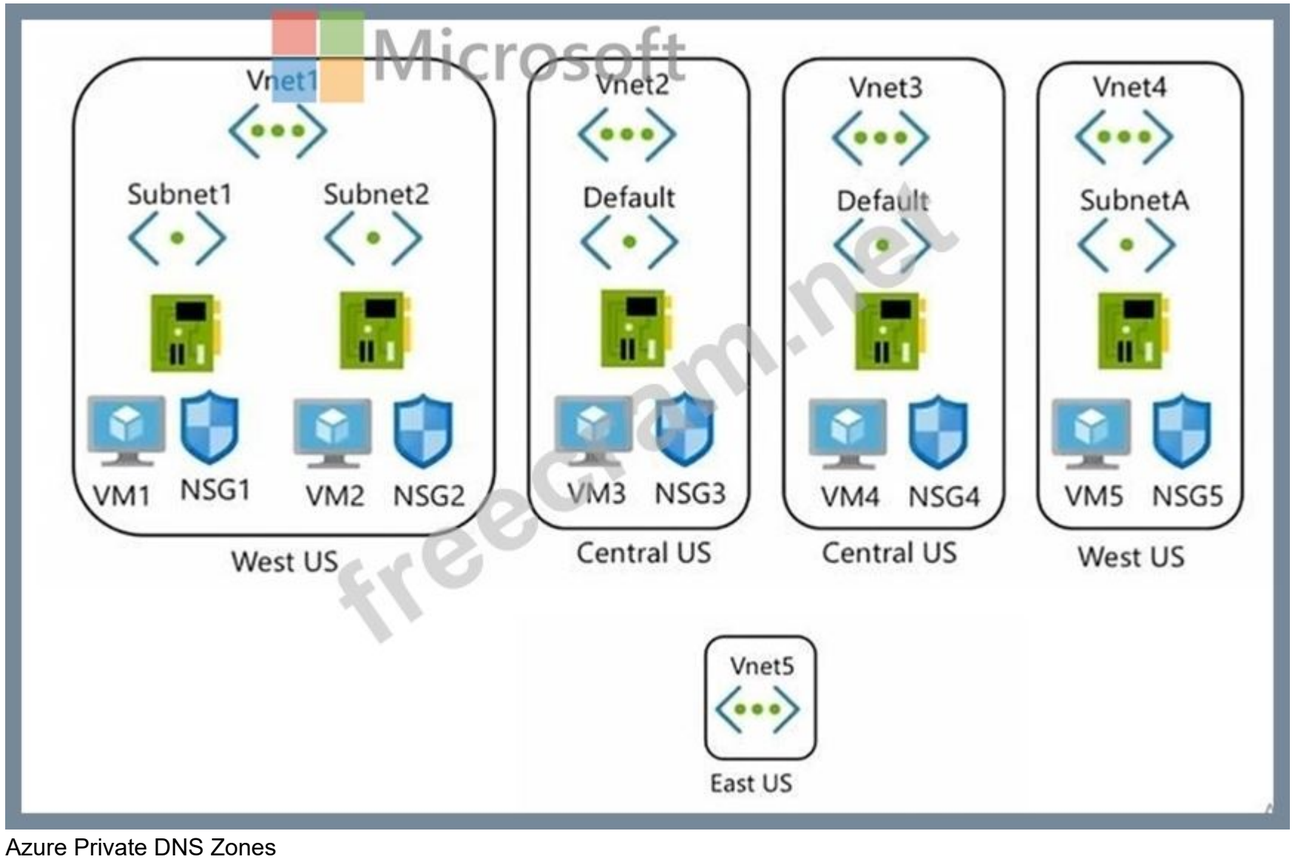
Vnet1 contains a virtual network gateway named GW1.
Azure Virtual Machines
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements:

Virtual Network Requirements

Contoso has the following virtual networks requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

Two container groups that connect to Vnet6

Three virtual machines that connect to Vnet6

Allow VPN connections to be established to Vnet6

Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network

- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements

Contoso has the following network security requirements:

- Configure Azure Active Directory (Azure AD) authentication for Point- to-Site (P2S) VPN users.
- Enable NSG flow logs for NSG3 and NSG4.
- Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

- Create an NSG named NSG11 that will be associated to Vnet1/Subnet2
and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

What should you implement to meet the virtual network requirements for the virtual machines that connect to Vnet4 and Vnet5?

A. a private endpoint
B. a virtual network peering
C. a private link service
D. a routing table
E. a service endpoint

Answer: (SHOW ANSWER)

There is no virtual network peering between VM4's VNet (VNet3) and VM5's VNet (VNet4). To enable the VMs to communicate over the Microsoft backbone network a VNet peering is required between VNet3 and VNet4.

NEW QUESTION: 48

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

Name	Type	Description
Vnet1	Virtual network	*None*
Subnet1	Virtual subnet	Hosted in Vnet1
GatewaySubnet	Virtual subnet	Hosted in Vnet1
VM1	Virtual machine	Connected to Subnet1 Basic SKU public IP address
VM2	Virtual machine	Connected to Subnet2 Standard SKU public IP address

freecram.net Microsoft

You plan to deploy an Azure Virtual Network NAT gateway named Gateway1. The solution must meet the following requirements:
- VM1 will access the internet by using its public IP address.
- VM2 will access the internet by using its public IP address.
- Administrative effort must be minimized.

You need to ensure that you can deploy Gateway1 to Vnet1.
What is the minimum number of subnets required on Vnet1?

A. 2
B. 3
C. 4
D. 5

Answer: (SHOW ANSWER)

1. GatewaySubnet
2. Subnet 2
3. Subnet 1 with Basic SKU for Public IP
4. NAT Gatway requires in VNET 1 and hence 4.

Otherwise you could have used Subnet2 to avoid creating 4th Subnet. Requirement is to create NAT GW in VNET1 so you need 4th Subnet.

https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview

NEW QUESTION: 49

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",
 }
}
```


freecram.net

Microsoft

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.

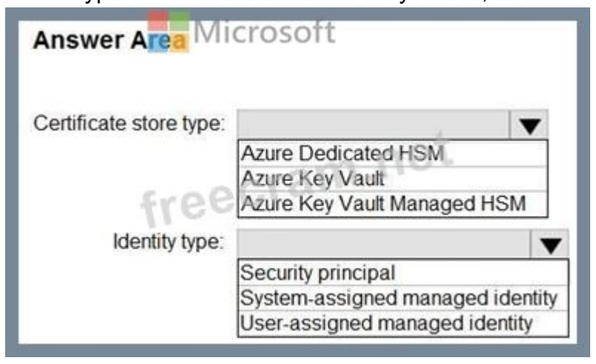
Does this meet the goal?

A. Yes

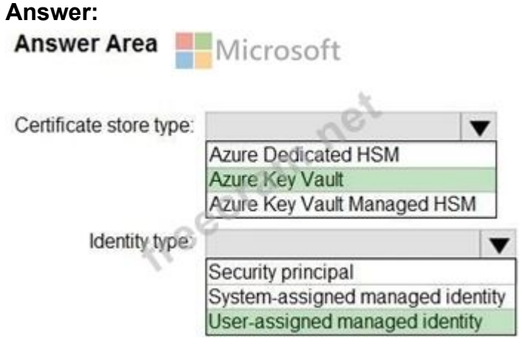
B. No

Answer: (SHOW ANSWER)
The log shows that WAF rule with ruleId 920300 was trigged. Instead we should disable the WAF rule that has a ruleId 920300.
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot

NEW QUESTION: 50
Hotspot Question
You have an Azure subscription.
You plan to implement an Azure application gateway named AGW1.
You need to implement an external TLS certificate store for AGW1. The solution must meet the following requirements:
- Keys must be stored by using the highest possible security.
- Administrative effort must be minimized.
Which type of certificate store should you use, and which type of identity should you use to access the store? To answer, select the appropriate options in the answer area NOTE: Each correct answer is worth one point.



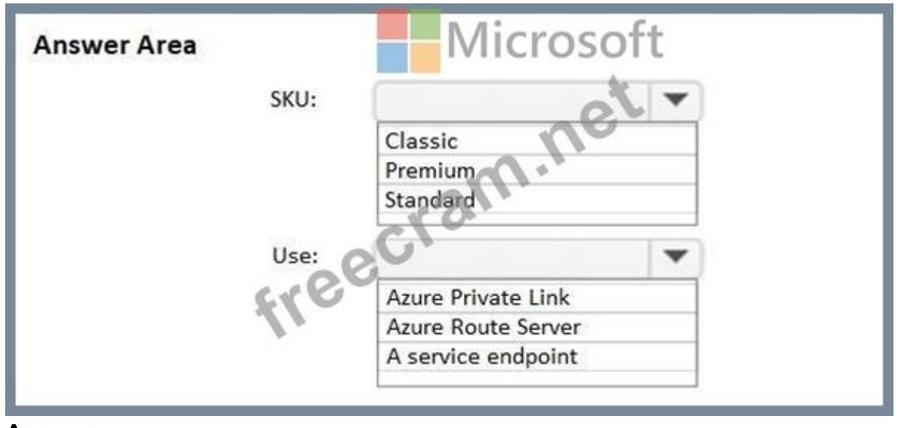
Answer:



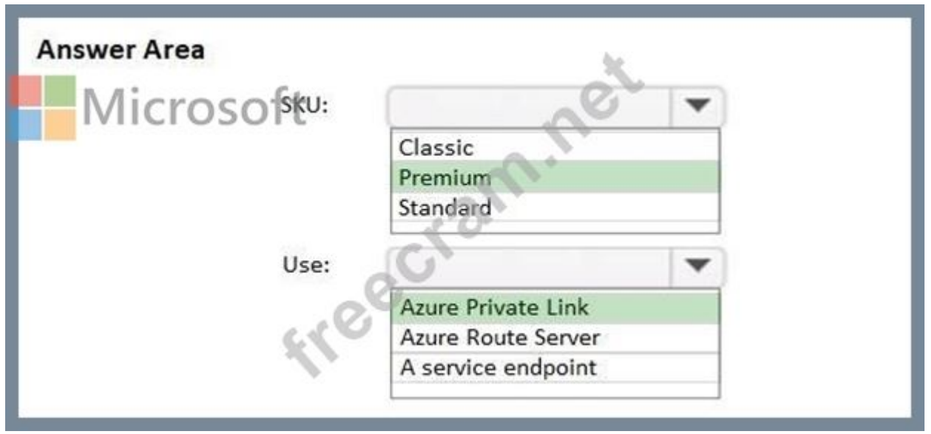
NEW QUESTION: 51
You have an Azure App Service that hosts your frontend application and is publicly accessible.
You also have some backend services in the same region deployed inside a Virtual Network (VNet). The backend services are private and not exposed outside the VNet.
You need to integrate your Azure Service with the VNet to establish a connection between the frontend and backend services.
Which two actions should you perform? Each correct answer presents part of the solution.
A. Use the Isolated App service plan.
B. Create an Integration subnet.
C. Create an Azure Virtual Network gateway.

D. Create a Network Security Group (NSG).
E. Use the Premium App service plan.
Answer: (SHOW ANSWER)
You should create an Integration subnet. Virtual Network integration requires a dedicated subnet in your Virtual Network. The subnet should have a minimum of /28 blocks to accommodate the App Service instances.
You should also use the Premium App service plan. Virtual Network integration requires Standard, Premium, Premium v2, or Premium v3 App service plans.
You should not create a Network Security Group. With Virtual Network integration, you can control the outbound traffic from your App Service using NSG rules. Inbound rules do not apply to the App Service. This also means that even if you enable Virtual Network integration, the App Service does not become private to your Virtual Network. This scenario does not suggest blocking any outbound traffic.
You should not use the Isolated App service plan. This plan is used for App Service Environment and is already deployed inside a Virtual Network.
You should not create Azure Virtual Network gateway. The App Service and Virtual Network are in the same region. Regional VNet integration does not require a Virtual Network Gateway. If the Virtual Network is in a different region or is deployed using a classic model, then a gateway is required to establish connectivity.
https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration
https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-enable

NEW QUESTION: 52
Hotspot Question
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.



Answer:



NEW QUESTION: 53
There are 6 traffic-routing methods in Azure Traffic Manager to control network traffic routing to the different service endpoints.
Which Traffic manager routing method would you use when you are having endpoints in various geographic locations and you want to ensure that end users utilize the "closest" endpoint for the lowest network latency?
A. Priority
B. Network
C. Performance
D. Singlevalue
E. Weighted
Answer: (SHOW ANSWER)
Azure Traffic Manager supports the following traffic-routing methods:
Priority
Weighted
Performance
Multivalue
Geographic
Subnet
Performance Routing is recommended when there are endpoints in various geographic locations.
You need end-users to utilize the "closest" endpoint for the minimum possible network latency.
Option A is incorrect. Priority traffic routing is recommended when you want to have a primary/main service endpoint for all traffic.
Option B is incorrect. The network is not a valid traffic routing method.
Option C is correct. Performance Routing is recommended when there are endpoints in various geographic locations. You need end-users to utilize the "closest" endpoint for the minimum possible network latency.
Option D is incorrect. Singlevalue is not a valid traffic routing method.
Option E is incorrect. Weighted routing is recommended when traffic is distributed all across a set of endpoints depending upon their weight.
Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods?WT.mc_id=modinfra-33046-thmaure

NEW QUESTION: 54
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

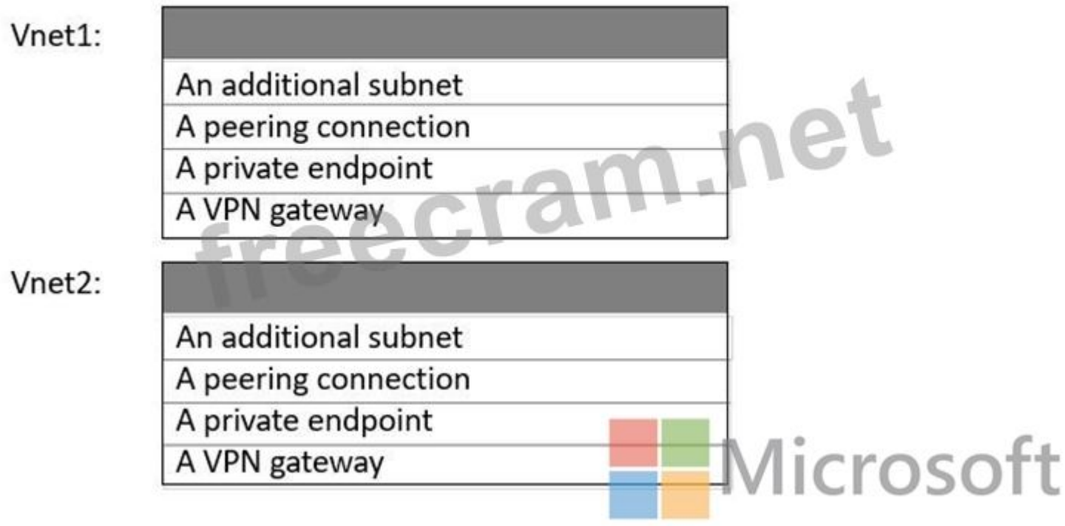
correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 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 NAT Gateway.
Does this meet the requirement?
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Hotspot Question
You have the Azure resources shown in the following table.

Name	Type	Location
Vnet1	Virtual network	East US
Vnet1\Subnet1	Subnet	East US
Vnet1\GatewaySubnet	Subnet	East US
Vnet2	Virtual network	West US
Vnet2\Subnet1	Subnet	West US
Vnet2\GatewaySubnet	Subnet	West US
WebApp1	Azure App Service web app	East US

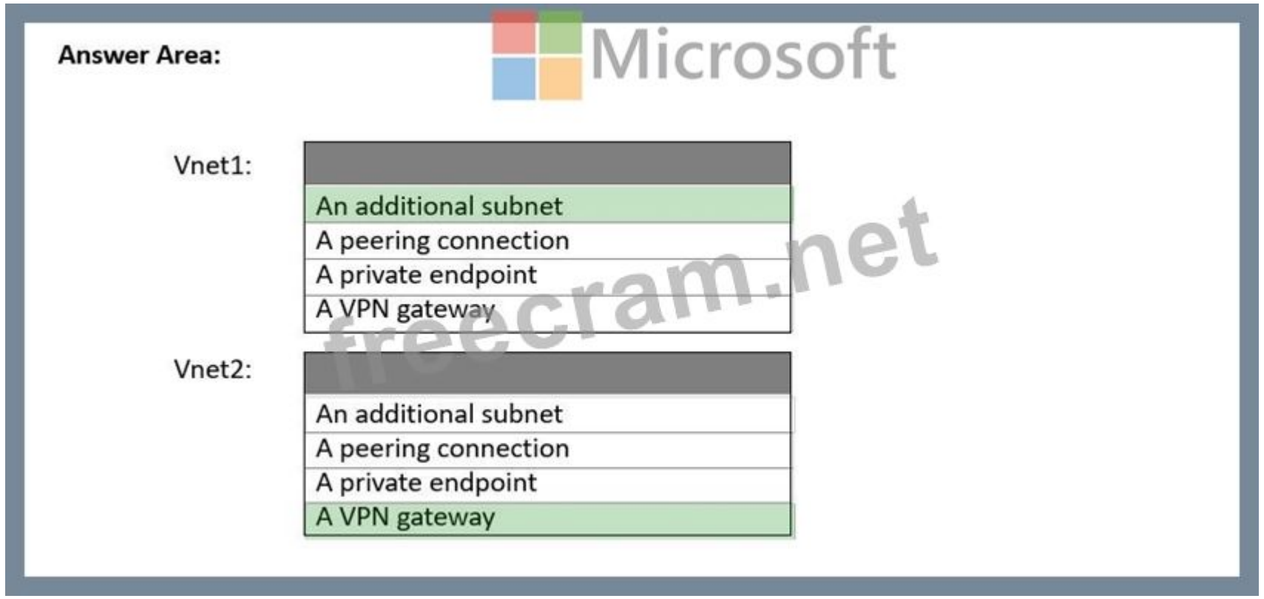
WebApp1 uses the Standard pricing tier.
You need to ensure that WebApp1 can access the virtual machines deployed to Vnet1\Subnet1 and Vnet2\Subnet1. The solution must minimize costs.
What should you create in each virtual network? To answer, select the appropriate options in the answer area.

Answer Area:



freecram.net
Microsoft

Answer:



Microsoft
freecram.net

Explanation:

Box 1: An additional subnet

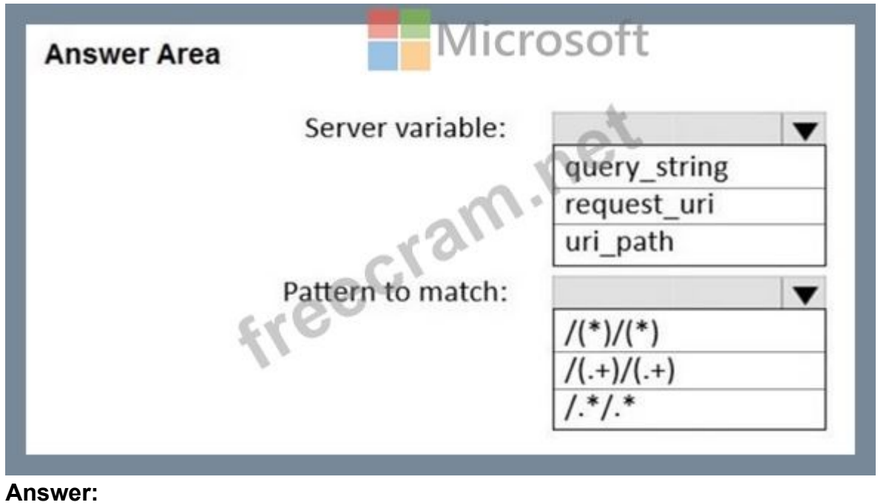
Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

Box 2: A VPN gateway

Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target

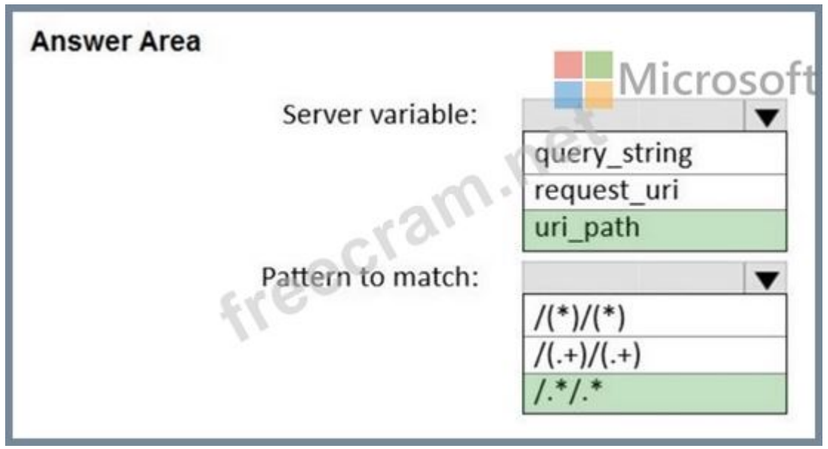
virtual network.
Note: If your app is in an App Service Environment, it's already in a virtual network and doesn't require use of the VNet integration feature to reach resources in the same virtual network.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration

NEW QUESTION: 56
Hotspot Question
You have an Azure subscription that contains an Azure application gateway named AGW1.
You need to create a rewrite rule on AGW1 that will convert web requests as follows:
- Input: https://www.contoso.com/fashion/shirts
- Output:
https://www.contoso.com/buy.aspx?category=fashion&product=shirts
The rewrite rule will have the following settings:
- Type of variable to check: Server variable
- Case-sensitive: No
- Operator: equal (=)
To what should you set Server variable and Pattern to match? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Microsoft
freecram.net

Answer:



NEW QUESTION: 57

Hotspot Question

You have an on-premises network.

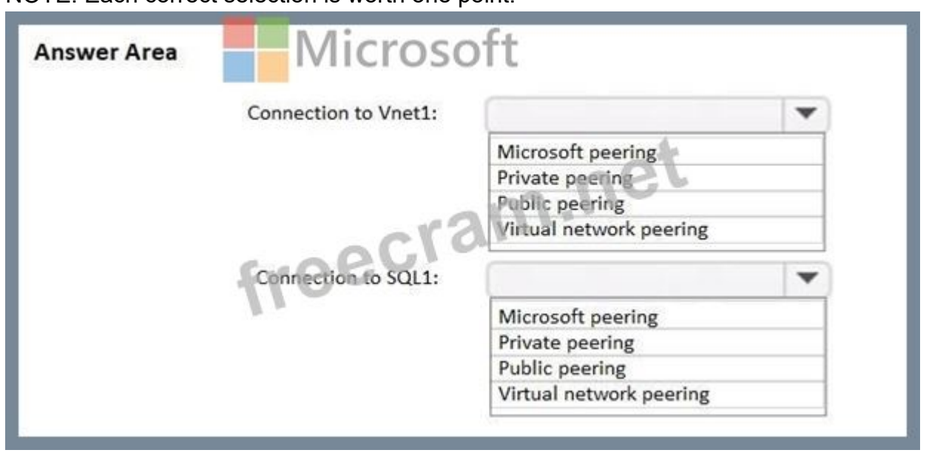
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
Vnet1	Virtual network	*None*
VM1	Virtual machine	Connect to Vnet1
VM2	Virtual machine	Connect 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.

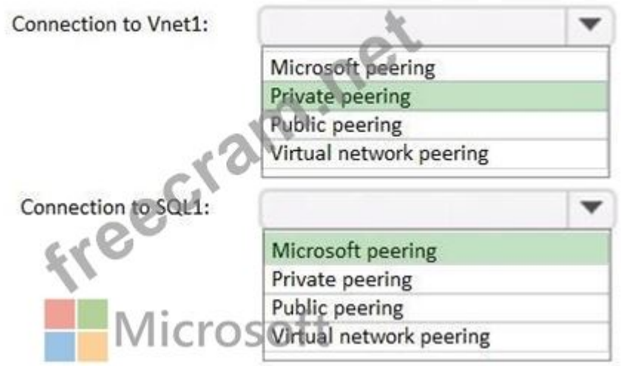
Which type of peering should you use for each connection? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Explanation:
https://learn.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings

NEW QUESTION: 58
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.
Answer: (SHOW ANSWER)
You can use private DNS zones to override the DNS resolution for a private endpoint. A private DNS zone can be linked to your virtual network to resolve specific domains.
When you use Private Endpoint for Web App, the requested URL must match the name of your Web App. When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net. For example, the name resolution will be (Name, Type, Value): mywebapp.azurewebsites.net CNAME mywebapp.privatelink.azurewebsites.net Reference:
https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint

NEW QUESTION: 59
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.

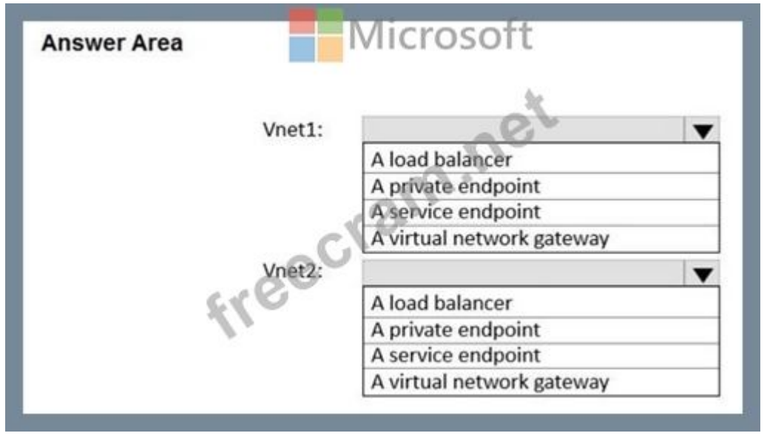
You need to increase the available SNAT connections.
What should you do?
A. Add a public IP address.
B. Bind the NAT gateway to another subnet.
C. Deploy Azure Standard Load Balancer that has outbound rules.
Answer: (SHOW ANSWER)
Evaluate if SNAT port exhaustion should be mitigated with additional IP addresses assigned to NAT gateway resource.
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#snat-exhaustion

NEW QUESTION: 60
You have an on-premises network.
You have an Azure subscription that includes a virtual network named VNet1 and a private Azure Kubernetes Service (AKS) cluster named AKS1. VNet1 is connected to your on-premises environment via an Azure ExpressRoute circuit. AKS1 is connected to VNet1.
You need to implement an off-cluster ingress controller for AKS1. The solution must provide connectivity from the on-premises environment to containerized workloads hosted on AKS1.
Which Azure service should you use?
Freecram.net
A. Azure Application Gateway
B. Azure Front Door
C. Azure Traffic Manager
D. Azure Load Balancer
Answer: (SHOW ANSWER)
The Application Gateway Ingress Controller (AGIC) is a Kubernetes application, which makes it possible for Azure Kubernetes Service (AKS) customers to leverage Azure's native Application Gateway L7 load-balancer to expose cloud software to the Internet.
https://learn.microsoft.com/en-us/azure/application-gateway/ingress-controller-overview

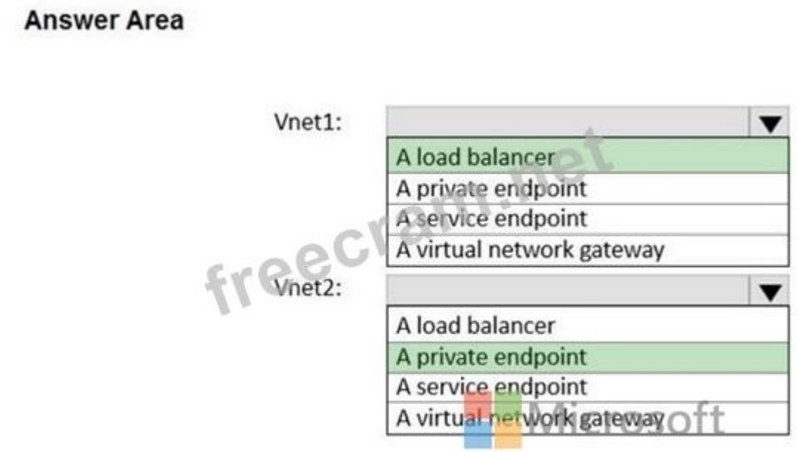
NEW QUESTION: 61
Hotspot Question
You have two Azure subscriptions named Sub1 and Sub2 that contain the resources shown in the following table.

Name	Subscription	Type	Description
VNet1	Sub1	Virtual network	• Contains Subnet1
VM1	Sub1	Virtual machine	• Connected to Subnet1 • Hosts a resource named Resource1
VNet2	Sub2	Virtual network	• Contains Subnet2
VM2	Sub2	Virtual machine	• Connected to Subnet2 • Hosts an app named App1

You need to ensure that App1 can access Resource1 by using the Azure Private Link service.
Which should you deploy to each virtual network to meet the prerequisites of the Private Link service? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



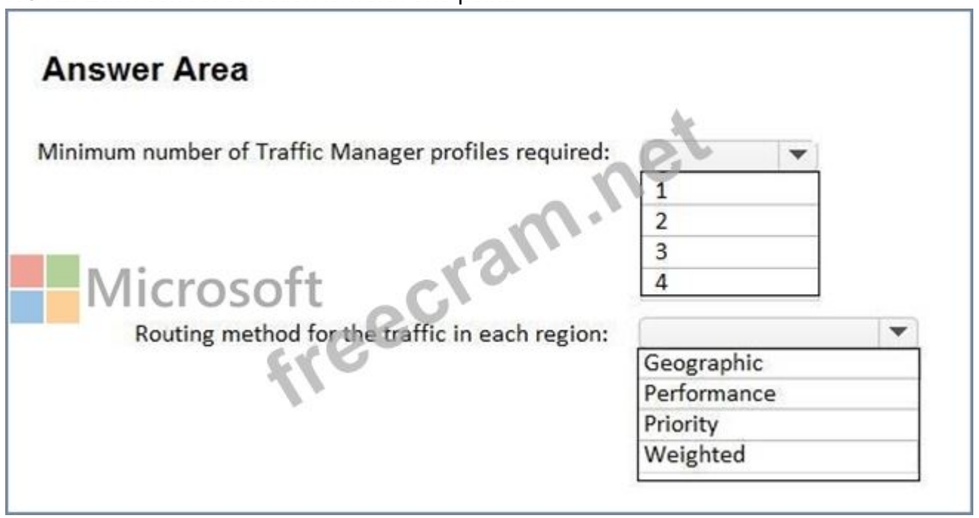
Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
Hotspot Question
You have an Azure subscription that contains an app named App1. App1 is hosted on the Azure App Service instances shown in the following table.

Name	Location
AppSrv1	East US
AppSrv2	East US
AppSrv3	North Europe
AppSrv4	North Europe

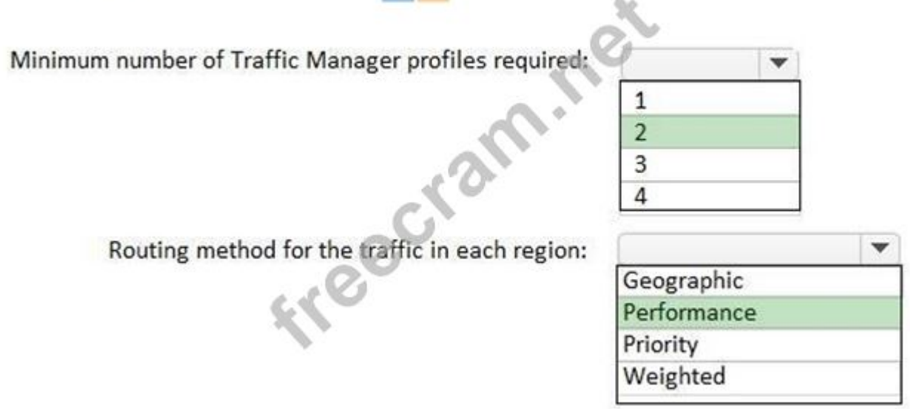
You need to implement Azure Traffic Manager to meet the following requirements:
- App1 traffic must be assigned equally to each App Service instance in each Azure region.
- App1 traffic from North Europe must be routed to the App1 instances in the North Europe region.
- App1 traffic from North America must be routed to the App1 instances in the East US Azure region.
- If an App Service instance fails, all the traffic for that instance must be routed to the remaining instances in the same region.

How should you configure the Traffic Manager profiles? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Explanation:
One parent profile configured for 'performance' and 2 child profiles configured for 'priority' each child profile configured on having 2 nodes.

NEW QUESTION: 63
Case Study 3 - Contoso, Ltd
Overview
Proseware, Inc. is a financial services company that has a main office in New York City and a branch office in San Francisco.
Existing Environment. Hybrid Environment
Proseware has an on-premises Active Directory Domain Services (AD DS) forest named corp.proseware.com that syncs with a Microsoft Entra tenant named proseware.com.
Proseware has an Azure subscription that is linked to proseware.com.
Proseware has an internal certification authority (CA).
Existing Environment. Network Infrastructure
The offices contain the resources shown in the following table.

Name	Type	Office	Description
NYCNet	On-premises network	New York City	IP address space of 192.168.0.0/22
SFONet	On-premises network	San Francisco	IP address space of 192.168.100.0/22
NYCDNS1	Server	New York City	DNS server that runs Windows Server 2019 and has an IP address of 192.168.0.100

NYCNet connects to Azure by using an ExpressRoute circuit.
SFONet connects to Azure by using a Site-to-Site (S2S) VPN.
Existing Environment. Azure Resources
The Azure subscription contains the virtual networks and subnets shown in the following table.

Name	Type	Location	Description
HubVNet	Virtual network	East US Azure region	IP address space of 10.0.0.0/20 peered to SpokeVNet
SpokeVNet	Virtual network	East US Azure region	IP address space of 10.0.16.0/20 peered to HubVNet
VPNGW1	Virtual network gateway	HubVNet	Active-passive resiliency, in the Generation 2, VpnGw3 SKU that has the default ASN connected to SFONet
SUBNET-PE	Subnet	HubVNet	Used for private endpoints
SUBNET-JUMPHOSTS	Subnet	HubVNet	Used for jump hosts
SUBNET-APPGW1	Subnet	SpokeVNet	Contains an Azure application gateway named APPGW1

The subscription contains four virtual machines named VM1, VM2, VM3, and VM4. VM1 and VM2 host an app named App1.

VM3 and VM4 host a web app named App2 that is accessed by using a FQDN of app2.proseware.com. Users access app2.proseware.com by using HTTP or HTTPS.

VM1, VM2, and VM4 are connected to SpokeVNet.

The subscription contains Application Gateway resources shown in the following table.

Name	Type	Location	Description
APPGW1	Application Gateway	SpokeVNet	In the Azure Web Application Firewall (WAF) V2 SKU Terminates HTTPS connections to a backend pool that contains VM3 and VM4
APPGW1-NSG1	Network security group (NSG)	East US region	Associated with SUBNET-APPGW1
APPGW1-WAFPolicy	Azure Web Application Firewall (WAF) policy	East US region	Applied to APPGW1

The subscription contains an Azure Front Door Standard profile named FD1. FD1 contains a single origin group that targets APPGW1 by using the default endpoint name.

HubVNet connects to NYCNet by using an ExpressRoute gateway named ERGW1.

Planned Changes and Requirements. Planned Changes

Proseware plans to implement the following changes:

- Deploy an Azure Private DNS Resolver named PRDNS1 to HubVNet and link PRDNS1 to SpokeVNet.
- Create a DNS forwarding ruleset named DNSRS1 and associate DNSRS1 with PRDNS1.
- Deploy Azure Virtual Network Manager and implement the following rules:
- Allow inbound connections on TCP port 3389 from the on-premises networks to SUBNET- JUMPHOSTS.
- Block inbound connections on TCP port 80 from the internet to SpokeVNet.
- Ensure that Azure Virtual Network Manager rules take precedence over conflicting NSG rules.
- Deploy two network virtual appliances (NVAs) named NVA1 and NVA2 to HubVNet.
- Deploy a gateway load balancer named LBGW1 to HubVNet.
- Configure LBGW1 to inspect traffic on TCP ports 443, 1433, and 1434 from LBS1 by using NVA1 and NVA2.
- Ensure that all the traffic to App2 is processed by using FD1.

Planned Changes and Requirements. Connectivity requirements

Proseware identifies the following connectivity requirements:

- Minimize the complexity of the Azure Virtual Network Manager deployment.
- Route traffic between NYCNet and SFONet via the ExpressRoute circuit and the S2S VPN.
- Ensure that remote users on Windows 11 devices can connect to HubVNet by using a Point-to- Site (P2S) VPN and their proseware.com credentials.

Planned Changes and Requirements. Security requirements

Proseware identifies the following security requirements:

- Whenever possible, use the internal CA.
- Ensure that all connections routed via APPGW1 use end-to-end encryption.
- Ensure that user connections to Azure-hosted apps use end-to-end encryption.
- Ensure that all inbound internet traffic to app2.proseware.com is routed via FD1.
- Prevent devices that connect to NYCNet from accessing Azure services that use private endpoints.
- Enable the virtual machines that connect to HubVNet and SpokeVNet to access Azure services that use private endpoints.

Planned Changes and Requirements. General requirements

Proseware identifies the following general requirements:

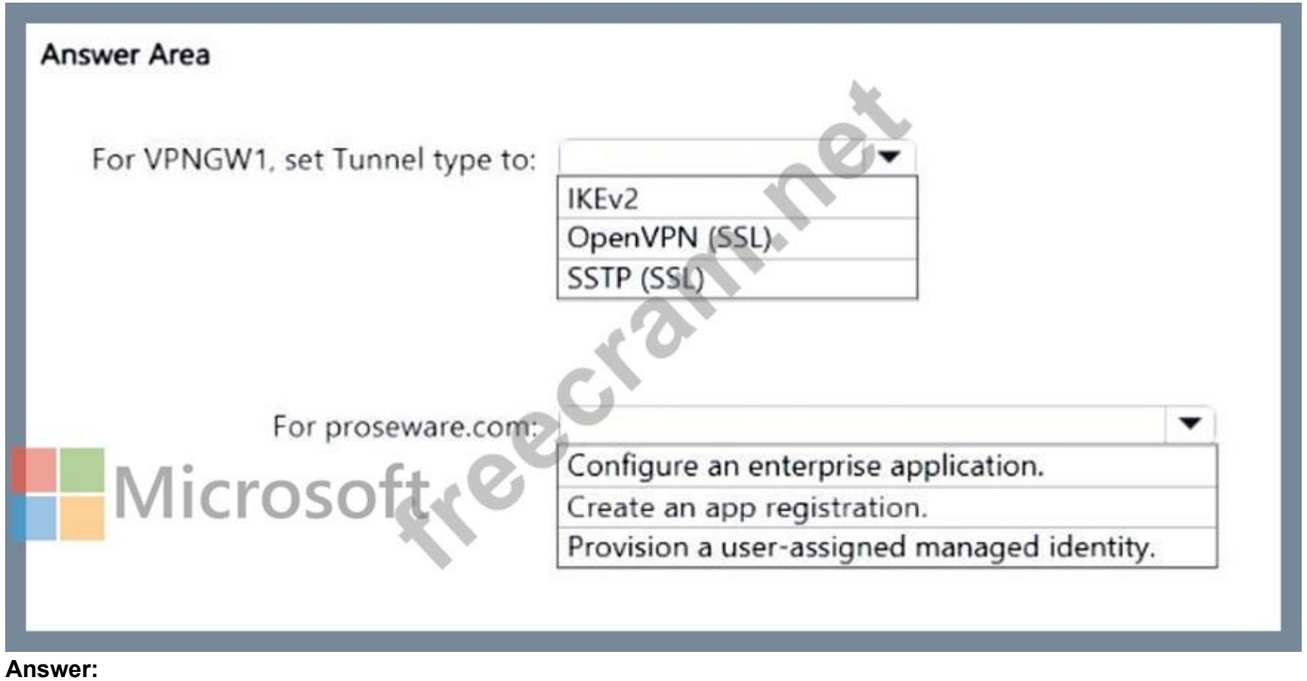
- Minimize the IP address space required to deploy platform-managed resources to the virtual networks.
- From SpokeVNet, resolve name resolution requests for the azure.proseware.com namespace and the corp.proseware.com namespace by using PRDNS1.
- Whenever possible, minimize administrative effort.

Hotspot Question

You need to configure the P2S VPN to meet the connectivity requirements.

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

NOTE: Each correct selection is worth one point.



Microsoft
freecram.net

Answer:

Answer Area



freecram.net
Microsoft

NEW QUESTION: 64
You can get the current service tag and range information by downloading the JSON file or programmatically adding it as part of your on-premises firewall configuration. Which of the following can be used to programmatically retrieve the current list of service tags?
A. REST
B. Azure PowerShell
C. Azure CLI
D. All of these
Answer: (SHOW ANSWER)
The current list of service tags along with IP address range details can be programmatically retrieved using:
REST
Azure PowerShell
Azure CLI
Option A is incorrect. The list of service tags can be retrieved using any REST, Azure PowerShell or Azure CLI.
Option B is incorrect. The list of service tags can be retrieved using any REST, Azure PowerShell or Azure CLI.
Option C is incorrect. The list of service tags can be retrieved using any REST, Azure PowerShell or Azure CLI.
Option D is correct. Any of the REST, Azure PowerShell or Azure CLI can be used to get the list of service tags.
Option E is incorrect. Any of the REST, Azure PowerShell or Azure CLI can be used to get the list of service tags.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview?WT.mc_id=modinfra-33046-thmaure

NEW QUESTION: 65
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

Answer: B (LEAVE A REPLY)

TLS Inspection and IDPS features available in Azure Firewall Premium tier only.

https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku#feature-comparison

NEW QUESTION: 66

Hotspot Question

You have an Azure subscription.

You have the on-premises sites shown the following table.

Number	Number of users	Connection type to Azure
Site 1	500	ExpressRoute
Site 2	100	Site-to-Site VPN
Site 3	1	Point-to-Site (P2S) VPN

You plan to deploy Azure Virtual WAN.

You are evaluating Virtual WAN Basic and Virtual WAN Standard.

Which type of Virtual WAN can you use for each site? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Virtual WAN Basic:

- Site2 only
- Site3 only
- Site2 and Site3 only
- Site1, Site2, and Site3

Virtual WAN Standard:

- Site1 only
- Site1 and Site3 only
- Site2 and Site3 only
- Site1, Site2, and Site3

freecram.net

Microsoft

Answer:

Answer Area

Virtual WAN Basic:

- Site2 only
- Site3 only
- Site2 and Site3 only
- Site1, Site2, and Site3

Virtual WAN Standard:

- Site1 only
- Site1 and Site3 only
- Site2 and Site3 only
- Site1, Site2, and Site3

Microsoft freecram.net

Explanation:
VWAN Type Hub type Available configurations
Vitual WAN
Basic
Site-to-site Only
Standard
ExpressRoute
User VPN (P2S)
VPN (site-to-site)
Inter-hub and VNet-to-VNet transiting through the virtual hub
Azure Firewall
NVA in a virtual WAN
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#basicstandard

NEW QUESTION: 67

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 NSG1 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 131.1071.15.
- Minimize changes to NSG1 when a new subnet is created.
What should you use as the destination in the inbound security rule?
A. an application security group
B. a service tag
C. a virtual network
D. an IP address
Answer: (SHOW ANSWER)
Create an ASG and assign to each monitoring vm. Then in the NSG1, create an allow rule to allow the IP 131.107.1.15 to the ASG.
https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

NEW QUESTION: 68
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 add a rule to the rule set of AFD1.
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 69
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 Firewall.
Does this meet the requirement?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Hotspot Question

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

Name	Address space	Associated network security group (NSG)
Subnet1	10.10.0.0/24	NSG1
Subnet2	10.10.1.0/24	NSG2

In NSG1, you create inbound rules as shown in the following table.

Source	Priority	Port	Action
*	101	80	Allow
*	150	443	Allow
Virtual network	200	*	Deny

NSG2 has only the default rules configured.

You have the Azure virtual machines shown in the following table.

Name	Subnet
VM1	Subnet1
VM2	Subnet1
VM3	Subnet2

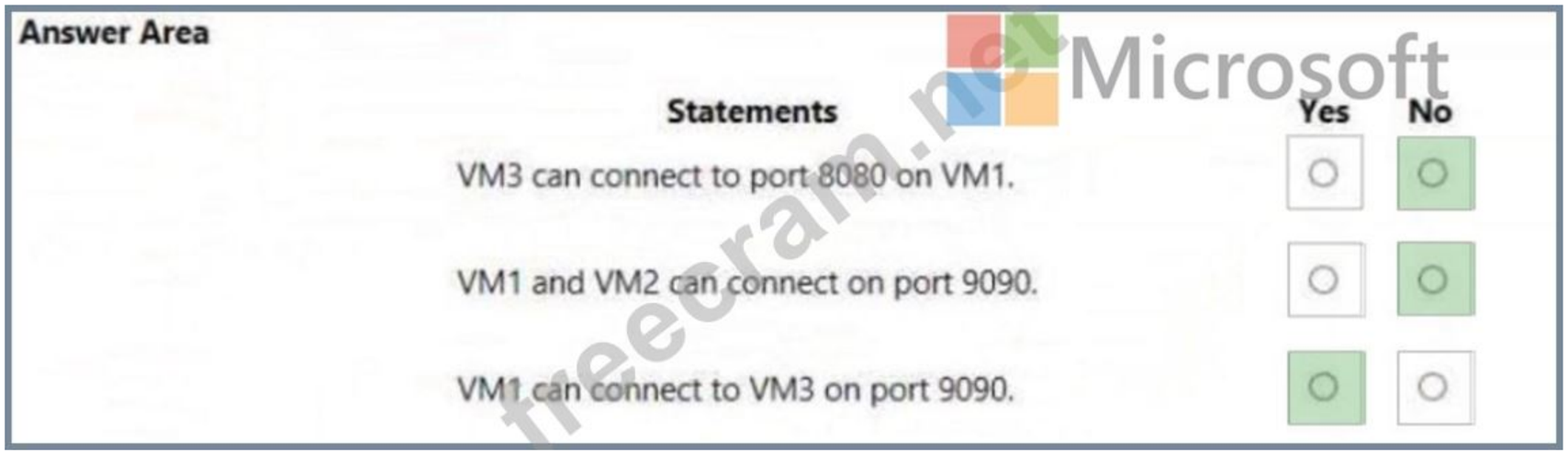
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM3 can connect to port 8080 on VM1.	○	○
VM1 and VM2 can connect on port 9090.	○	○
VM1 can connect to VM3 on port 9090.	○	○

Answer:



Explanation:

Box 1: No

VM3 will be allowed to access VM1 on any port outbound on NSG2. VM3 will be blocked by NSG1 inbound since it is trying to access port 8080.

Box 2: No

VM1 and VM2 belongs to the same subnet 1 and each of them has default Outbound policy rule that will allow the traffic but Inbound is restricted for any port except 80 and 443.

Box 3: Yes

NSG2 has the default rules applied, it means that Subnet2 can accept traffic from any subnet within the VNET.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

NEW QUESTION: 71

You have an Azure subscription.

You plan to deploy Azure Firewall Premium, enable all the Premium features, and configure both network and application rules.

Which type of rule will the firewall process first?

A. network

B. application

C. threat intelligence

D. infrastructure

Answer: (SHOW ANSWER)

https://learn.microsoft.com/en-us/azure/firewall/rule-processing#threat-intelligence

NEW QUESTION: 72

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

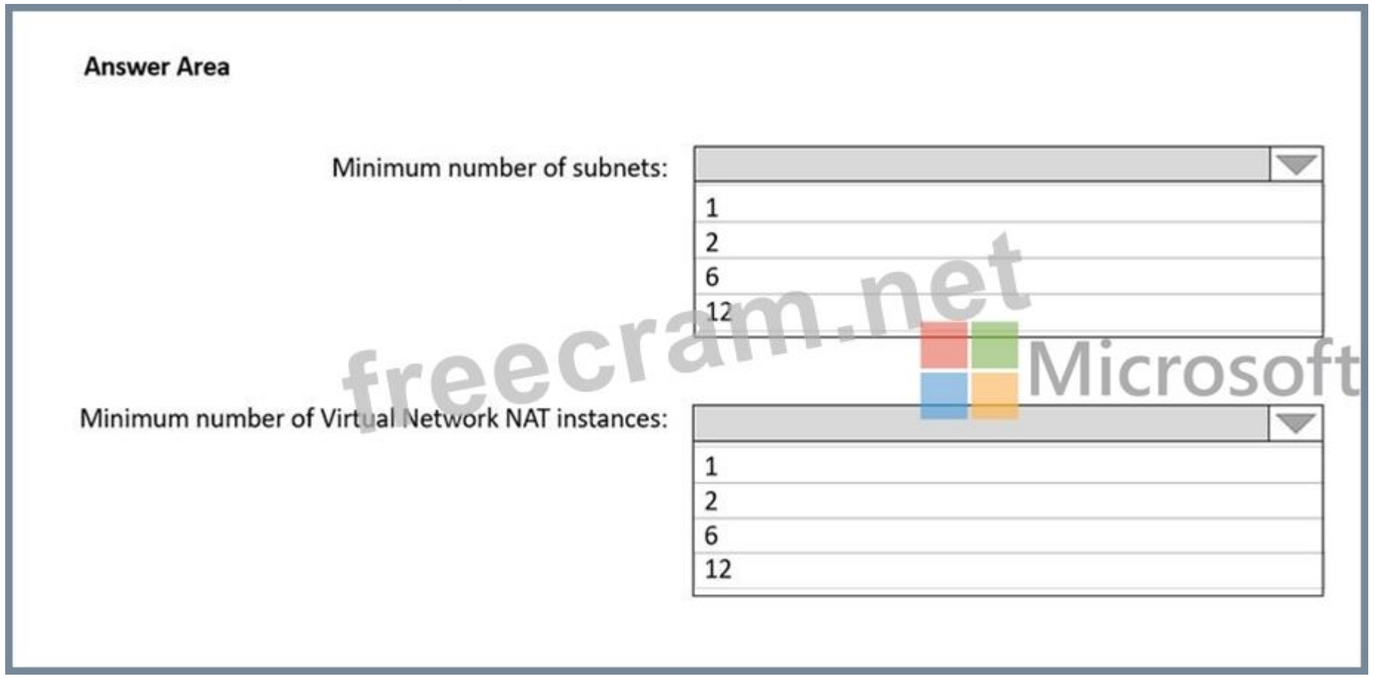
Name	Type	Description
FW1	Azure Firewall Premium	Has a network intrusion detection and prevention system (IDPS) enabled
HP1	Azure Virtual Desktop host pool	All outbound traffic from HP1 to the subscription's resources route through FW1
Server1	Virtual machine	Hosts an application named App1
KV1	Azure Key Vault	*None*

Users on HP1 connect to App1 by using a URL of https://app1.contoso.com.
You need to ensure that the IDPS on FW1 can identify security threats in the connections from HP1 to Server1.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Enable TLS inspection for FW1.
B. Import a server certificate to KV1.
C. Enable threat intelligence for FW1.
D. Add an application group to HP1.
E. Add a secured virtual network to FW1.
Answer: (SHOW ANSWER)
The Firewall needs to be able to decrypt the traffic so the IDS can inspect the traffic. To do this TLS inspection needs to be enabled and a copy of the certificate needs to be stored.
https://learn.microsoft.com/en-us/azure/firewall/premium-certificates
https://learn.microsoft.com/en-us/azure/firewall/premium-features#tls-inspection

NEW QUESTION: 73
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. On FW1, create an outbound service tag rule for AzureCloud.
B. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.
C. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.
D. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Hotspot Question
You have two Azure virtual networks named Vnet1 and Vnet2 in an Azure region that has three availability zones.

You deploy 12 virtual machines to each virtual network, deploying four virtual machines per zone.
The virtual machines in Vnet1 host an app named App1. The virtual machines in Vnet2 host an app named App2.
You plan to use Azure Virtual Network NAT to implement outbound connectivity for App1 and App2.
You need to identify the minimum number of subnets and Virtual Network NAT instances required to meet the following requirements:
- A failure of two zones must NOT affect the availability of either
App1 or App2.
- A failure of two zones must NOT affect the outbound connectivity of
either App1 or App2.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



freecram.net
Microsoft

Answer:

Answer Area

Minimum number of subnets:

- 1
- 2
- 6
- 12

Minimum number of Virtual Network NAT instances:

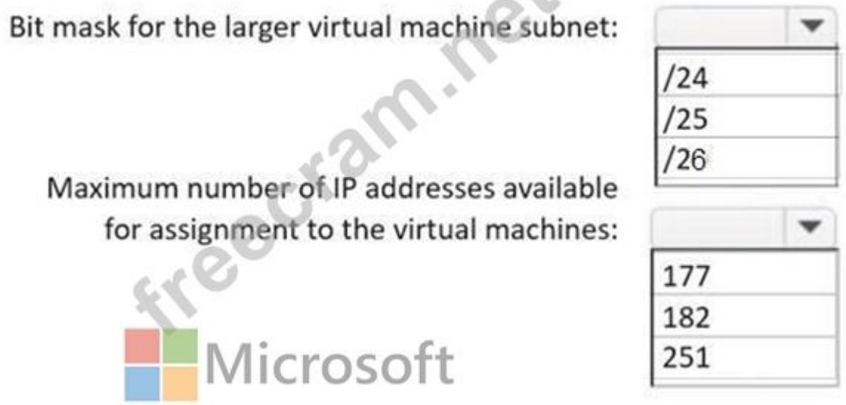
- 1
- 2
- 6
- 12

Explanation:
Availability zone isolation cannot be provided, unless each subnet only has resources within a specific zone. Instead, deploy a subnet for each of the availability zones where VMs are deployed, align the zonal VMs with matching zonal NAT gateways, and build separate zonal stacks. For example, a virtual machine in availability zone 1 is on a subnet with other resources that are also only in availability zone 1. A NAT gateway is configured in availability zone 1 to serve that subnet.
ttps://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network- address-translation-gateway

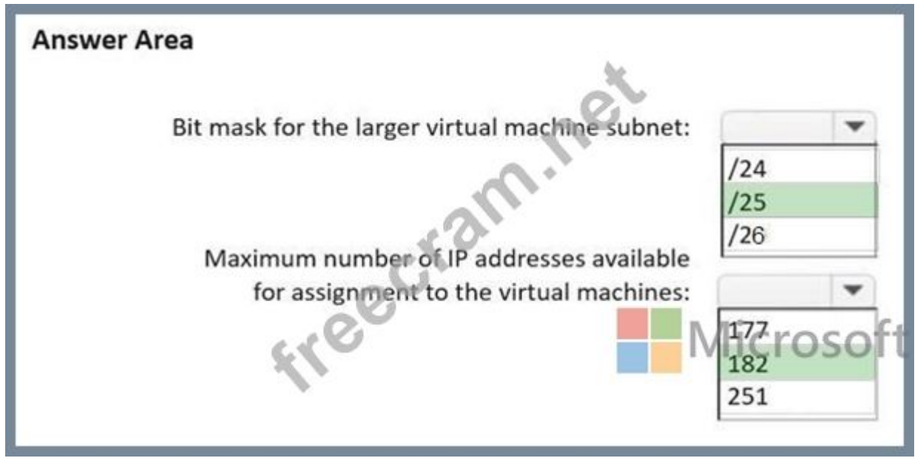
NEW QUESTION: 75
Hotspot Question
You have an Azure subscription that contains a virtual network named VNet1. VNet1 uses an IP address space of 192.168.0.0/24.
You plan to deploy Azure virtual machines and Azure Bastion to VNet1.

You need to recommend an IP subnetting configuration for VNet1. The solution must maximize the number of IP addresses that can be assigned to the virtual machines.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:



NEW QUESTION: 76
You have an Azure subscription that contains a distributed web app named App1. App1 is hosted across multiple Azure regions.
You need to recommend a solution for routing user requests to App. The solution must meet the following requirements:
- Support the routing of a user request to a resource based on the URL
of the request.
- Support query string replacement.
- Minimize network latency.
What should you include in the recommendation?
A. Azure Load Balancer

B. Azure Traffic Manager
C. Azure Content Delivery Network (CDN)
D. Azure Front Door
Answer: (SHOW ANSWER)
* Azure Front Door is ideal for companies that have globally distributed web applications and want to reduce latency, improve security with DDoS and WAF protection, and optimize performance with advanced caching.
* Azure Front Door supports routing user requests based on the URL path. This is achieved through URL path-based routing, which allows you to define rules that match specific URL paths and direct traffic to different backend pools accordingly. You can also use the URL rewrite action to modify the URL path before forwarding the request to the backend, enabling more flexible routing scenarios.
* Redirect using query string, URL path segments, or incoming hostname captures Managing redirects is critical for search engine optimization (SEO), user experience, and the proper functioning of a website. Azure Front Door's rules engine and server variables allow you to efficiently manage batch redirects based on various parameters.
Reference:
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq
https://learn.microsoft.com/en-us/azure/frontdoor/rules-engine-scenarios

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
Hotspot Question
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.



Microsoft
freecram.net

You have the virtual machine shown in the VM1 exhibit.



Microsoft
freecram.net

Subnet1 is configured as shown in the Subnet1 exhibit.



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

NOTE: Each correct selection is worth one point.

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:

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	○	○

Microsoft
freecram.net

Explanation:
Box 1: Yes
You will not achieve zone redundancy with that setup, but it will work "While the scenario will appear to work, its health model and failure mode is undefined from an availability zone point of view".
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#cross- zone-outbound-scenarios-not-supported Box 2: No NAT GW has configured only 1 subnet and in Subnet1 Config you can clearly see that it is linked to NatGateway1. This is possible because subnets are not a zonal construct, i.e. not assigned to a zone.
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

NEW QUESTION: 78
The Domain Name System (DNS) resolves or translates a service name to an IP address.
Which of the following records types can't be used by Azure Private DNS?
A. CNAME
B. A
C. AA
D. AAA
E. AAAA
F. PTR
Answer: (SHOW ANSWER)
Azure Domain Name Service supports A, AAAA, MX, CNAME, PTR, SRV, SOA, and TXT records.
Option A is incorrect. CNAME is a valid DNS record type.

Option B is incorrect. A is a valid DNS record type.
Option C is correct. Azure DNS does not support AA type.
Option D is correct. Azure DNS does not support AAA type.
Option E is incorrect. Azure Domain Name Service supports A, AAAA, MX, CNAME, PTR, SRV, SOA, and TXT records.
Reference:
https://docs.microsoft.com/en-us/azure/dns/private-dns-overview?WT.mc_id=modinfra-33046- thmaure

NEW QUESTION: 79
SIMULATION

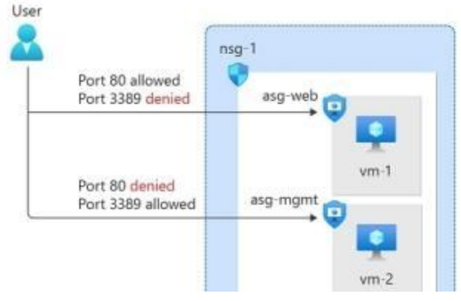


Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You need to ensure that subnet3-2 can only access resources on subnet3-1.
To complete this task, sign in to the Azure portal.
Answer:

Azure network rules

You can use a network security group to filter inbound and outbound network traffic to and from Azure resources in an Azure virtual network.

Network security groups contain security rules that filter network traffic by IP address, port, and protocol. When a network security group is associated with a subnet, security rules are applied to resources deployed in that subnet.





Stage 1: Create a network security group
A network security group (NSG) secures network traffic in your virtual network.

Step 1: In the search box at the top of the portal, enter Network security group. Select Network security groups in the search results.

Step 2: Select + Create.

Step 3: On the Basics tab of Create network security group, enter or select something like this information

Project details
Subscription: Select your subscription.
Resource group: Select test-rg.
Instance details
Name: Enter nsg-1.
Location: Select East US 2.

Step 4: Select Review + create.

Step 5: Select Create.

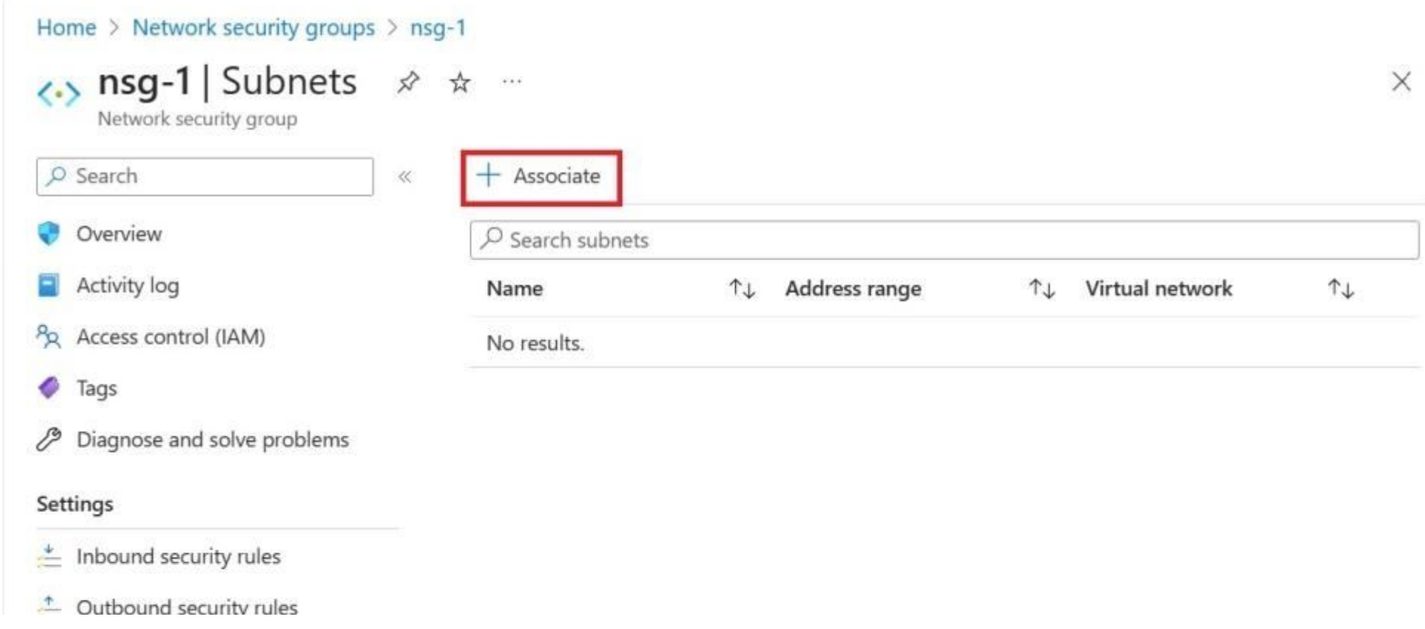
Stage 2
Associate network security group to subnet
In this section, you associate the network security group with the subnet of the virtual network you created earlier.

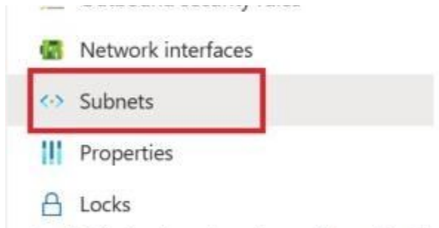
Step 1: In the search box at the top of the portal, enter Network security group. Select Network security groups in the search results.

Step 2: Select nsg-1.

Step 3: Select Subnets from the Settings section of nsg-1.

Step 4: In the Subnets page, select + Associate:





Step 5: Under Associate subnet, select vnet-1 (test-rg) for Virtual network.

Step 6: Select subnet3-2 for Subnet, and then select OK.

Stage 3:
Create security rules
Step 1: Select Outbound security rules from the Settings section of nsg-1.

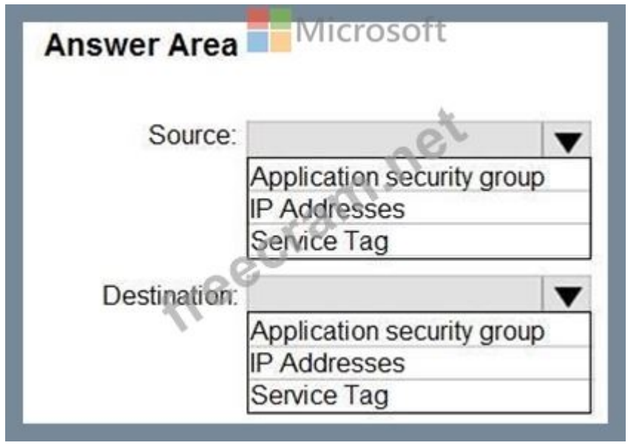
Step 2: In Outbound security rules page, select + Add.

Step 3: Create a security rule that allows any ports, any protocol, to subnet3-1.

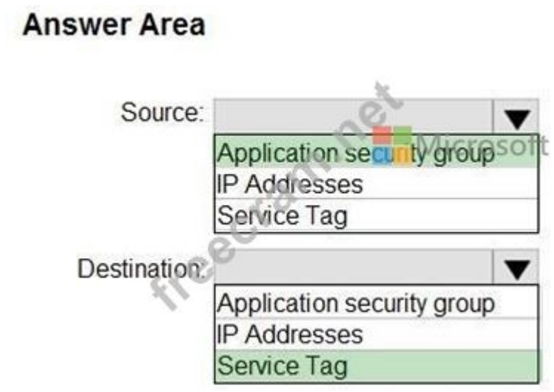
Step 4: Select Add.

Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic

NEW QUESTION: 80
Hotspot Question
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.



Answer:



NEW QUESTION: 81

Hotspot Question

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.

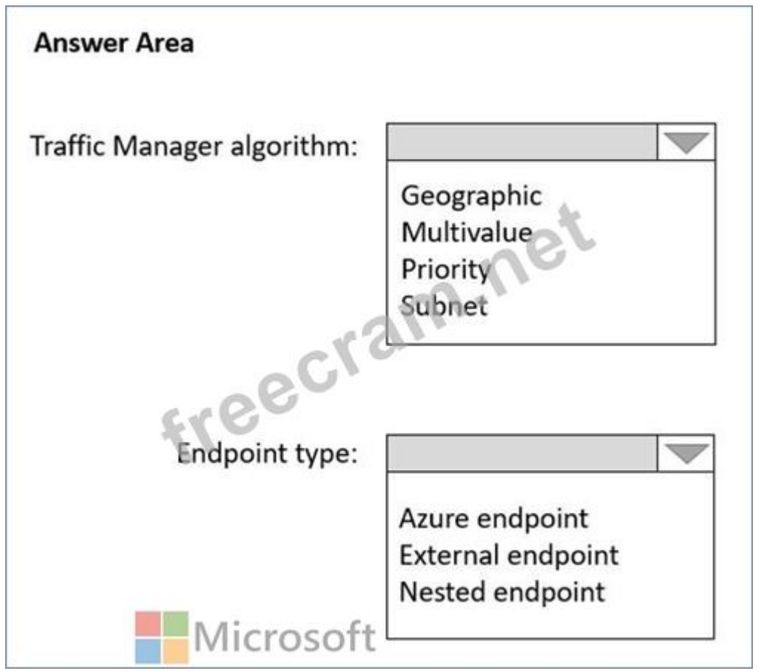
You plan to use Azure Traffic Manager to maintain the list of endpoints.

The development department at the company is creating an application named App1. Every 10 minutes. App1 will use a list of end points and connect to the first available endpoint.

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.

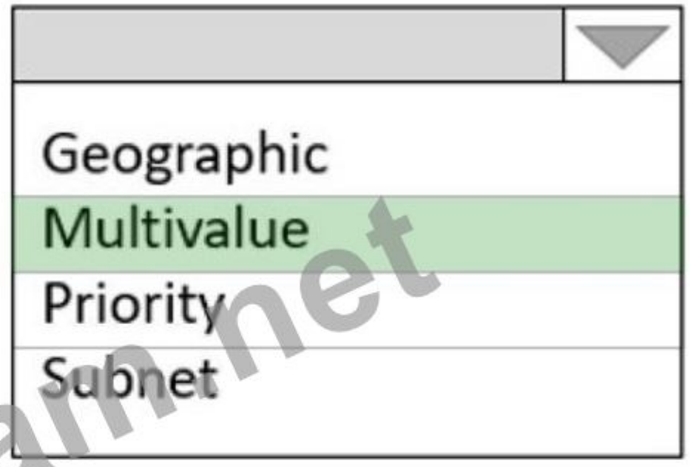
NOTE: Each correct selection is worth one point.


Answer Area
Traffic Manager algorithm:
Geographic
Multivalue
Priority
Subnet
Endpoint type:
Azure endpoint
External endpoint
Nested endpoint
Microsoft

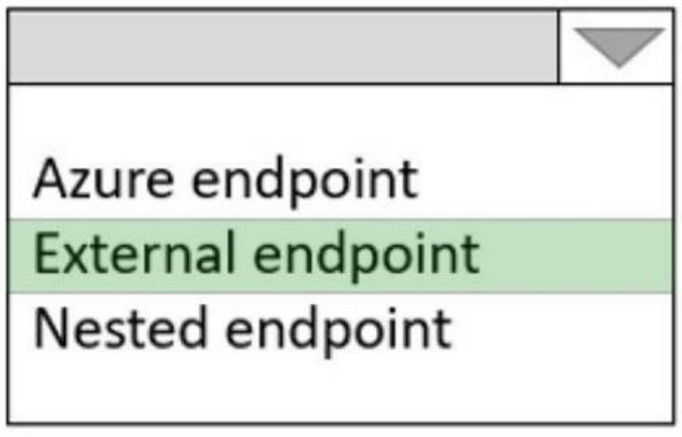
Answer:

Answer Area

Traffic Manager algorithm:



Endpoint type:



freecram.net

Explanation:

A traffic manager Multivalue profile can have only endpoints of type "External" Multivalue traffic-routing method The Multivalue traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response. This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive. This pattern can increase the availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint.

MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses. When a query is received for this profile, all healthy endpoints are returned and are subject to a configurable maximum return count.
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing- methods#multivalue

NEW QUESTION: 82
SIMULATION


Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You need to block all outbound internet traffic for HTTP and HTTPS that originates from subnet1-1. All other traffic must be allowed.
To complete this task, sign in to the Azure portal.
Answer:

Use firewall to restrict outbound traffic using Azure portal
Azure Firewall can restrict outbound HTTP and HTTPS traffic.

Configure the firewall with network rules

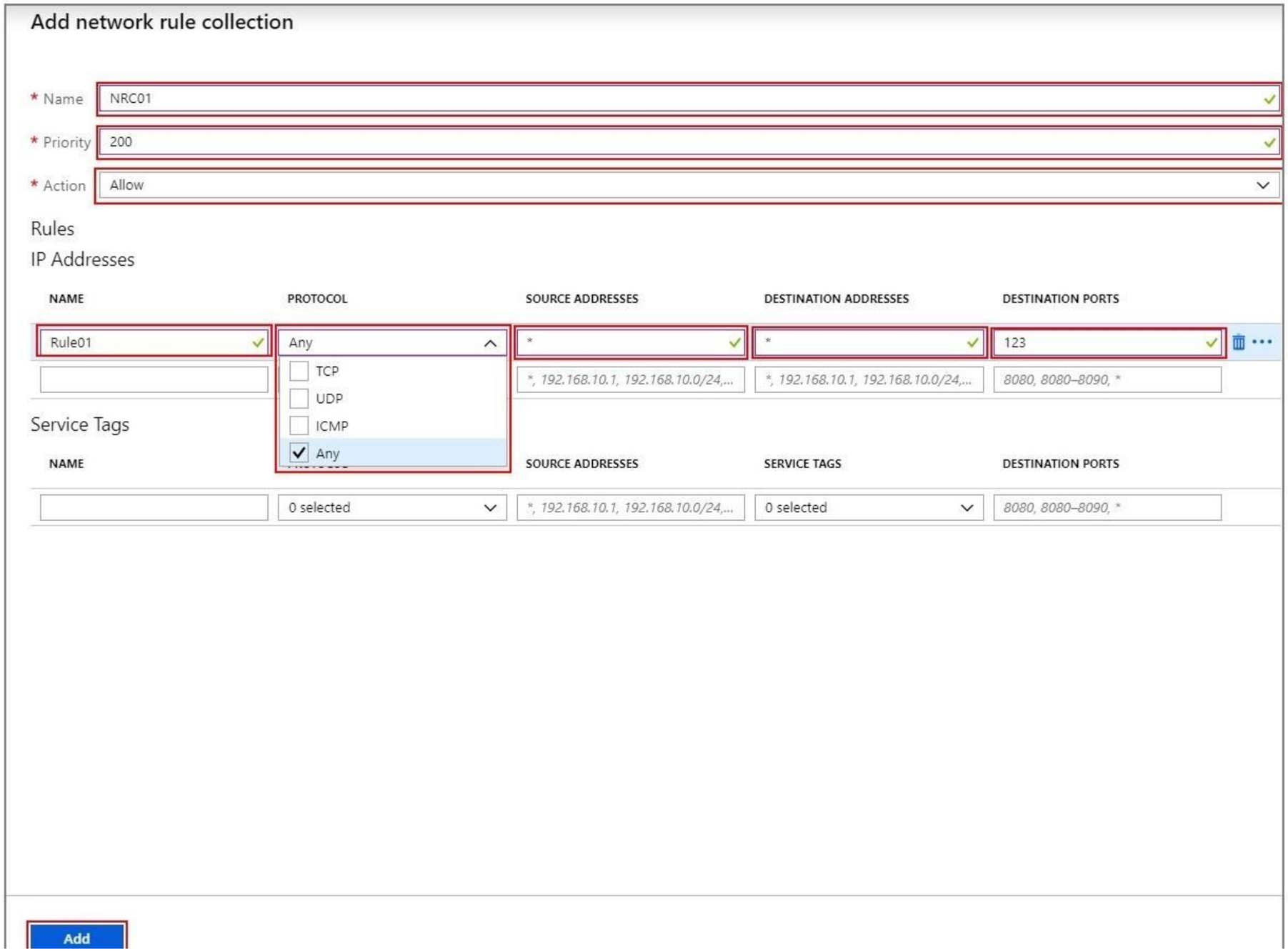
Step 1: Navigate to Network rule collection > + Add network rule collection.

Step 2: On the Add network rule collection screen, provide the following information:
Top Section

Name: SomeRule
Priority: 200
Action; Block

Service section
Name: Rule_1

Protocols: HTTP, HTTPS
Source addresses: subnet1-1
Destination addresses: *
Destination ports: *



Step 3: Select Add.

Reference:
https://learn.microsoft.com/en-us/azure/hdinsight/hdinsight-restrict-outbound-traffic
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-inbound-and-outbound-internet-connectivity

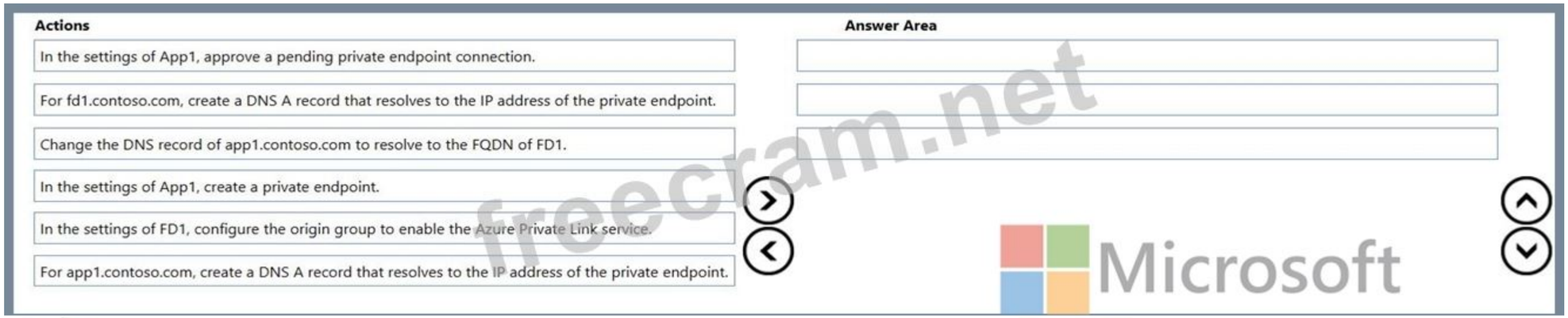
NEW QUESTION: 83
You are planning the IP addressing for the subnets in Azure virtual networks.
Which type of resource requires IP addresses in the subnets?
A. storage account
B. internal load balancers
C. service endpoints
D. service endpoint policies
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Drag and Drop Question
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

freeexam.net
Microsoft

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.



freecram.net

Actions

For fd1.contoso.com, create a DNS A record that resolves to the IP address of the private endpoint.

In the settings of App1, create a private endpoint.

For app1.contoso.com, create a DNS A record that resolves to the IP address of the private endpoint.

Answer Area

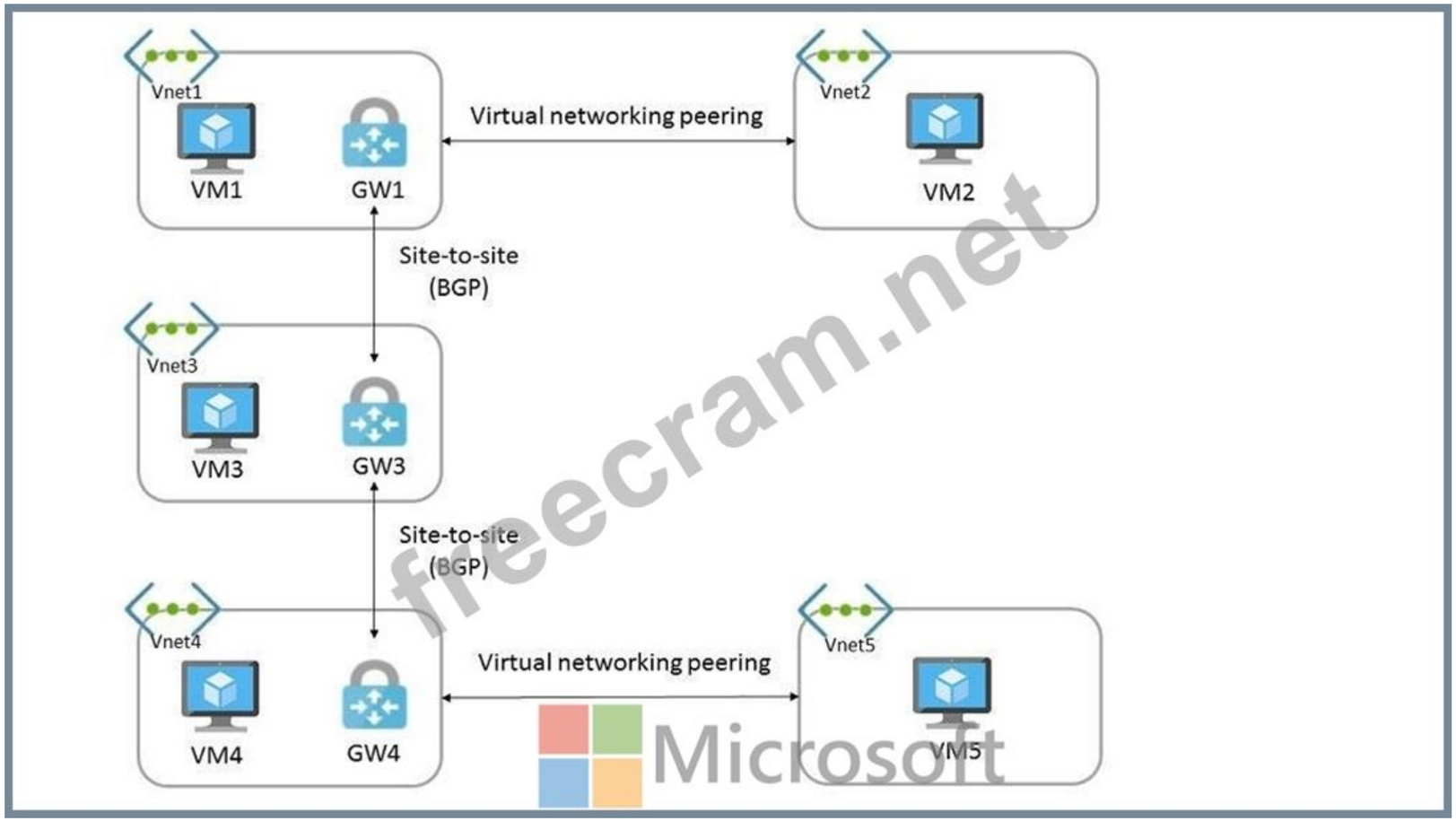
Change the DNS record of app1.contoso.com to resolve to the FQDN of FD1.

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.

NEW QUESTION: 85
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. Increase the number of frontend IP configurations for LB1.
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. Redeploy LB1 with a different SKU.
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview

NEW QUESTION: 86
Hotspot Question
You have the Azure environment shown in the exhibit.



You have virtual network peering between Vnet1 and Vnet2. You have virtual network peering between Vnet4 and Vnet5. The virtual network peering is configured as shown in the following table.

Virtual network	Traffic to remote virtual network	Use remote gateway	Allow gateway transit
Vnet1	Allow	**None**	Enabled
Vnet2	Allow	Enabled	**None**
Vnet4	Allow	**None**	Enabled
Vnet5	Block	Enabled	**None**

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

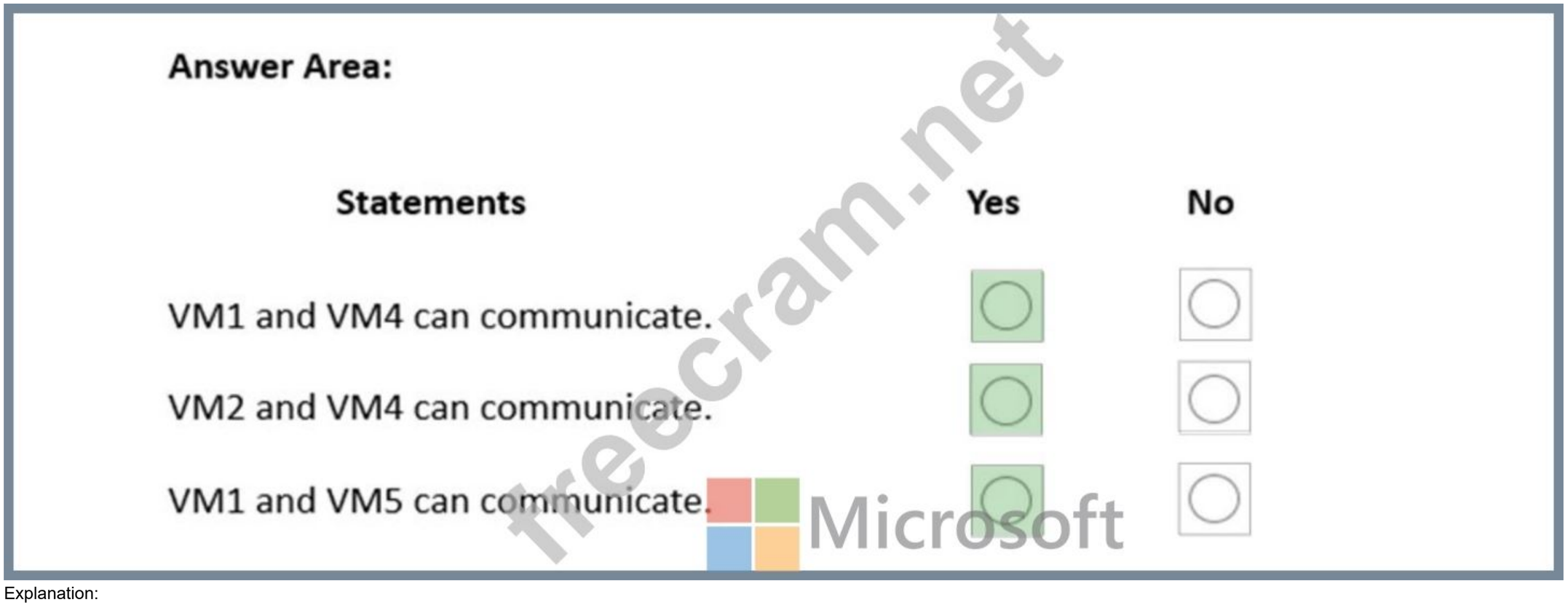
NOTE: Each correct selection is worth one point.

Answer Area:

Statements	Yes	No
VM1 and VM4 can communicate.	○	○
VM2 and VM4 can communicate.	○	○
VM1 and VM5 can communicate.	○	○

freecram.net
Microsoft

Answer:

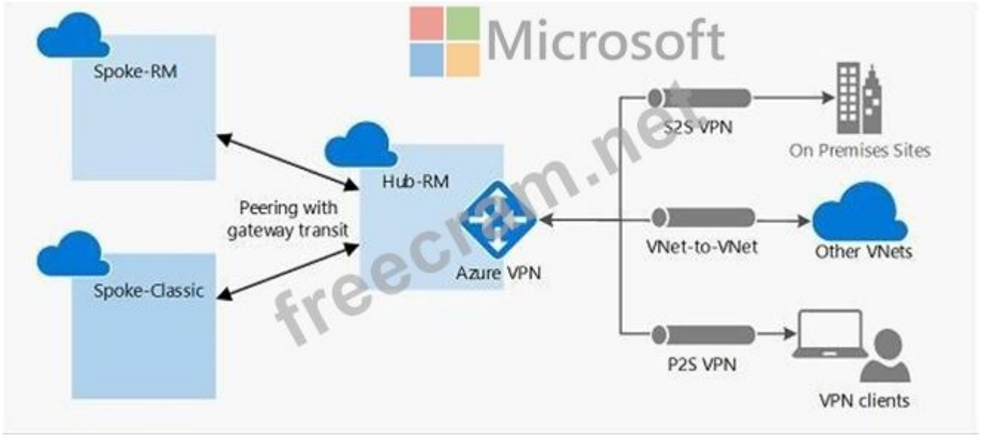


Explanation:

Box 1: Yes

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes. Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to- VNet connectivity.

The following diagram shows how gateway transit works with virtual network peering.



In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual networks.

In hub-and-spoke network architecture, gateway transit allows spoke virtual networks to share the VPN gateway in the hub, instead of deploying VPN gateways in every spoke virtual network.

Box 2: Yes

VM2 uses the remote gateway GW1 to reach VM4.

Box 3: Yes

Traffic to remove virtual network: Block' setting in Vnet5 does not block communication between VM5 and GW4, while it blocks communication between VM5 and VM4.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-troubleshoot-peering-issues

NEW QUESTION: 87

Case Study 3 - Contoso, Ltd

Overview

Proseware, Inc. is a financial services company that has a main office in New York City and a branch office in San Francisco.

Existing Environment. Hybrid Environment

Proseware has an on-premises Active Directory Domain Services (AD DS) forest named corp.proseware.com that syncs with a Microsoft Entra tenant named proseware.com.

Proseware has an Azure subscription that is linked to proseware.com.

Proseware has an internal certification authority (CA).

Existing Environment. Network Infrastructure

The offices contain the resources shown in the following table.

Name	Type	Office	Description
NYCNet	On-premises network	New York City	IP address space of 192.168.0.0/22
SFONet	On-premises network	San Francisco	IP address space of 192.168.100.0/22
NYCDNS1	Server	New York City	DNS server that runs Windows Server 2019 and has an IP address of 192.168.0.100

NYCNet connects to Azure by using an ExpressRoute circuit.

SFONet connects to Azure by using a Site-to-Site (S2S) VPN.

Existing Environment. Azure Resources

The Azure subscription contains the virtual networks and subnets shown in the following table.

Name	Type	Location	Description
HubVNet	Virtual network	East US Azure region	IP address space of 10.0.0.0/20 peered to SpokeVNet
SpokeVNet	Virtual network	East US Azure region	IP address space of 10.0.16.0/20 peered to HubVNet
VPNGW1	Virtual network gateway	HubVNet	Active-passive resiliency, in the Generation 2, VpnGw3 SKU that has the default ASN connected to SFONet
SUBNET-PE	Subnet	HubVNet	Used for private endpoints
SUBNET-JUMPHOSTS	Subnet	HubVNet	Used for jump hosts
SUBNET-APPGW1	Subnet	SpokeVNet	Contains an Azure application gateway named APPGW1

The subscription contains four virtual machines named VM1, VM2, VM3, and VM4. VM1 and VM2 host an app named App1.

VM3 and VM4 host a web app named App2 that is accessed by using a FQDN of app2.proseware.com. Users access app2.proseware.com by using HTTP or HTTPS.

VM1, VM2, and VM4 are connected to SpokeVNet.

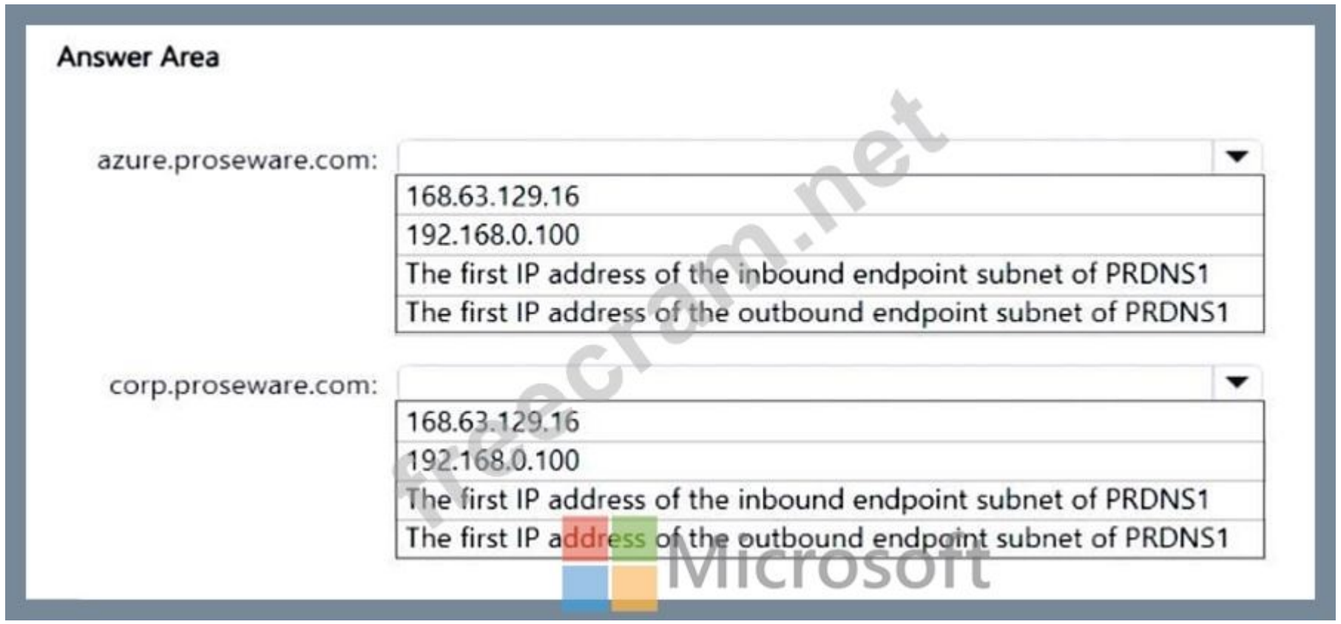
The subscription contains Application Gateway resources shown in the following table.

Name	Type	Location	Description
APPGW1	Application Gateway	SpokeVNet	In the Azure Web Application Firewall (WAF) V2 SKU Terminates HTTPS connections to a backend pool that contains VM3 and VM4
APPGW1-NSG1	Network security group (NSG)	East US region	Associated with SUBNET-APPGW1
APPGW1-WAFPolicy	Azure Web Application Firewall (WAF) policy	East US region	Applied to APPGW1

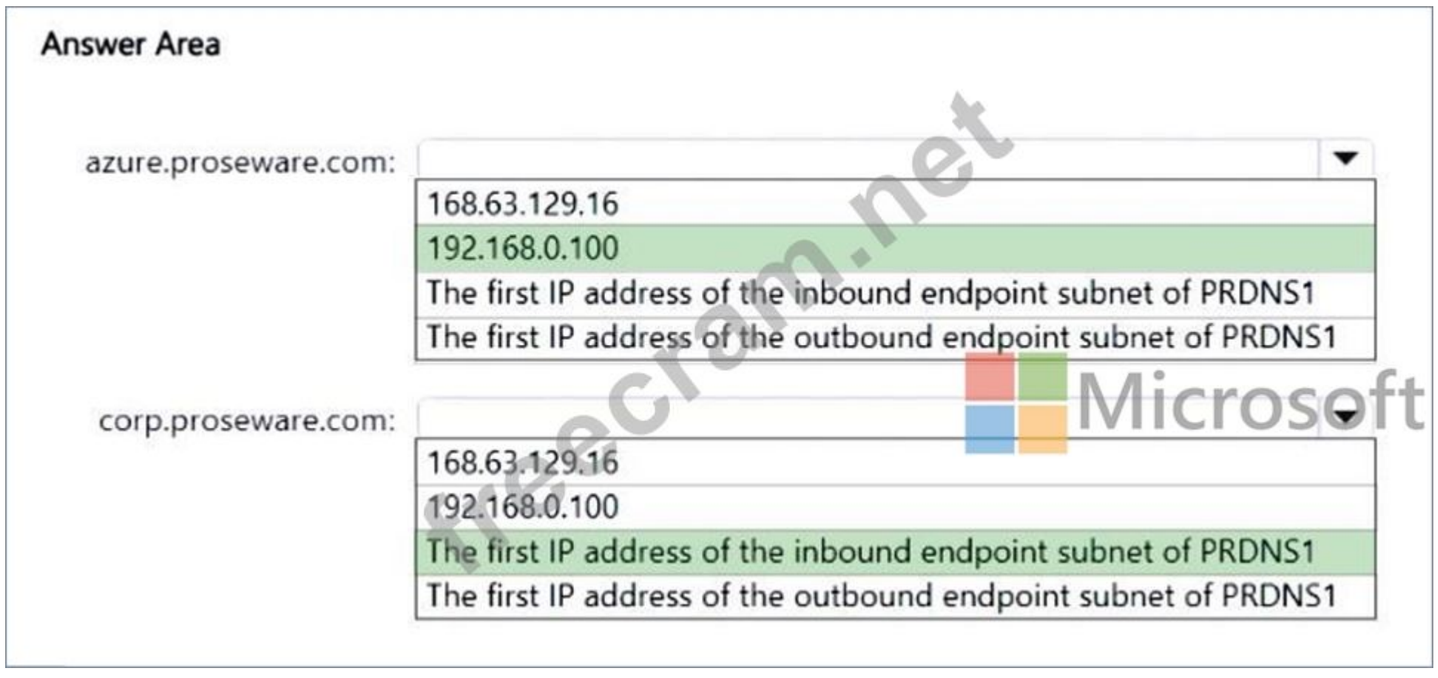
The subscription contains an Azure Front Door Standard profile named FD1. FD1 contains a single origin group that targets APPGW1 by using the default endpoint name.

HubVNet connects to NYCNet by using an ExpressRoute gateway named ERGW1.

Planned Changes and Requirements. Planned Changes
Proseware plans to implement the following changes:
- Deploy an Azure Private DNS Resolver named PRDNS1 to HubVNet and link PRDNS1 to SpokeVNet.
- Create a DNS forwarding ruleset named DNSRS1 and associate DNSRS1 with PRDNS1.
- Deploy Azure Virtual Network Manager and implement the following rules:
- Allow inbound connections on TCP port 3389 from the on-premises networks to SUBNET- JUMPHOSTS.
- Block inbound connections on TCP port 80 from the internet to SpokeVNet.
- Ensure that Azure Virtual Network Manager rules take precedence over conflicting NSG rules.
- Deploy two network virtual appliances (NVAs) named NVA1 and NVA2 to HubVNet.
- Deploy a gateway load balancer named LBGW1 to HubVNet.
- Configure LBGW1 to inspect traffic on TCP ports 443, 1433, and 1434 from LBS1 by using NVA1 and NVA2.
- Ensure that all the traffic to App2 is processed by using FD1.
Planned Changes and Requirements. Connectivity requirements
Proseware identifies the following connectivity requirements:
- Minimize the complexity of the Azure Virtual Network Manager deployment.
- Route traffic between NYCNet and SFONet via the ExpressRoute circuit and the S2S VPN.
- Ensure that remote users on Windows 11 devices can connect to HubVNet by using a Point-to- Site (P2S) VPN and their proseware.com credentials.
Planned Changes and Requirements. Security requirements
Proseware identifies the following security requirements:
- Whenever possible, use the internal CA.
- Ensure that all connections routed via APPGW1 use end-to-end encryption.
- Ensure that user connections to Azure-hosted apps use end-to-end encryption.
- Ensure that all inbound internet traffic to app2.proseware.com is routed via FD1.
- Prevent devices that connect to NYCNet from accessing Azure services that use private endpoints.
- Enable the virtual machines that connect to HubVNet and SpokeVNet to access Azure services that use private endpoints.
Planned Changes and Requirements. General requirements
Proseware identifies the following general requirements:
- Minimize the IP address space required to deploy platform-managed resources to the virtual networks.
- From SpokeVNet, resolve name resolution requests for the azure.proseware.com namespace and the corp.proseware.com namespace by using PRDNS1.
- Whenever possible, minimize administrative effort.
Hotspot Question
You are configuring the DNS forwarding ruleset for DNSRS1.
You need to configure the destination IP address for azure.proseware.com and for corp.proseware.com. The solution must meet the general requirements.
Which IP addresses should you configure for each namespace? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 88

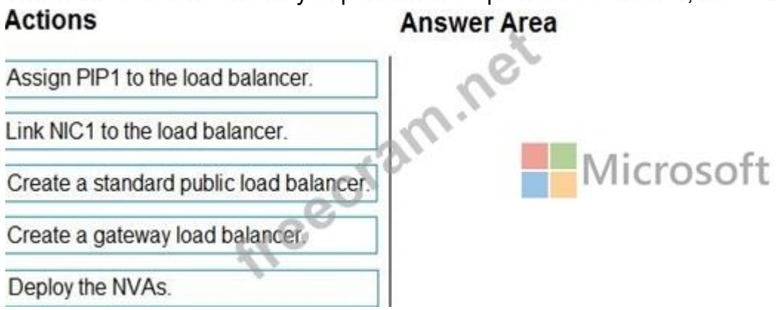
You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

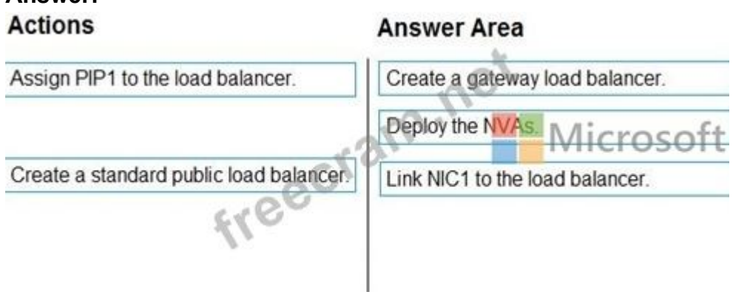
A. Azure Virtual Network NAT
B. virtual network peering
C. service endpoint policies
D. internal load balancers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 89
You are planning the IP addressing for the subnets in Azure virtual networks.
Which type of resource requires IP addresses in the subnets?
A. virtual network peering
B. service endpoints
C. internal load balancers
D. storage account
Answer: C (LEAVE A REPLY)

NEW QUESTION: 90
Drag and Drop Question
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.



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/load-balancer/tutorial-gateway-portal

NEW QUESTION: 91

Hotspot Question

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: Subnet12
- 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.

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:

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.	○	○

freecram.net

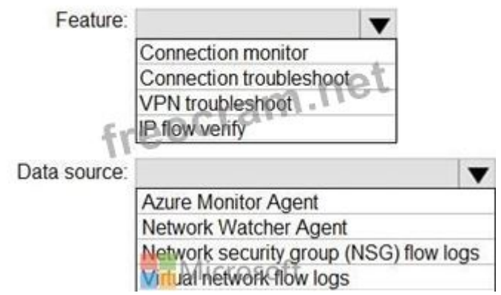
Explanation:
Basic LB needs vms to be in Avail set or VM scale set and in same vnet where LB is deployed but STD LB can load balance single VMs by adding single vms to backend pool but they also MUST be n same vNET where the LB is deployed.

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

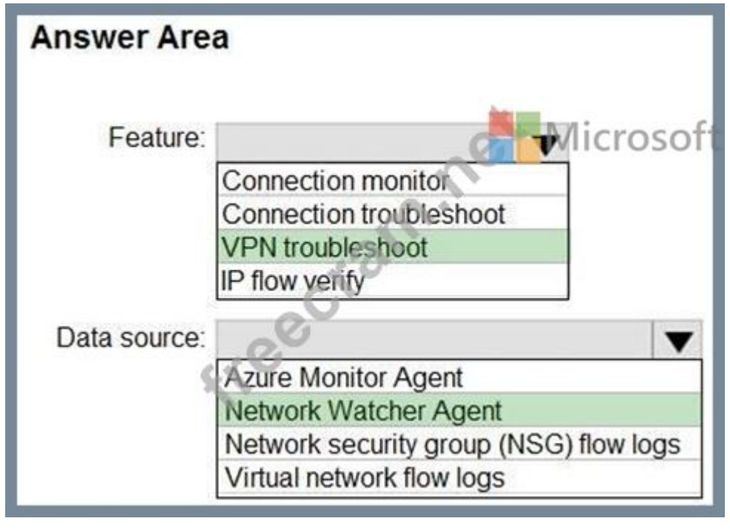
NEW QUESTION: 92
You have an application named App1 that listens for incoming requests on a preconfigured group of 50 TCP ports and UDP ports.
You install App1 on 10 Azure virtual machines.
You need to implement load balancing for App1 across all the virtual machines. The solution must minimize the number 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
Answer: (SHOW ANSWER)
App1 is installed on 10 VMs which can be put in a Backend pool. The req is to minimize the number of load balancing rules. If you select HA it will allow you to have 1 rule for TCP and UDP ports, if you don't select HA you will need to have a minimum of 2 rules for TCP and UDP with a * range.

ttps://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview

NEW QUESTION: 93
Hotspot Question
You have an Azure subscription that contains a virtual network named VNet1.
Your on-premises network connects to VNet1 by using a Site-to-Site (S2S) VPN connection.
You need to ensure that Azure Network Watcher generates an alert if the VPN connection fails.
Which Network Watcher feature should you use to generate the alert, and which data source should the feature query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area



Answer:



NEW QUESTION: 94
You have an Azure Front Door instance named FD that contains an origin group named OG1.
You need to configure a health probe for OG1. The solution must minimize the amount of traffic generated by the health probe.
Which HTTP method should you use?
A. CONNECT
B. HEAD

C. TRACE
D. GET
Answer: B (LEAVE A REPLY)
Azure Front Door supports the following HTTP methods for sending the health probes:
GET: The GET method means retrieve whatever information (in the form of an entity) gets identified by the Request-URI.
HEAD: The HEAD method is identical to GET except that the server MUST NOT return a message-body in the response. For new Front Door profiles, by default, the probe method is set as HEAD.
https://learn.microsoft.com/en-us/azure/frontdoor/health-probes

NEW QUESTION: 95
You have an on-premises server named Server1 that runs Windows Server.
You have an Azure subscription that contains a virtual network named VNet1.
You plan to connect Server1 to VNet1 by using Azure Network Adapter.
You need to minimize how long it takes to deploy the adapter to Server1.
What should you create first?
A. a route server
B. an Azure Bastion host
C. a private endpoint
D. an Azure VPN gateway
Answer: (SHOW ANSWER)
Considering that in the Microsoft process (here attached) for Azure Network adapter a VPN Gateway is included.
https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/use-azure-network-adapter

NEW QUESTION: 96
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a subnet named Subnet1.
You deploy an instance of Azure Application Gateway v2 named AppGw1 to Subnet1. You create a network security group (NSG) named NSG1 and link NSG1 to Subnet1.
You need to ensure that AppGw1 will only load balance traffic that originates from VNet1. The solution must minimize the impact on the functionality of AppGw1.
What should you add to NSG1?
A. an inbound rule that has a priority of 4096 and blocks all internet traffic
B. an outbound rule that has a priority of 4096 and blocks all internet traffic
C. an outbound rule that has a priority 100 and blocks all internet traffic
D. an inbound rule that has a priority of 100 and blocks all internet traffic
Answer: (SHOW ANSWER)

NEW QUESTION: 97
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 on-premises virtual machine.
What should you use?
A. Azure Monitor
B. IP flow verify
C. Connection Monitor
D. Azure Internet Analyzer

Answer: (SHOW ANSWER)
Connection Monitor provides unified, end-to-end connection monitoring in Azure Network Watcher. The Connection Monitor feature supports hybrid and Azure cloud deployments. Network Watcher provides tools to monitor, diagnose, and view connectivity-related metrics for your Azure deployments.
https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview

NEW QUESTION: 98
You have a network security group named NSG1.
You need to enable network security group (NS) 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 standard general-purpose v1 Azure Storage account
D. A premium Block blobs Azure Storage account
Answer: (SHOW ANSWER)
Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG. Flow data is sent to Azure Storage accounts from where you can access it as well as export it to any visualization tool, SIEM, or IDS of your choice.
https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview

NEW QUESTION: 99
You have an Azure subscription that contains the resources shown in the following table.

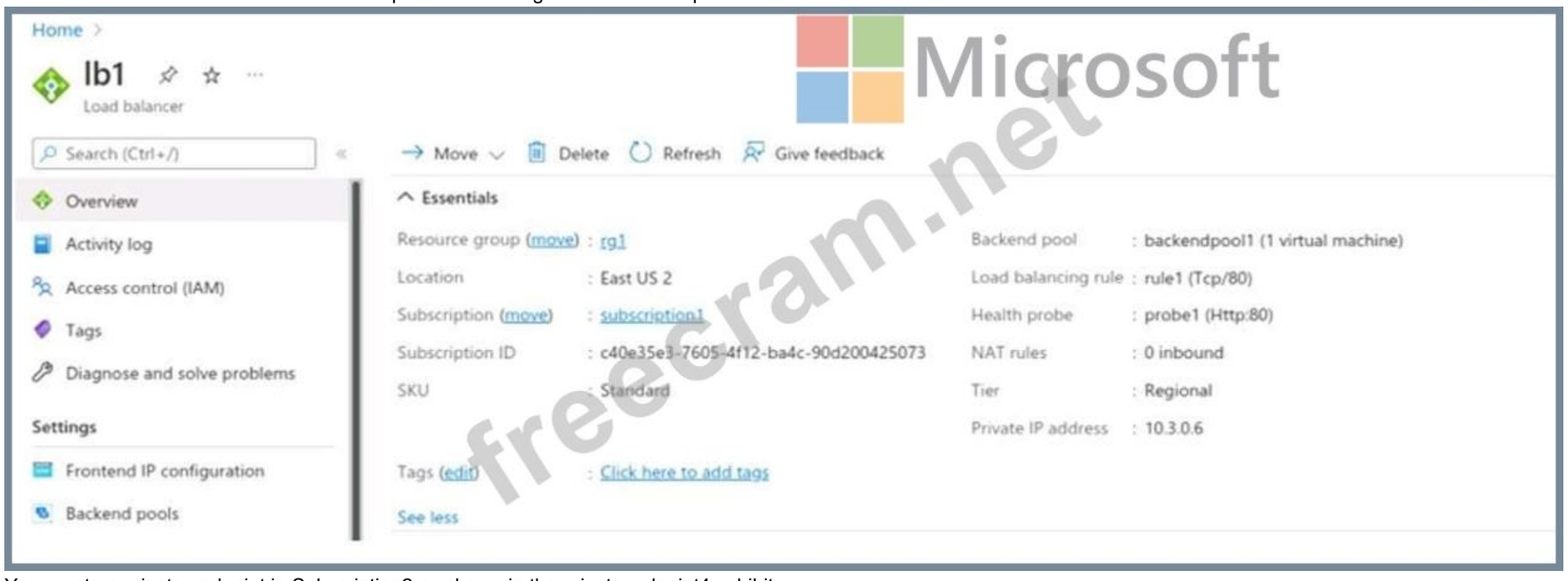
Name	Type	Description
App1	Azure App Service	A web app
Gateway1	Azure Application Gateway	includes an SSL certificate that has a subject name of *.contoso.com

Gateway1 provides access to App1 by using a URL of https://app1.contoso.com.
You create a new web app named App2.
You need to configure Gateway1 to enable access to App2 by using a URL of https://app2.contoso.com. The solution must 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
Answer: (SHOW ANSWER)
You can't use the same backend pool.

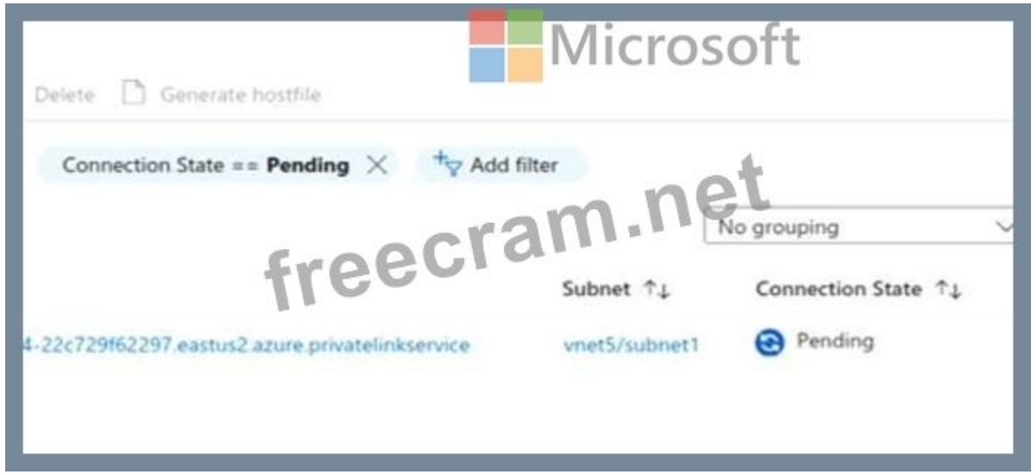
NEW QUESTION: 100
Hotspot Question
You have two Azure subscriptions named Subscription1 and Subscription2.
There are no connections between the virtual networks in two subscriptions.
You configure a private link service as shown in the privatelinkservice1 exhibit.



You create a load balancer name in Subscription1 and configure the backend pool shown in the lb1 exhibit.



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



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



Answer:



NEW QUESTION: 101

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the following subnets:

- AzureFirewallSubnet
- GatewaySubnet
- Subnet1
- Subnet2
- Subnet3

Subnet2 has a delegation to the Microsoft.Web/serverfarms service.

The subscription contains the resources shown in the following table.

Name	Type	Connected to
AZVNGW1	Azure VPN Gateway	GatewaySubnet
AZFW1	Azure Firewall Premium	AzureFirewallSubnet
VMSS1	Virtual machine scale set	Subnet1

You need to implement an Azure application gateway named AG1 that will be integrated with an Azure Web Application Firewall (WAF). AG1 will be used to publish VMSS1.
To which subnet should you connect AG1?

A. GatewaySubnet
B. AzureFirewallSubnet
C. Subnet2
D. Subnet1
E. Subnet3

Answer: (SHOW ANSWER)

An application gateway is a dedicated deployment in your virtual network. Within your virtual network, a dedicated subnet is required for the application gateway. You can have multiple instances of a given application gateway deployment in a subnet. You can also deploy other application gateways in the subnet. But you can't deploy any other resource in the application gateway subnet.

NEW QUESTION: 102

Case Study 2 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment:

Azure Network Infrastructure

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	**None**

freecram.net Microsoft

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

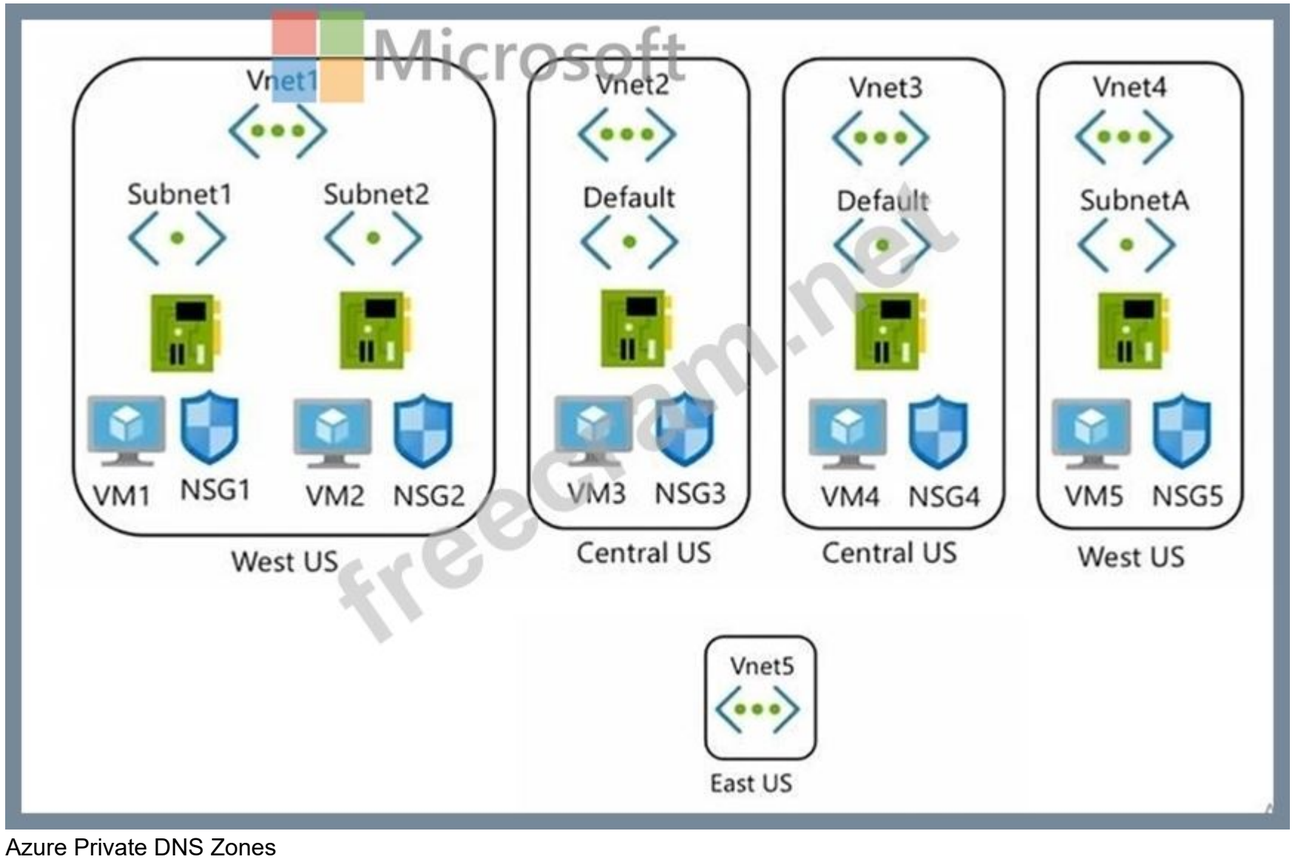
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1.

Azure Network Infrastructure Diagram



Azure Private DNS Zones

The Azure subscription contains the Azure private DNS zones shown in the following table.

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Requirements:

Virtual Network Requirements

Contoso has the following virtual networks requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

Two container groups that connect to Vnet6

Three virtual machines that connect to Vnet6

Allow VPN connections to be established to Vnet6

Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network

- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements

Contoso has the following network security requirements:

- Configure Azure Active Directory (Azure AD) authentication for Point- to-Site (P2S) VPN users.
- Enable NSG flow logs for NSG3 and NSG4.
- Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

- Create an NSG named NSG11 that will be associated to Vnet1/Subnet2
and will have the custom outbound security rules shown in the following table.

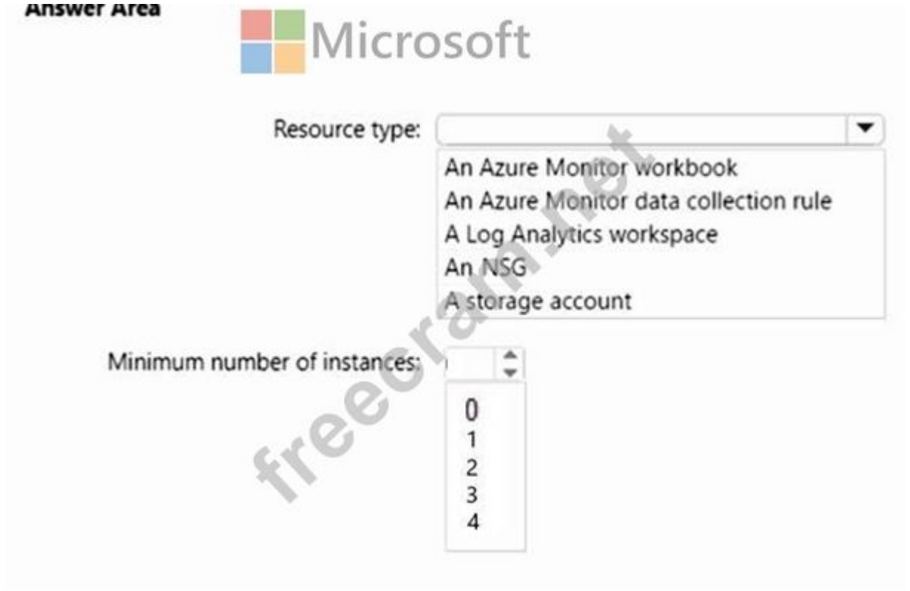
Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Hotspot Question

You need to meet the network security requirements for the NSG flow logs.

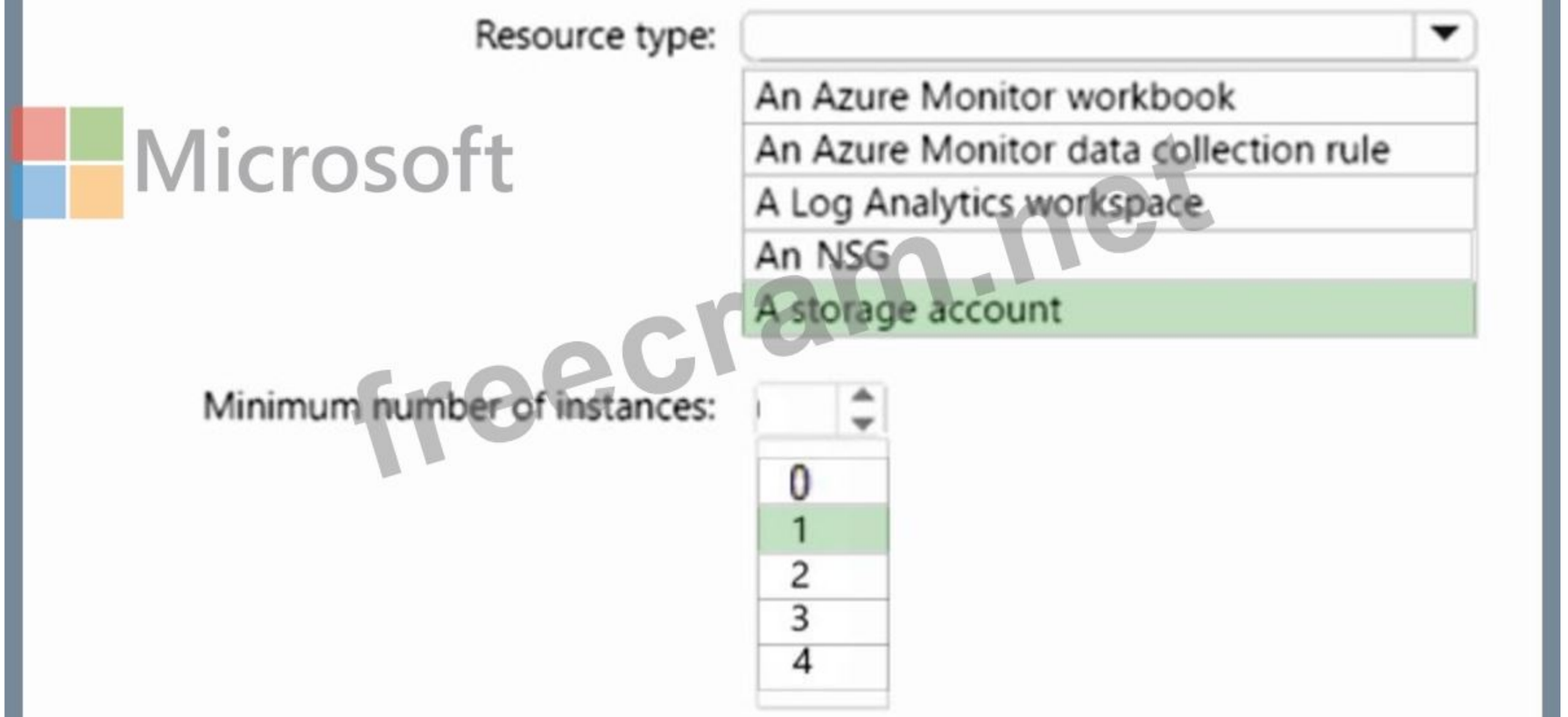
Which type of resource do you need, and how many instances should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Microsoft
freecram.net

NEW QUESTION: 103
Drag and Drop Question
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location
WebApp1	Web app	West US
VNet1	Virtual network	East US

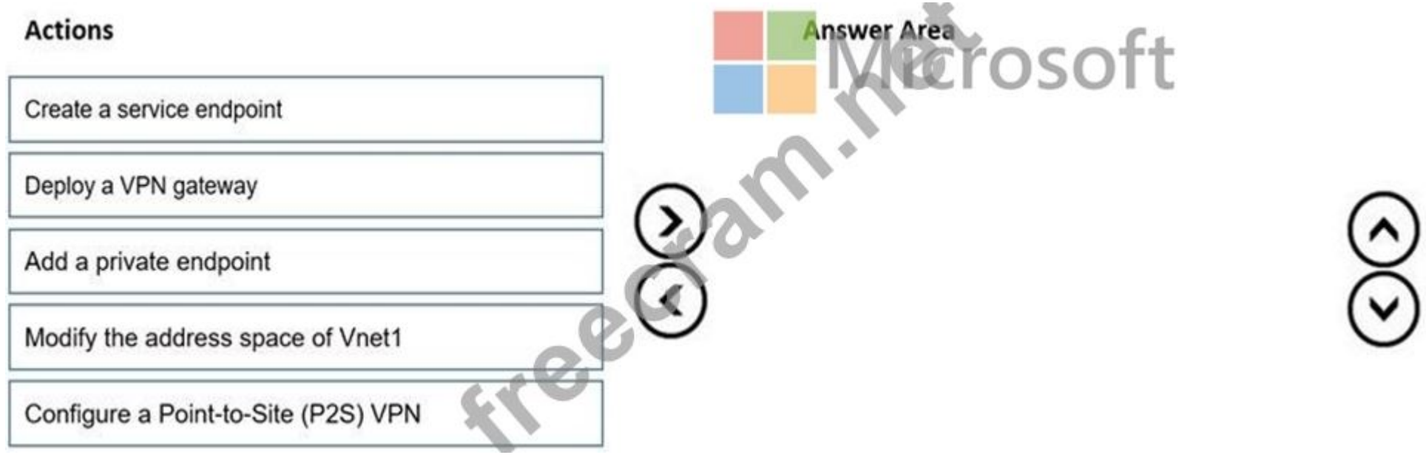
The IP Addresses settings for Vnet1 are configured as shown in the exhibit.



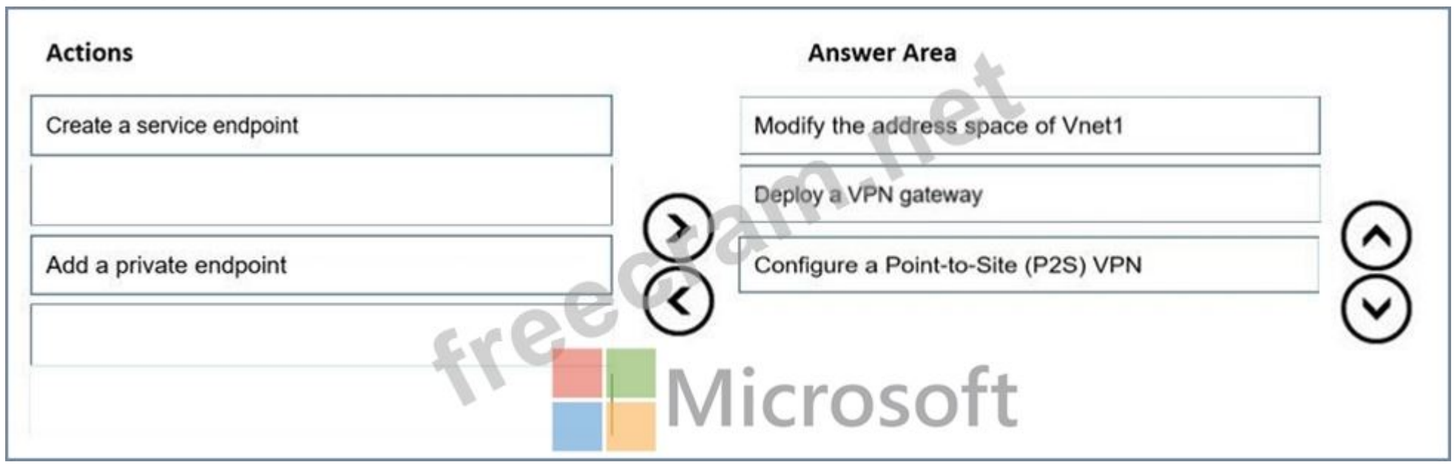
freecram.net
Microsoft

You need to ensure that you can integrate WebApp1 and Vnet1.

Which three actions should you perform in sequence before you can integrate WebApp1 and Vnet1? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:

Existing subnet space spans the entire address space of vnet, so it needs to be modified. Cross region vnet integration requires a vpn gateway and a point to site vpn connection. So you need to add the gateway, then configure the p2s to add address space.

https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required- vnet-integration

NEW QUESTION: 104

Hotspot Question

You have an Azure subscription that contains virtual networks, network security groups (NSGs), load balancer, virtual machines, and virtual network gateways.

You enable Azure Monitor Network Insights.

You need to perform the following actions:

- Review the NSG flow logs.
- Monitor resource utilization.
- Review the results of IP flow verify testing.

Which Azure Monitor Network Insights feature should you use for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area Microsoft

Review the NSG flow logs:

- Connectivity
- Diagnostic Toolkit
- Topology
- Network health
- Traffic

Monitor resource utilization:

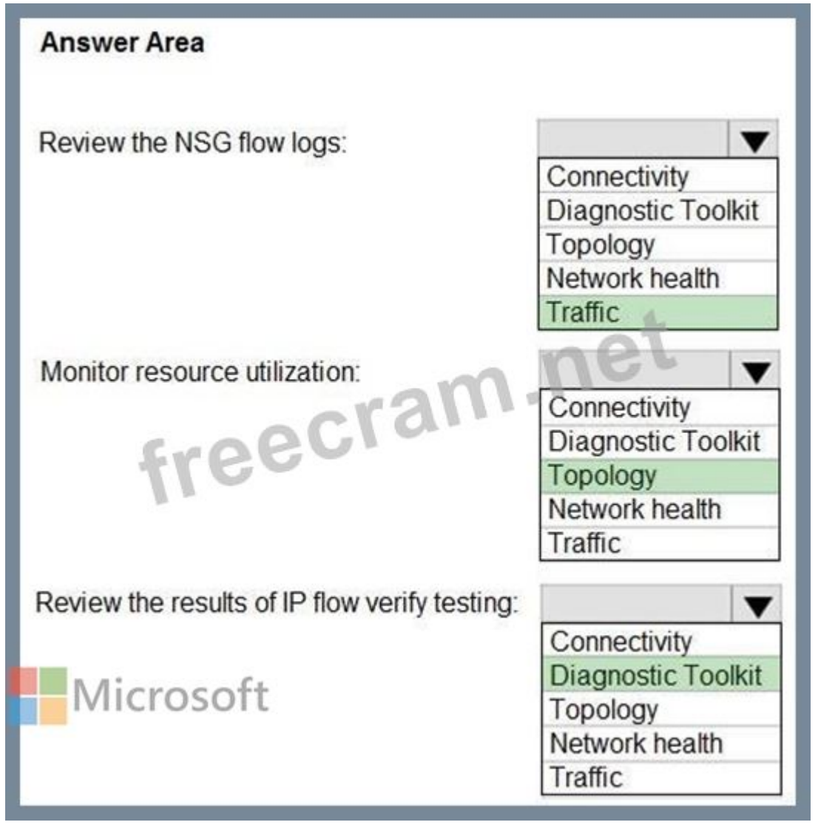
- Connectivity
- Diagnostic Toolkit
- Topology
- Network health
- Traffic

Review the results of IP flow verify testing:

- Connectivity
- Diagnostic Toolkit
- Topology
- Network health
- Traffic

freecram.net

Answer:



Explanation:

Box 1: Traffic

Traffic Analytics within Network Insights can be used to monitor network traffic to and from clusters and identify potential data exfiltration. This feature, also part of Azure Monitor Network Insights, leverages NSG flow logs to provide a comprehensive view of traffic flow, helping you identify potential security risks and optimize network configurations.

Box 2: Topology

To monitor resource utilization in your Azure network, use Network Watcher's Topology and Traffic Analytics features in conjunction with Azure Monitor's Metrics and Logs capabilities Azure Monitor Network Insights:

Topology:

Provides a visual representation of your Azure virtual network and connected resources, helping you understand the relationships between them. You can drill down into specific resources, like VMs, to see their traffic and connectivity insights and access diagnostic tools.

Box 3: Diagnostic Toolkit

Diagnostic Toolkit provides access to all the diagnostic features available for troubleshooting the network. You can use this drop-down list to access features like packet capture, VPN troubleshoot, connection troubleshoot, next hop, and IP flow verify:

Reference:

https://learn.microsoft.com/en-us/azure/network-watcher/network-insights-overview

NEW QUESTION: 105

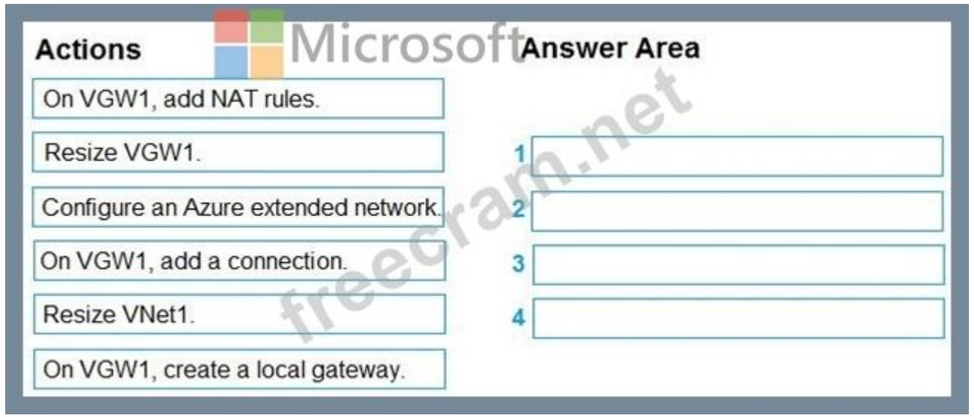
Drag and Drop Question

You have 100 on-premises servers with IP addresses from the 10.0.0.0/24 IP address space.

You have an Azure subscription that contains a virtual network named VNet1, an Azure VPN gateway named VGW1, and 100 virtual machines. VNet1 has an IP address space of 10.0.0.0/22. VGW1 uses the VpnGw1 SKU.

You need to ensure that the Azure virtual machines and the on-premises servers can communicate by using VGW1. The solution must minimize administrative effort.

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.



Answer:



NEW QUESTION: 106

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

Answer: (SHOW ANSWER)

Traffic Analytics requires the following prerequisites:

A Network Watcher enabled subscription.

Network Security Group (NSG) flow logs enabled for the NSGs you want to monitor.
An Azure Storage account, to store raw flow logs.
An Azure Log Analytics workspace, with read and write access.
https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq#what-are-the-prerequisites-to-use-traffic-analytics-

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
Basic and Standard are two types of virtual WANs. Both WANs support different configurations.
From the below-given options, select the configuration(s) that are available for Basic virtual WAN.
A. User VPN(P2S)
B. ExpressRoute
C. Azure Firewall
D. Site-to-site VPNright
Answer: (SHOW ANSWER)
Both Basic and Standard WANs support different types of configurations. The below-given table demonstrates the available configurations for each:
Option A is incorrect. Basic Virtual WAN supports only site-to-site VPN configuration.
Option B is incorrect. ExpressRoute is not the available configuration for Basic Virtual WAN.
Option C is incorrect. Azure Firewall is not the available configuration for Basic Virtual WAN.
Option D is correct. Basic Virtual WAN supports only site-to-site VPN configuration.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about?WT.mc_id=modinfra-33046-thmaure

NEW QUESTION: 108
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 machine operating systems were activated.
You need to ensure that the virtual machines can be activated.
What should you do?
A. On FW1, create an outbound service tag rule for AzureCloud.
B. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
C. Deploy an application security group that allows outbound traffic to 1688.
D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

Answer: (SHOW ANSWER)

NEW QUESTION: 109
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 private endpoint
C. a subnet delegation
D. an application security group
Answer: (SHOW ANSWER)
What is service tag in Azure?
Image result for azure service tags
A service tag represents a group of IP address prefixes from a given Azure service. ... You can use service tags to define network access controls on network security groups or Azure Firewall.
Use service tags in place of specific IP addresses when you create security rules.
https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview

NEW QUESTION: 110
You have an Azure subscription that contains a virtual network named VNet1.
You plan to deploy Point-to-Site (P2S) VPN access to VNet1.
You need to recommend an authentication method for the deployment. The solution must meet the following requirements:
- Require the use of a FIDO2 security key
- Analyze user sign-in behavior
- Require a user to change their password if their sign-in behavior is identified as risky
What should you recommend?
Freecram.net
A. Azure certificate
B. Microsoft Entra
C. RADIUS
D. smart card
Answer: (SHOW ANSWER)

NEW QUESTION: 111
You are the team leader and you are addressing your team about the load balancing and various Azure load balancing services.
Which of the following statements would you use to describe the Azure Front Door load balancing service?
A. a DNS-based traffic load balancing service that allows optimal distribution of the traffic to services across global Azure regions, offering high responsiveness and availability
B. load balancing option that offers application delivery controller (ADC) as a service, supporting different Layer 7 load balancing capabilities.
C. a high-performance and ultra low-latency Layer 4 load balancing service (inbound & outbound) for all TCP and UDP protocols.
D. An application delivery network that offers global load balancing and site acceleration services for web applications with its layer 7 capabilities
Answer: (SHOW ANSWER)
Azure Front Door is an application delivery network that offers global load balancing and site acceleration services for web applications. It provides Layer seven capabilities for applications such as SSL offload, fast failover,

path-based routing, caching, etc. to enhance the performance and availability of applications.
Option A is incorrect. The given statement describes the Traffic Manager, not Front Door.
Option B is incorrect. The application gateway offers an application delivery controller (ADC) as a service, supporting different Layer 7 load balancing capabilities.
Option C is incorrect. Azure Load Balancer is a high-performance and ultra low-latency Layer 4 load balancing service (inbound & outbound) for all TCP and UDP protocols.
Option D is correct. The given statement rightly describes the Azure Front Door.
Reference:
https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing- overview

NEW QUESTION: 112
You have the Azure Traffic Manager profiles shown in the following table.

Name	Routing method
Profile1	Performance
Profile2	Multivalue

You plan to add the endpoints shown in the following table.

Name	Type	Additional settings
Endpoint1	Azure endpoint	Target resource type: App Service
Endpoint2	External endpoint	FQDN or IP: www.contoso.com
Endpoint3	External endpoint	FQDN or IP: 131.107.10.15
Endpoint4	Nested endpoint	Target resource: Profile1

Which endpoints can you add to Profile2?
A. Endpoint1 and Endpoint4 only
B. Endpoint1, Endpoint2, Endpoint3, and Endpoint4
C. Endpoint1 only
D. Endpoint2 and Endpoint3 only
E. Endpoint3 only
Answer: (SHOW ANSWER)
Multivalue traffic-routing method
The Multivalue traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response. This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive. This pattern can increase the availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint.
MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses. When a query is received for this profile, all healthy endpoints are returned and are subject to a configurable maximum return count.
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing- methods#multivalue

NEW QUESTION: 113
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 2

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 and IP3 only
B. IP3 only
C. IP3 and IP5 only
D. IP2 only
E. IP1, IP2. IP3. IP4. and IP5
F. IP1, IP3, IP4, and 1P5 only

Answer: B (LEAVE A REPLY)

Public LBs are regional and require a standard SKU PIP.

NEW QUESTION: 114

Hotspot Question

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:

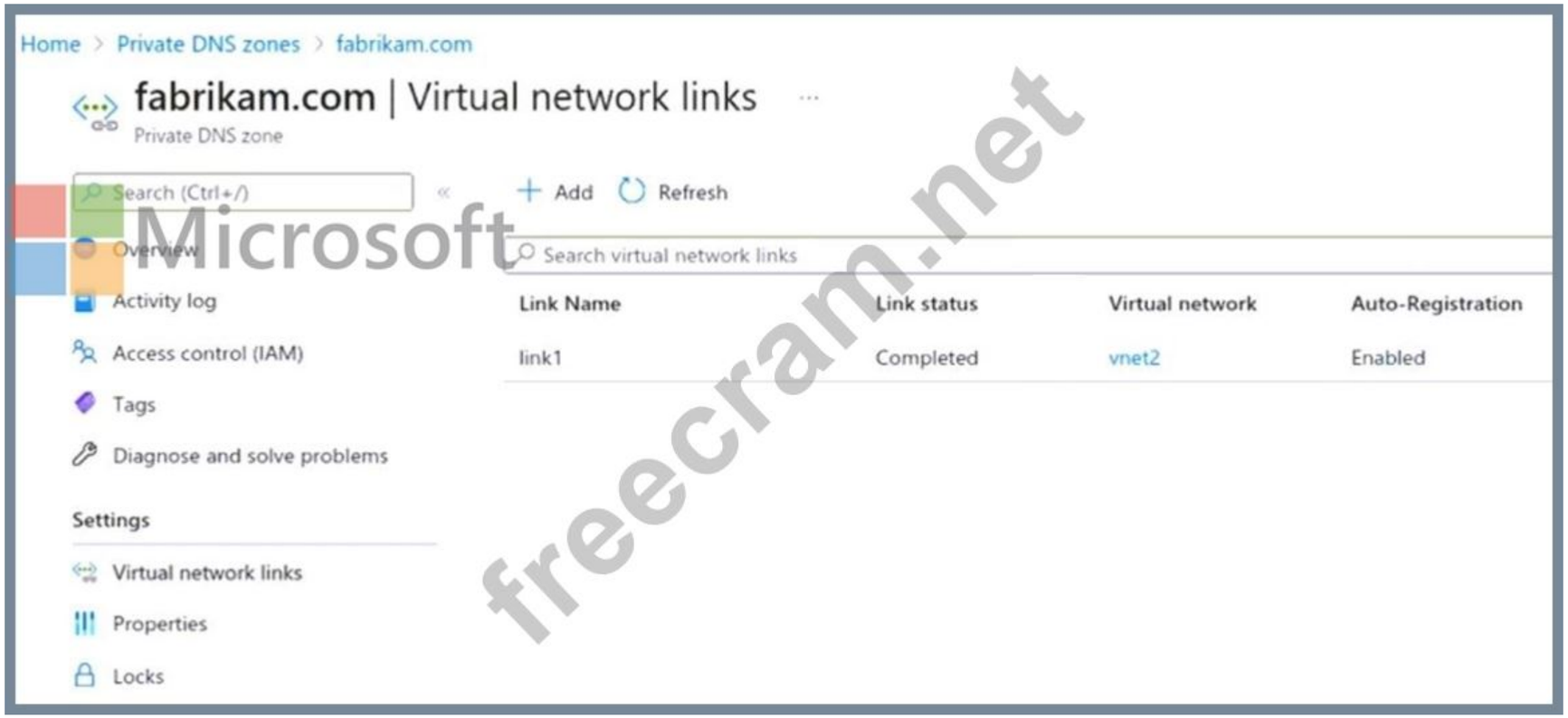
- IP address:10.4.0.5
- Subnet mask:255.255.255.0
- Default gateway: 10.4.0.1
- DNS server: 168.63.129.16

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 zone are configured as shown in the exhibit.

(Click the Exhibit tab.)



VM5 fails to resolve the IP address for app1.fabrikam.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.

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.	○	○

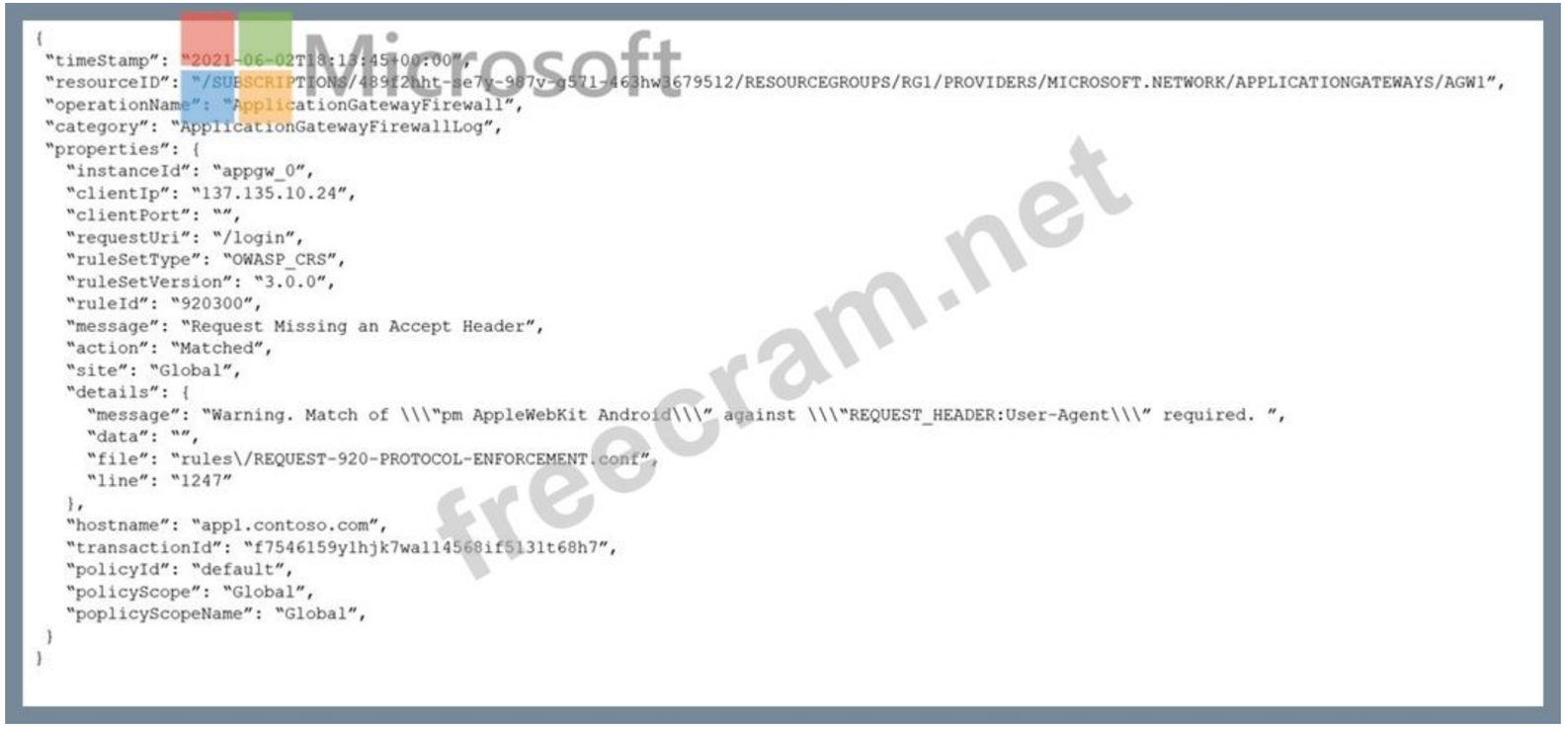
Answer:

Microsoft
freecram.net



Explanation:
VM5 is in VNET3 and VNET3 isn't linked to the fabrikam.com private DNS zone. This means it won't be able to resolve anything in that private DNZ zone until it is linked.

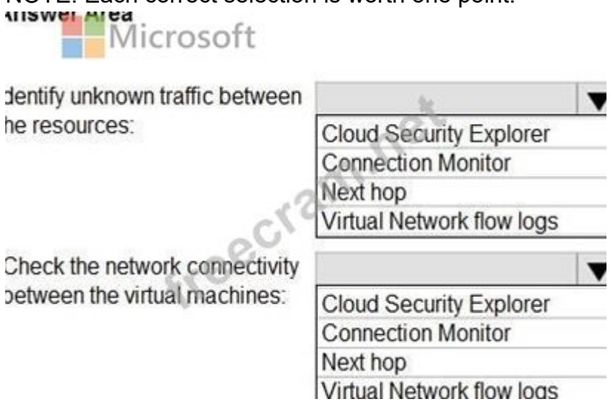
NEW QUESTION: 115
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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.



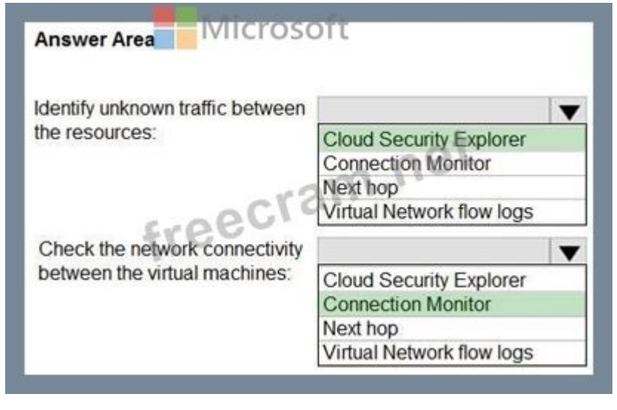
You need to ensure that the URL is accessible through the application gateway.

Solution: You disable the WAF rule that has a ruleId 920300.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
The log shows that WAF rule with ruleId 920300 was trigged. We should disable the WAF rule that has a ruleId 920300.
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall- troubleshoot

NEW QUESTION: 116
Hotspot Question
You have an Azure subscription that contains virtual networks, network security groups (NSGs), and virtual machines.
You need to perform the following actions:
- Identify unknown traffic between the resources.
- Check the network connectivity between the virtual machines.
What should you use to perform each action? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



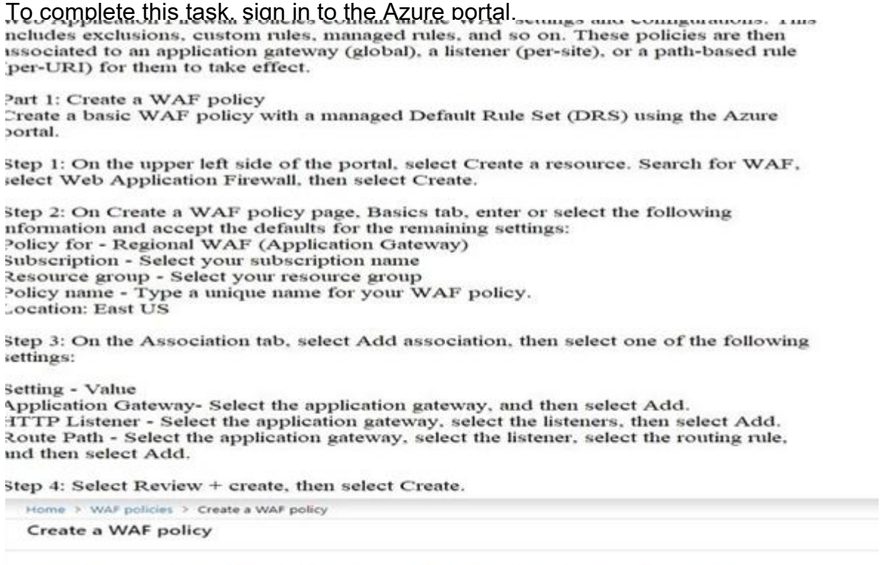
Answer:



NEW QUESTION: 117
SIMULATION



Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
- If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You plan to implement an Azure application gateway in the East US Azure region. The application gateway will have Web Application Firewall (WAF) enabled.
You need to create a policy that can be linked to the planned application gateway. The policy must block connections from IP addresses in the 131.107.150.0/24 range. You do NOT need to provision the application gateway to complete this task.
To complete this task, sign in to the Azure portal.


ncludes exclusions, custom rules, managed rules, and so on. These policies are then
ssociated to an application gateway (global), a listener (per-site), or a path-based rule
per-URI) for them to take effect.

Part 1: Create a WAF policy
Create a basic WAF policy with a managed Default Rule Set (DRS) using the Azure
portal.

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

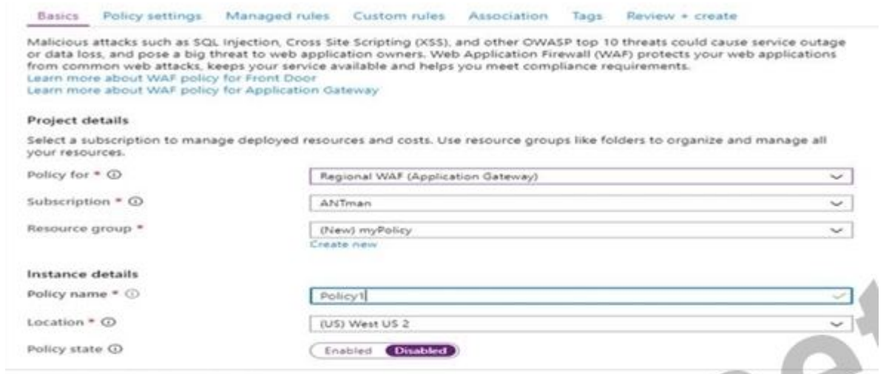
Step 2: On Create a WAF policy page, Basics tab, enter or select the following
nformation and accept the defaults for the remaining settings:
Policy for - Regional WAF (Application Gateway)
Subscription - Select your subscription name
Resource group - Select your resource group
Policy name - Type a unique name for your WAF policy.
Location: East US

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

Setting - Value
Application Gateway- Select the application gateway, and then select Add.
HTTP Listener - Select the application gateway, select the listeners, then select Add.
Route Path - Select the application gateway, select the listener, select the routing rule,
nd then select Add.

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

Home > WAF policies > Create a WAF policy
Create a WAF policy

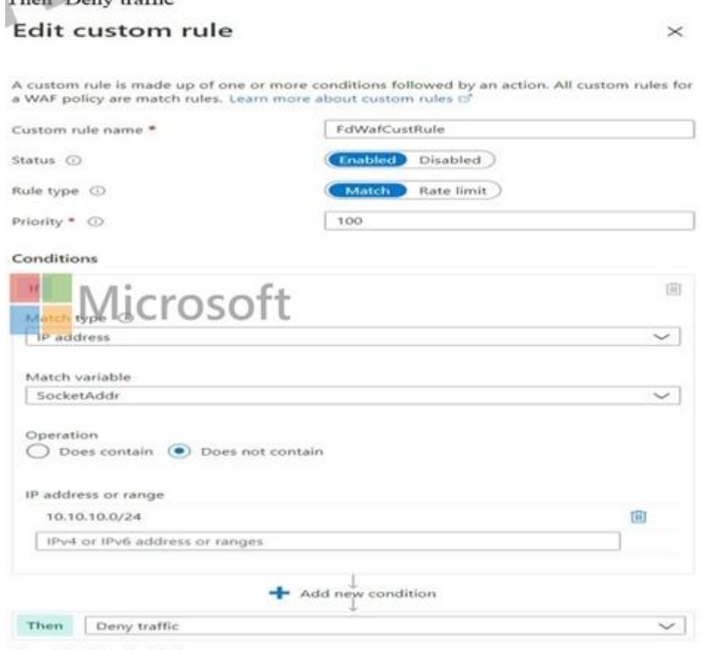


Part 2: Configure WAF rule

When you create a WAF policy, by default it is in Detection mode. In Detection mode, WAF doesn't block any requests. Instead, the matching WAF rules are logged in the WAF logs. To see WAF in action, you can change the mode settings to Prevention. In Prevention mode, matching rules defined in the CRS Ruleset you selected are blocked and/or logged in the WAF logs.

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

Step 6: On the Add custom rule page, use the following test values to create a custom rule:
Setting - Value
Custom rule name - AnyName
Status - Enabled
Rule type- Match
Priority - 100
Match type- IP address
Match variable - SocketAddr (for example)
Operation - Does contain
IP address or range - 131.107.150.0/24
Then Deny traffic



Step 7: Select Add.

Step 8: Select Next: Association.
Step 9: Select Associate a WAF policy.
Step 10: For WAF policy, select your WAF policy

Microsoft
Pecram.net

Step 10: For WAF policy, select your WAF policy.
Step 11: For Domain, select the domain.
Step 12. Select Add.
Step 13: Select Review + create.
Step 14: After your policy validation passes, select Create.

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

NEW QUESTION: 118

Drag and Drop Question

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2.

You plan to deploy the resources shown in the following table.

Name	Type	On virtual network	Description
VMSS1	Virtual machine scale set	VNet1	Each virtual machine hosts an application named App1
VM1	Virtual machine	VNet2	Is a network virtual appliances (NVA)
VM2	Virtual machine	VNet2	Is a network virtual appliances (NVA)

You need to deploy two load balancers to manage the traffic for VMSS1, VM1, and VM2. The solution must meet the following requirements:

- Either VM1 or VM2 must inspect all the traffic from the internet to App1.
- All user connections from the internet to App1 must be load balanced.
- Costs must be minimized.

Which load balancer SKU should you include in the solution? To answer, drag the appropriate SKUs to the correct resources. Each SKU 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.

SKUs **Answer Area**

Basic
Gateway
Standard

VMSS1: [ ]
VM1 and VM2: [ ]

Answer:

SKUs **Answer Area**

Standard

VMSS1: Basic
VM1 and VM2: Gateway

Explanation:

Box 1: Basic

Basic load balancer supports Virtual machines in a single availability set or virtual machine scale set.

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

Box 2: Gateway

Gateway Load Balancer is a SKU of the Azure Load Balancer portfolio catered for high performance and high availability scenarios with third-party Network Virtual Appliances (NVAs).

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

With the capabilities of Gateway Load Balancer, you can easily deploy, scale, and manage NVAs.

NEW QUESTION: 119

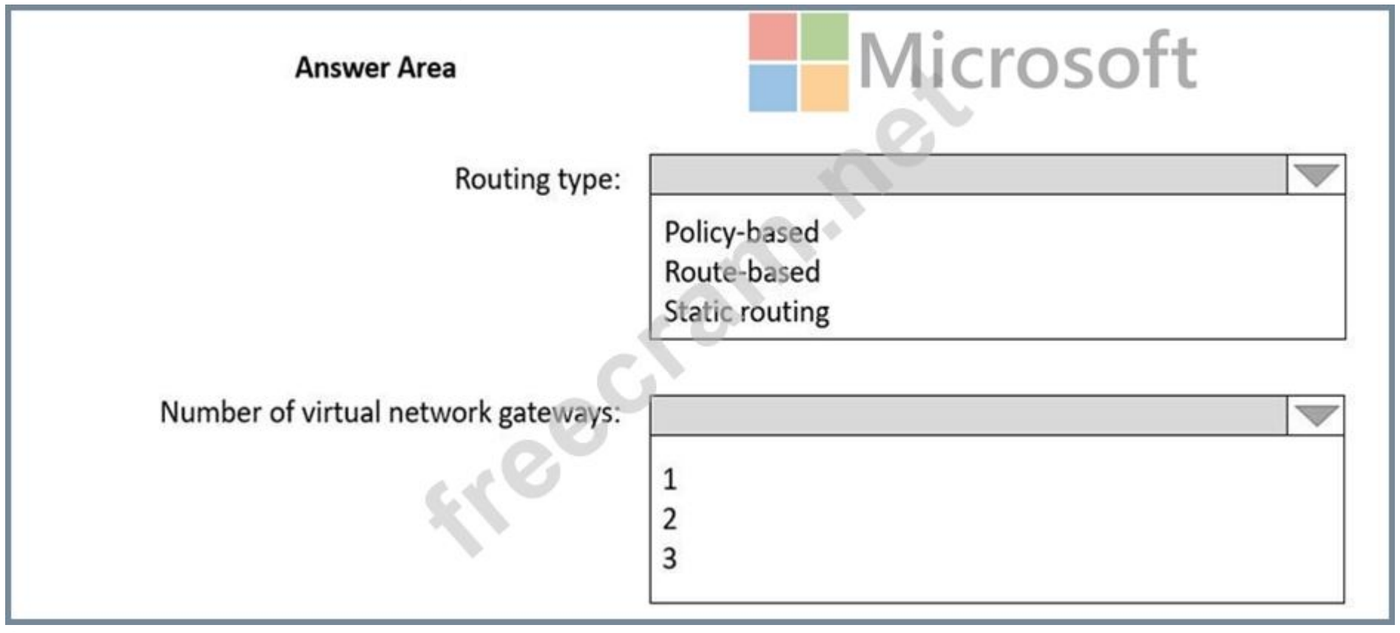
Hotspot Question

You need to connect an on-premises network and art Azure environment.

The solution must use ExpressRoute and support failing over to a Site-to Site VPN connection if there is an ExpressRoute failure.

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

NOTE: Each correct selection is worth one point.



Answer:

Answer Area

Routing type:

- Policy-based
- Route-based
- Static routing

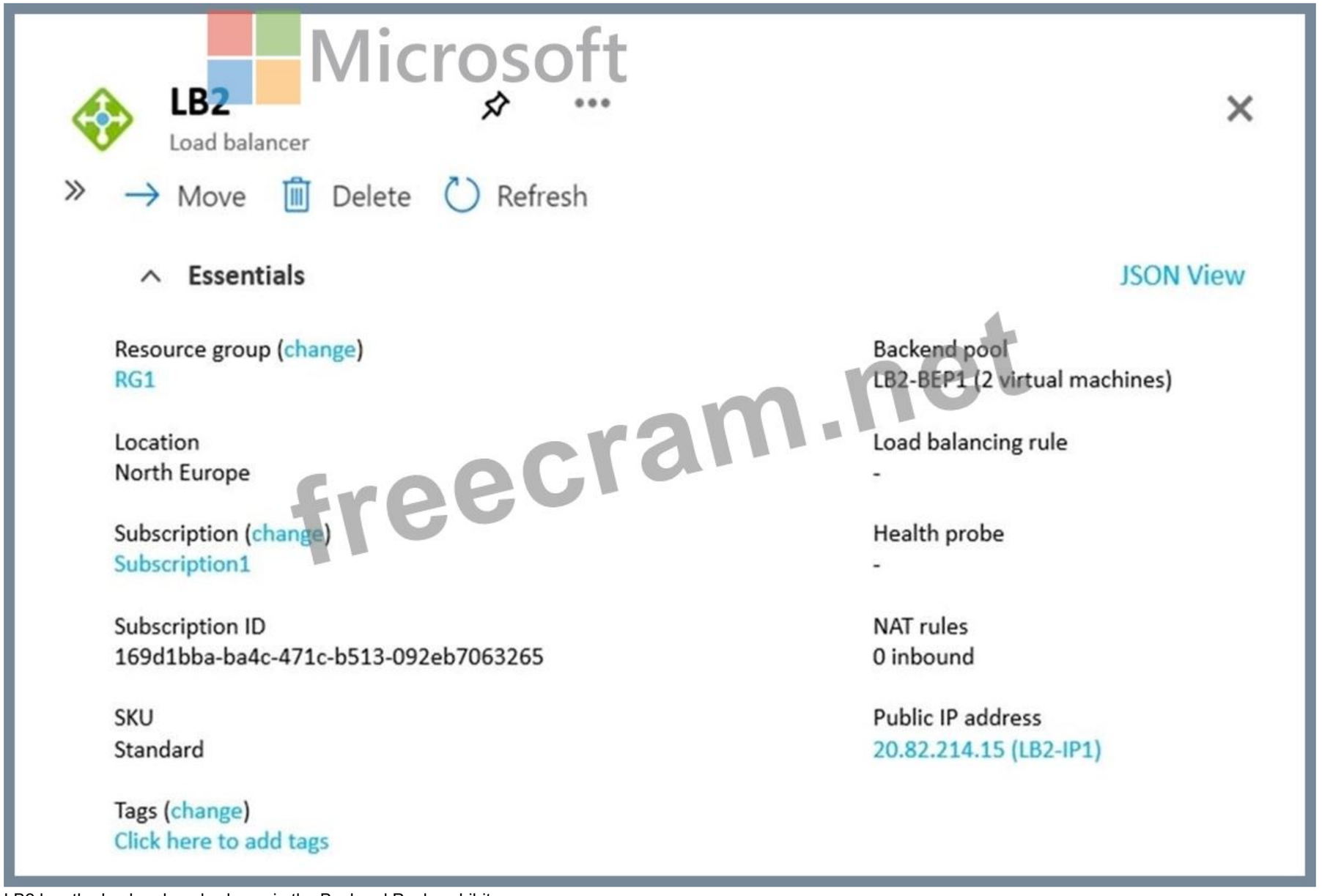
Number of virtual network gateways:

- 1
- 2
- 3

freecram.net

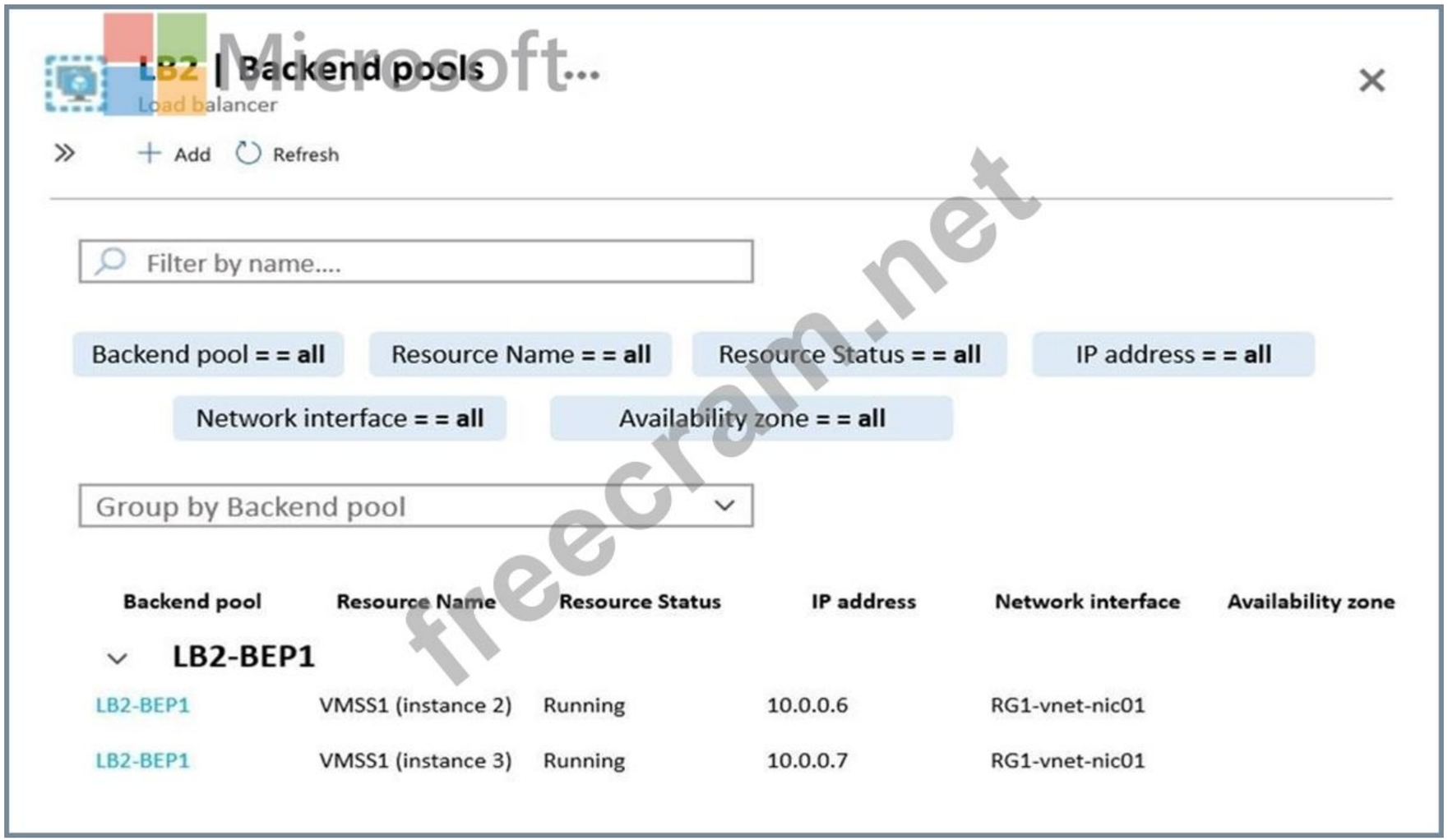
Explanation:
The answer is Route Based and 2 Virtual Network Gateways.
Both the Expressroute and VPN need distinct gateways identified by their SKU. You cannot have Expressroute on a VpnGw SKU. It must be on a dedicated ExpressRoute SKU gateway.
Both VPN Gateways will exist inside the same subnet but the connection are via 2 separate gateways.
This doc clearly shows the step of create 2 gateways.
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource- manager

NEW QUESTION: 120
You have the Azure load balancer shown in the Load Balancer exhibit.



Microsoft
freecram.net

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



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. Configure a health probe.

C. Add a public IP address to each member of VMSS1.

D. Add a load balancing rule.

Answer: (SHOW ANSWER)

https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public- portal?tabs=option-1-create-load-balancer-standard

NEW QUESTION: 121

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

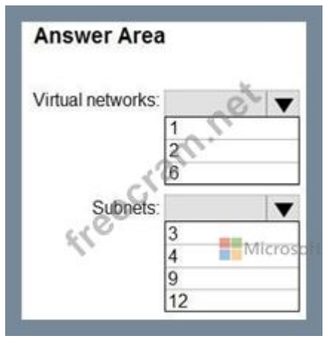
After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machine operating systems were activated.
You need to ensure that the virtual machines can be activated.
What should you do?

A. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.
B. Deploy a NAT gateway.
C. Deploy an application security group that allows outbound traffic to 1688.
D. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
Answer: (SHOW ANSWER)

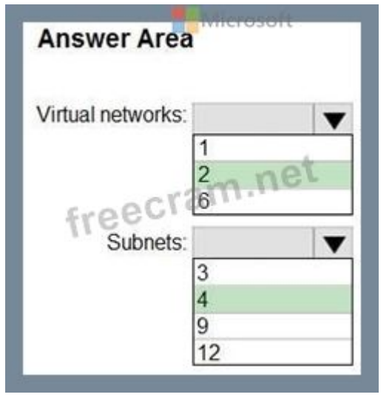
Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 122
Hotspot Question
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.

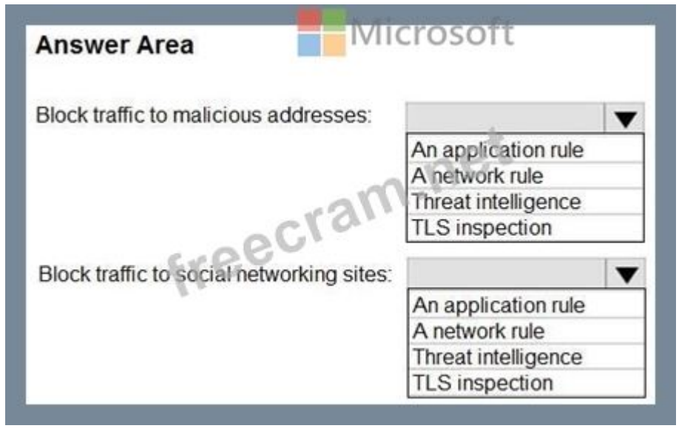


Answer:

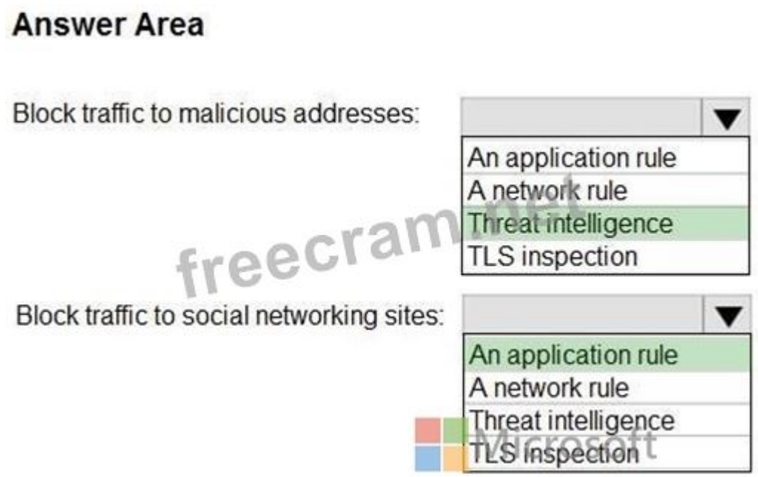


Explanation:
Normally, you just need to create a /24 Virtual Network with minimum of 2 different zones /25 subnets.
/25 Subnet = (128 - 5) IPs : 123 available IPs
=> 50 VMs in zone A, 50 VMs in zone B
/25 Subnet = (128 - 5) IPs: 123 available IPs
=> 50 VMs in zone C
But,
the questions mentioned that 2 subscriptions. (Highlighted the "each subscription").
So, the minimum requirements should be:
1 of /24 Vnets for each subscriptions => 2 Vnets
2 of /25 subnets for each subscriptions => 4 subnets

NEW QUESTION: 123
Hotspot Question
You have a firewall that is managed by using an Azure Firewall Premium policy named Policy1.
You need to configure Policy1 to block outbound traffic to the following locations:
- Malicious addresses identified by Microsoft.
- Social networking sites
The solution must minimize administrative effort.
What should you configure in Policy1 for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 124

Drag and Drop Question

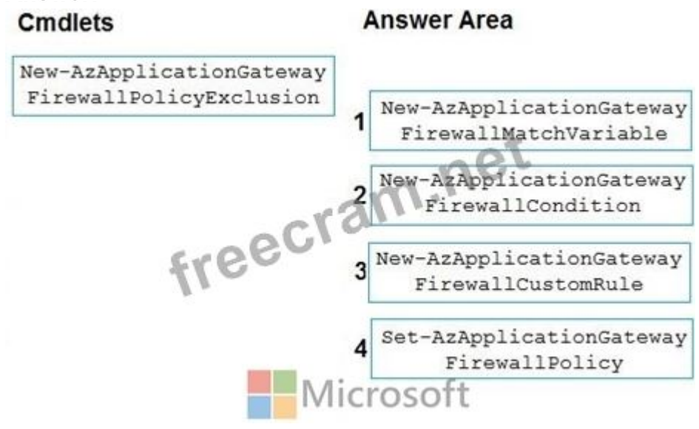
You have an Azure Web Application Firewall (WAF) v2 tier named AG1 on an Azure application gateway. AG1 has a policy named Policy1.

You need to add a custom rule to Policy1. 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.



Answer:



NEW QUESTION: 125

Hotspot Question

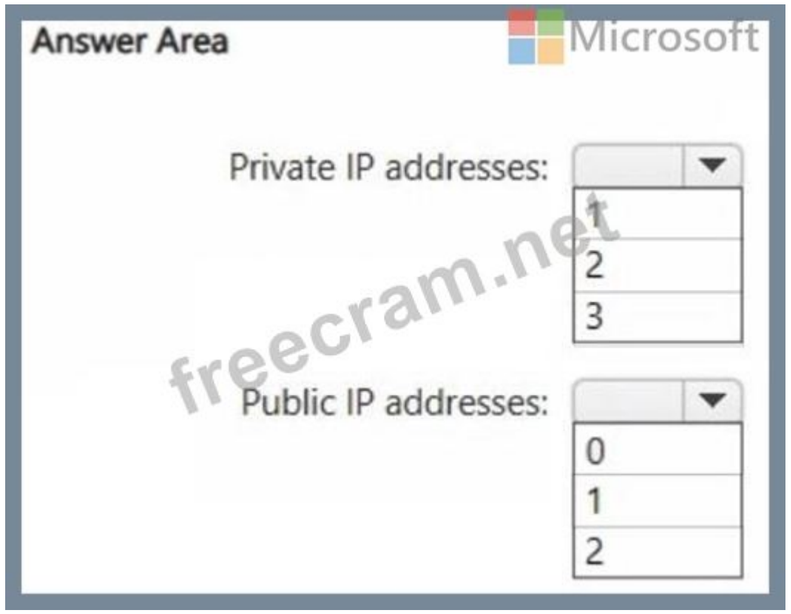
You have an Azure subscription that contains a virtual network named VNet1.

You need to deploy an instance of Azure Application Gateway v2 named AppGw1 to VNet1.

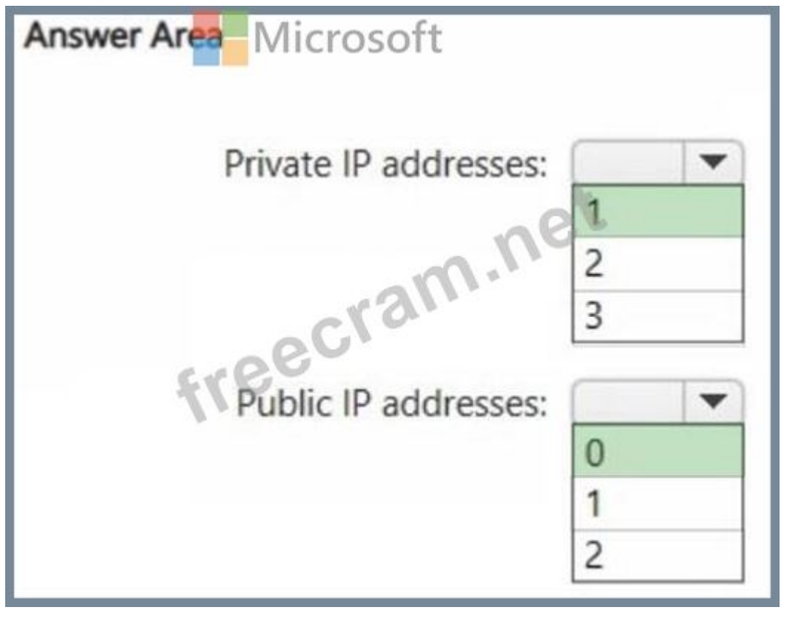
AppGw1 will include one basic listener and two multi-site listeners. The listeners will be accessible only from VNet1.

What is the minimum number of IP addresses required for AppGw1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 126

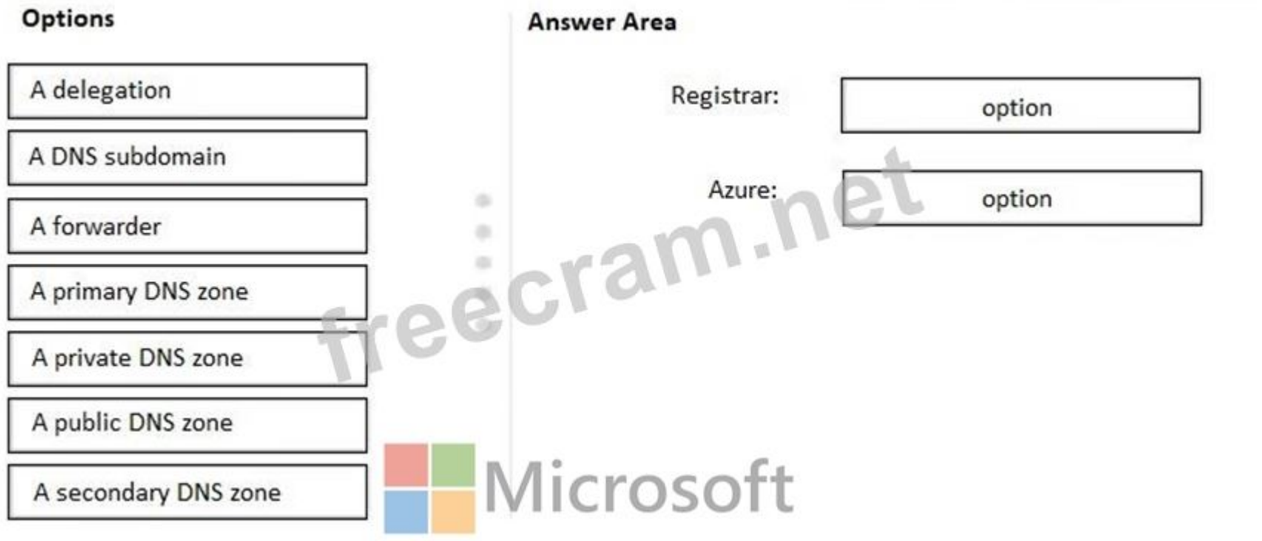
Drag and Drop Question

You have a DNS domain named contoso.com that is hosted by a third-party domain name registrar.

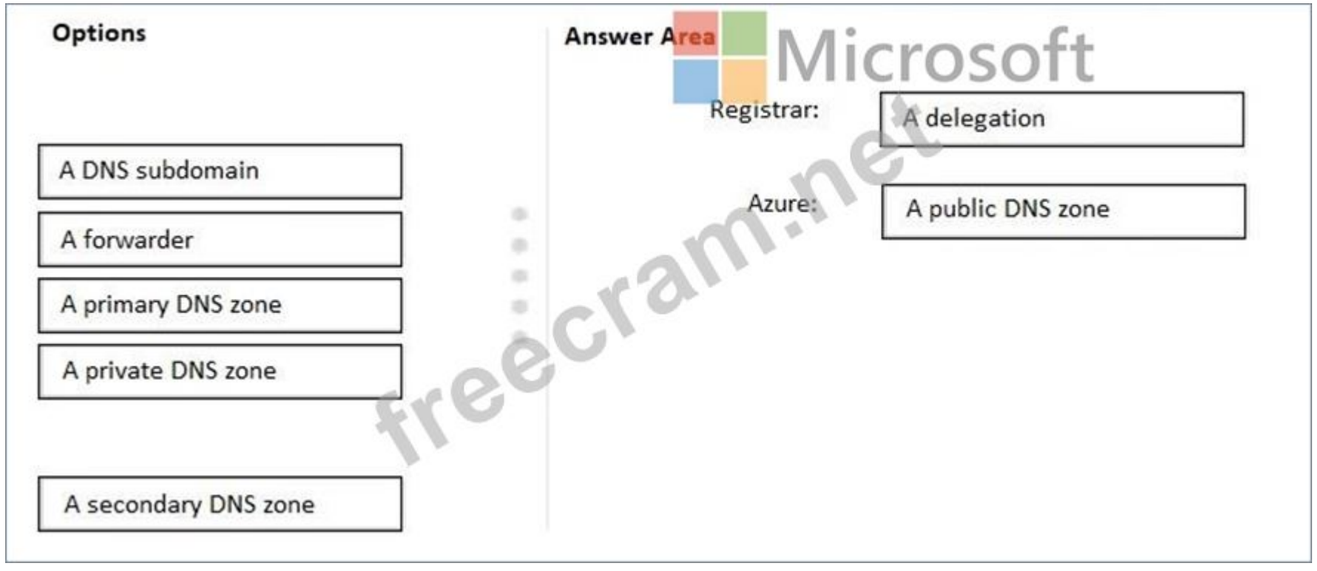
You have an Azure subscription.

You need to ensure that all DNS queries for the contoso.com domain are resolved by using Azure DNS.

What should you create in the registrar, and what should you create in Azure? 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.



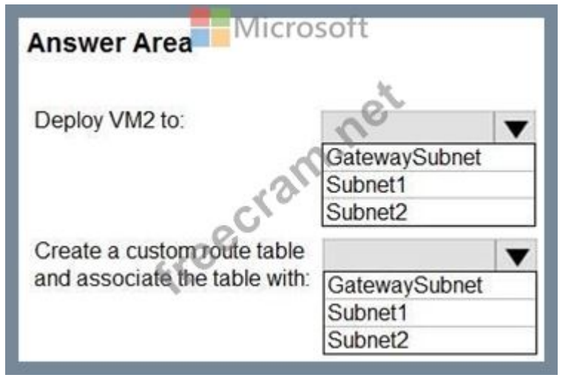
Answer:



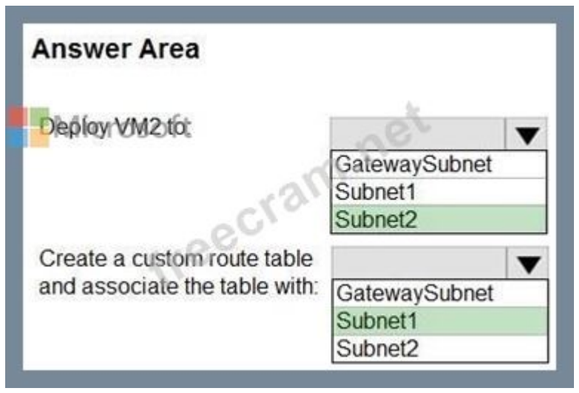
freecram.net
Microsoft

NEW QUESTION: 127
Hotspot Question
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 Subnet1.
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.



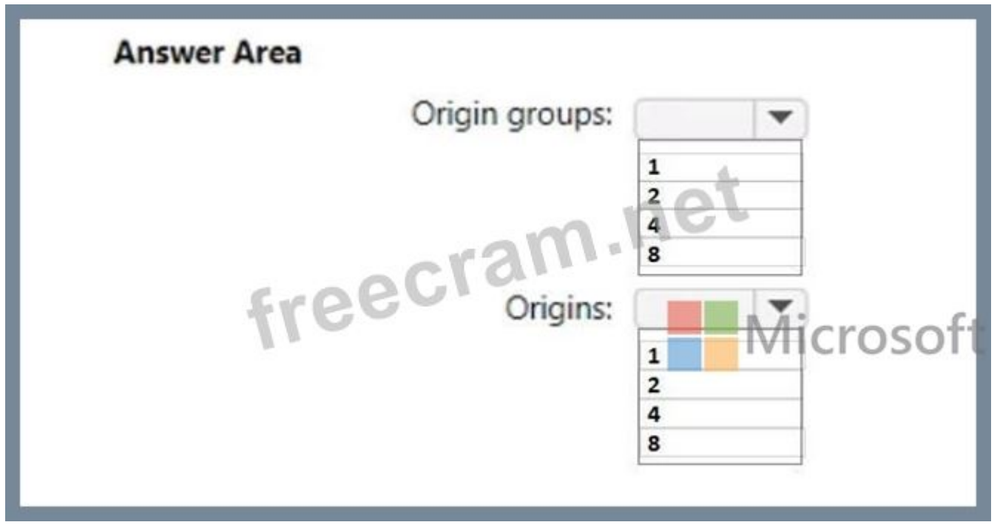
Answer:



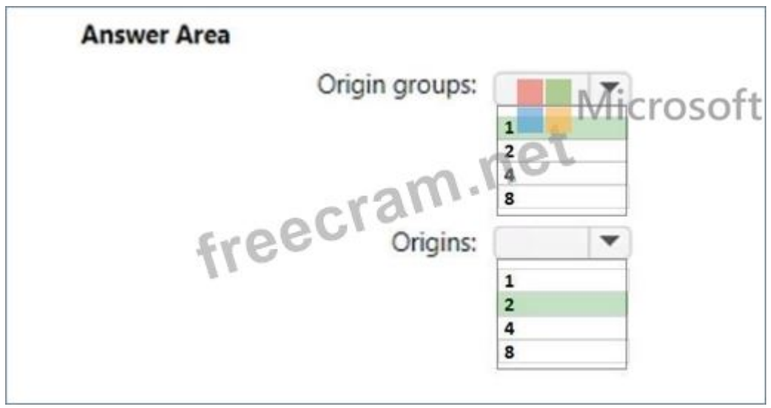
NEW QUESTION: 128
Hotspot Question
You have an Azure subscription that contains an app named App1. App1 is deployed to the Azure App Service apps shown in the following table.

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:



Explanation:

1 group: Multi-region active/active deployment: Create a single origin group. Within that origin group, create an origin for each of the App Service apps.

2 origins: Your App Service app might be configured to scale out across worker instances, but from Front Door's perspective there's a single origin.

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-faq

NEW QUESTION: 129

Case Study 1 - Litware. Inc

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-prernises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by usinq Azure AD Connect.

All the offices connect to a virtual network named Vnetl 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.

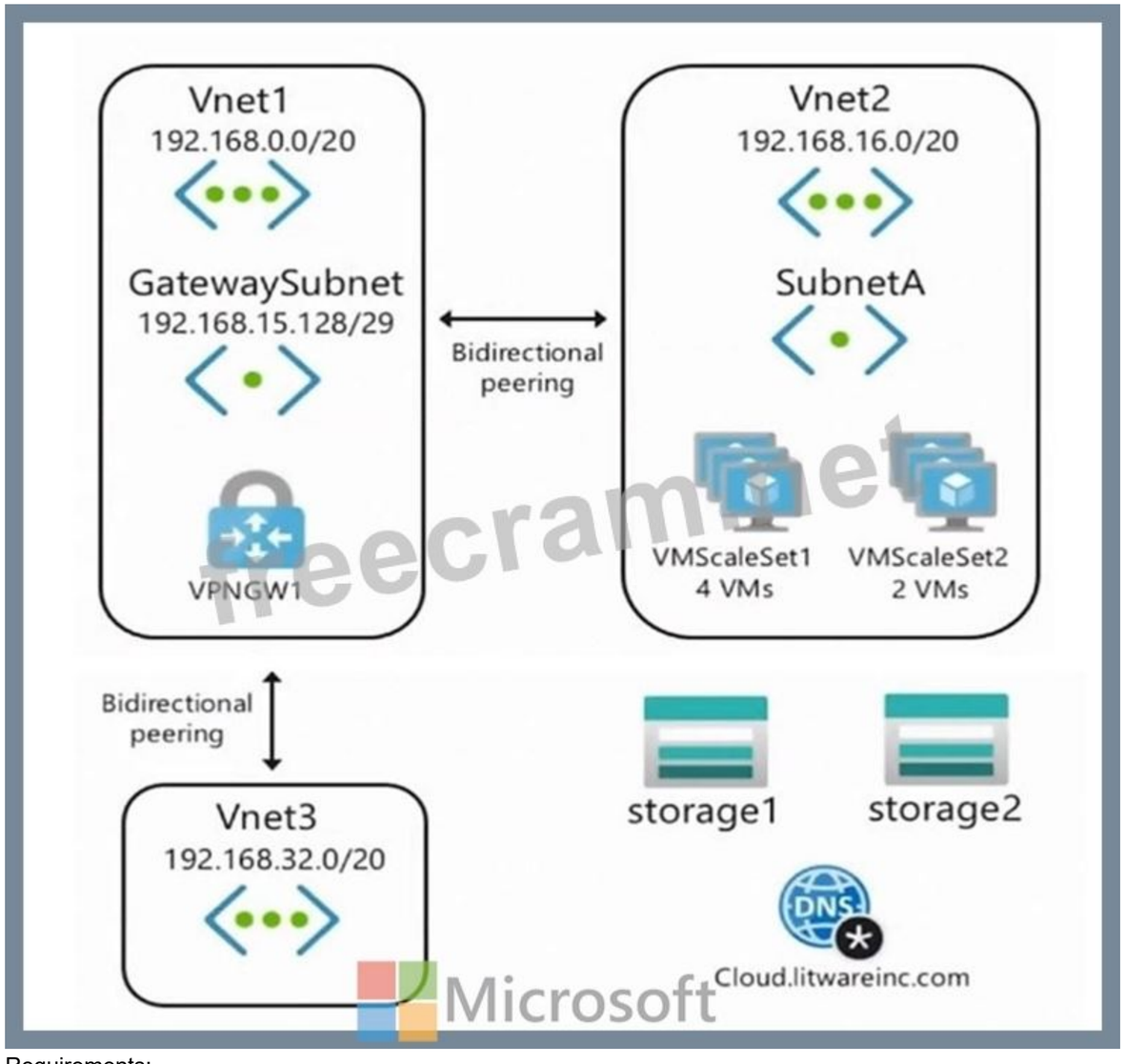
Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	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

freecram.net

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 zone 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):

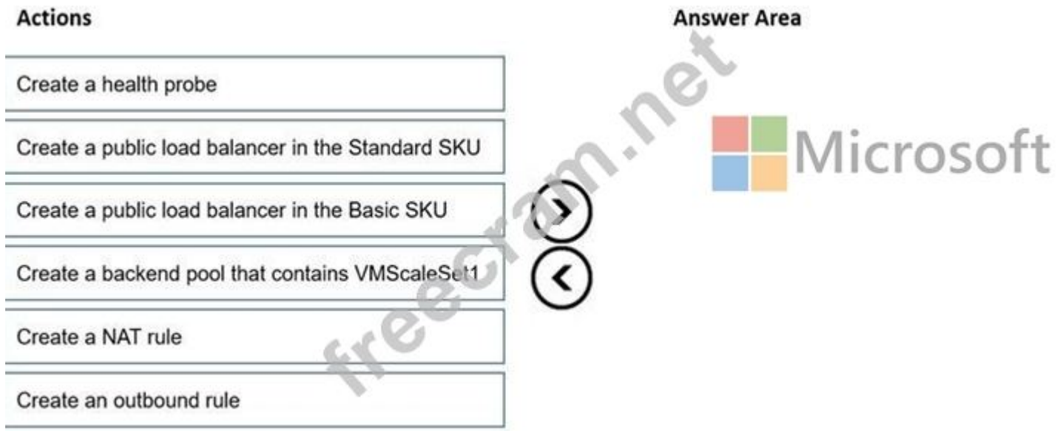
- The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.
- The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Drag and Drop Question

You need to implement outbound connectivity for VMScaleSet1.

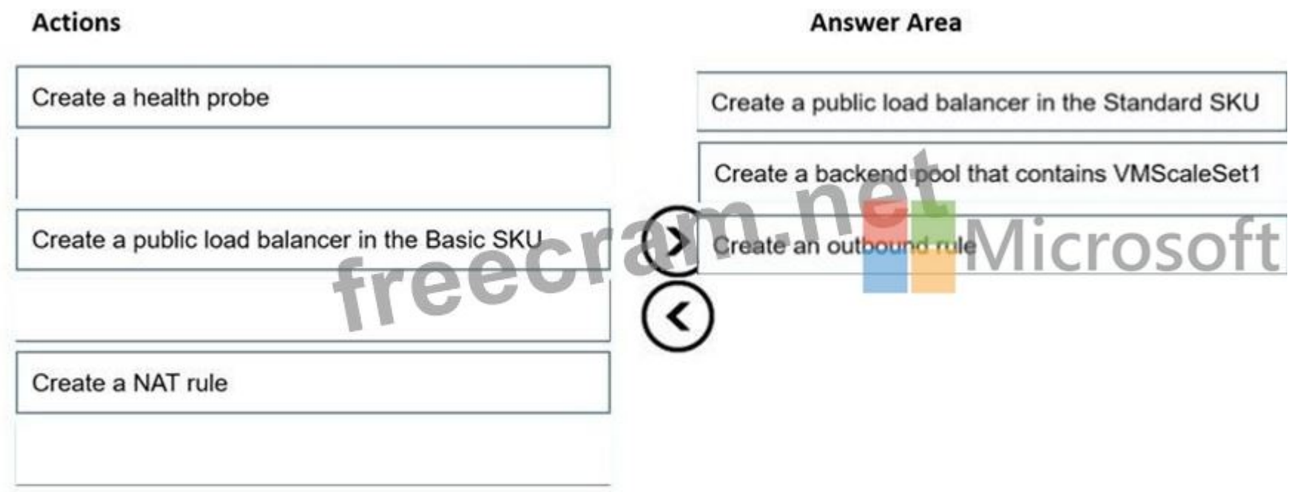
The solution must meet the virtual networking requirements and the business requirements.

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.



freecram.net
Microsoft

Answer:



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

NEW QUESTION: 130
You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains a virtual machine named VM1 and an Azure firewall named FW1.
You have an Azure Firewall Policy named FP1 that is associated to FW1.
You need to ensure that RDP requests to the public IP address of FW1 route to VM1.
What should you configure on FP1?
A. a network rule
B. URL filtering
C. a DNAT rule
D. an application rule
Answer: (SHOW ANSWER)
To allow RDP requests to reach VM1 through the public IP of FW1, you need to create a rule that translates the destination IP address of the incoming RDP requests to the private IP address of VM1. This is done through a type of rule called a DNAT rule, which is configured on the Azure Firewall Policy (FP1). Other types of rules, such as network rules, URL filtering, and application rules, are not relevant to this specific scenario.
https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat-policy

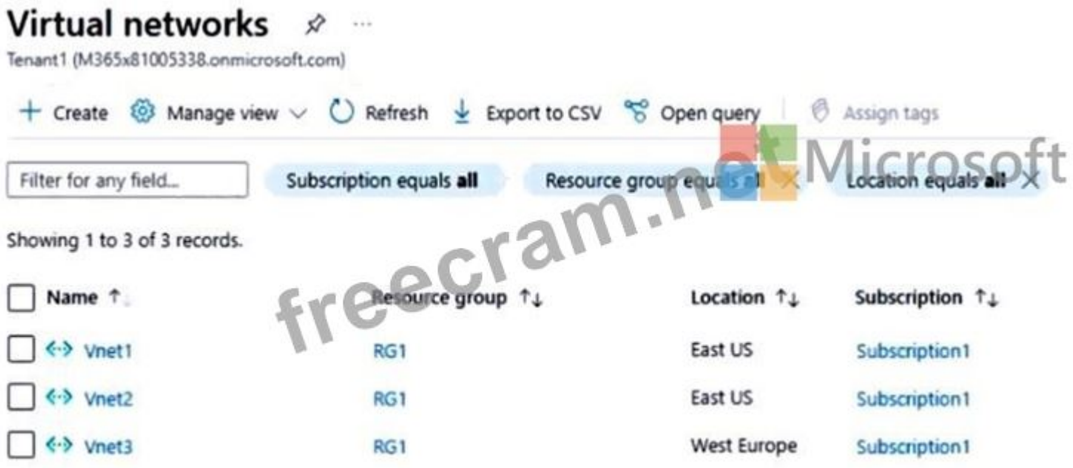
NEW QUESTION: 131
You have an Azure application gateway named AppGW1 that balances requests to a web app named App1.
You need to modify the server variables in the response header of App1.
What should you configure on AppGW1?
A. HTTP settings
B. listeners
C. path-based rules

D. URL rewrite rules
Answer: (SHOW ANSWER)

NEW QUESTION: 132
You have an on-premises datacenter and an Azure subscription.
You plan to implement ExpressRoute FastPath.
You need to create an ExpressRoute gateway. The solution must minimize downtime if a single Azure datacenter fails.
Which SKU should you use?
A. ErGw1AZ
B. High performance
C. Ultra performance
D. ErGw3AZ
E. ErGw2AZ
Answer: (SHOW ANSWER)
ErGw3Az and Ultra Performance SKU supports FastPath.
ErGw3Az is Zone-redundant, but not Ultra Performance SKU.
https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network- gateways#zrgw
https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath#gateways

NEW QUESTION: 133
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 configure a managed rule for WAF1.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Hotspot Question
You have an Azure subscription that contains the virtual networks shown in the Virtual networks exhibit.



freecram.net Microsoft

You create an Azure DNS Private Resolver as shown in the DNS private resolvers exhibit.

Create a DNS private resolver ...

Validation passed

Basics | Inbound Endpoints | Outbound Endpoints | Ruleset | Tags | **Review + Create**

View automation template

Basics

Subscription	Subscription1
Resource Group	RG1
Name	DNS-resolver-1
Region	West Europe
Virtual Network	Vnet3

Inbound endpoints

Endpoint name	DNS-resolver-inbound-endpoint-1

Outbound endpoints

Endpoint name	DNS-resolver-outbound-endpoint-1

Ruleset

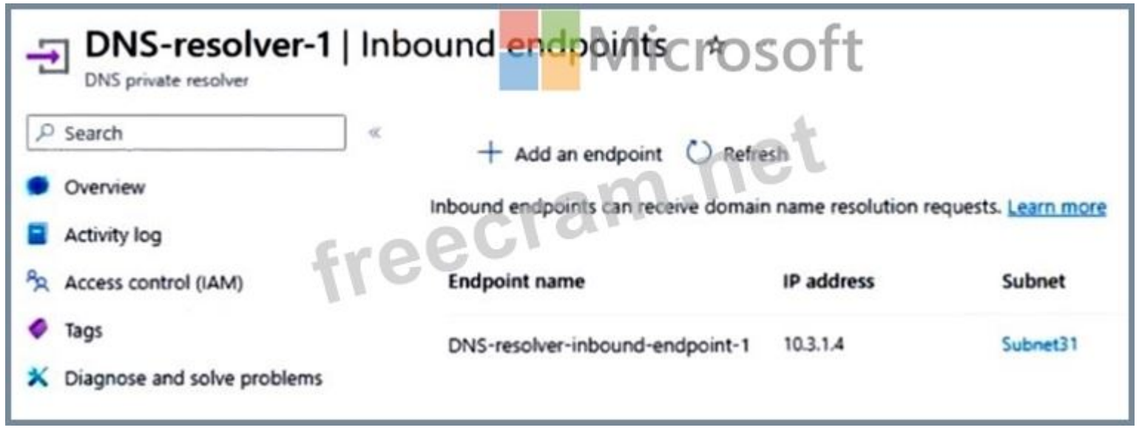
Ruleset name	DNS-resolver-ruleset-1
Outbound endpoints	DNS-resolver-outbound-endpoint-1
Virtual network link name	Vnet3-link
Rules	DNS-resolver-rule-1

Microsoft

Create | < Previous | Next >

freecram.net

DNS-resolver-inbound-endpoint-1 is configured as shown in the Inbound endpoints exhibit.



DNS-resolver-rule-1 is configured as shown in the Rules exhibit.



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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VNet1 can be linked to DNS-resolver-ruleset-1.	○	○
VNet2 must be configured to use 10.3.1.4 as the preferred DNS server.	○	○
Virtual machines connected to VNet3 can resolve names in the MargiesTravel.com domain.	○	○

Answer:

Answer Area

Statements	Yes	No
VNet1 can be linked to DNS-resolver-ruleset-1.	○	●
VNet2 must be configured to use 10.3.1.4 as the preferred DNS server.	●	○
Virtual machines connected to VNet3 can resolve names in the MargiesTravel.com domain.	●	○

NEW QUESTION: 135

You have an Azure virtual machine named VM1.

You need to capture all the network traffic of VM1 by using Azure Network Watcher.

To which locations can the capture be written?

A. a file path on VM1 only

B. General purpose v2 standard only

C. a Block blob premium account only

D. General purpose v2 standard and a file path on VM1 only

E. General purpose v2 standard and a Block blob premium account only

F. blob storage, a file path on VM1, and a Block blob premium account

Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/network-watcher/packet-capture-vm-portal You can choose to save captured data in the local disk or in Azure storage blob.
https://learn.microsoft.com/en-us/azure/network-watcher/packet-capture-overview

NEW QUESTION: 136
You have an Azure subscription that contains an Azure App Service app. The app uses a URL of
https:// www.contoso.com.
You need to use a custom domain on Azure Front Door for www.contoso.com. The custom domain must use a certificate from an allowed certification authority (CA).
What should you include in the solution?
A. an enterprise application in Azure Active Directory (Azure AD)
B. Active Directory Certificate Services (AD CS)
C. Azure Key Vault
D. Azure Application Gateway
Answer: (SHOW ANSWER)
You must create a complete certificate chain with an allowed certificate authority (CA) that is part of the Microsoft Trusted CA List. And Azure Key Vault allows you to store your certificates securely. Azure Front Door uses this secure mechanism to get your certificate (Self Signed or CA Provided) and it requires a few extra steps.
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https#option-2-use-your-own-certificate

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

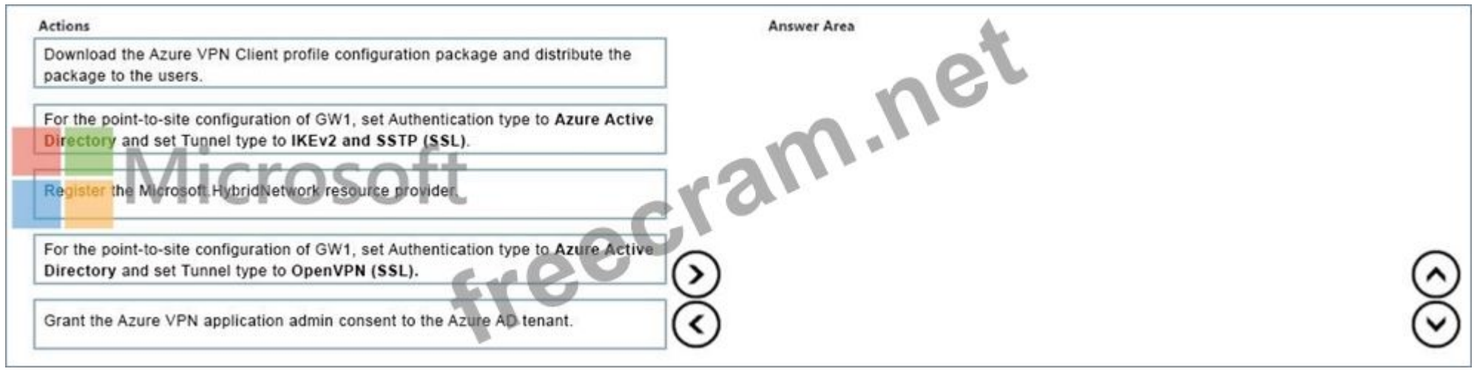
NEW QUESTION: 137
With the help of PowerShell, you need to retrieve/get an existing workspace named internWorkspace in a resource group named internWorkspaces. Which of the following cmdlets would you use?
A. Get-AzNetworkSecurityGroup
B. Get-AzOperationalInsightsWorkspace
C. Retrieve-AzOperationalInsightsWorkspace
D. Get-AzWorkspace
E. New-AzOperationalInsightsWorkspace.
Answer: (SHOW ANSWER)
Explanation: An existing Log Analytics workspace can be retrieved with the Get- AzOperationalInsightsWorkspace cmdlet. For example, to retrieve/get an existing workspace named internWorkspace in a resource group named internWorkspaces, use the below-given command:
$Oms=Get-AzOperationalInsightsWorkspace `
-ResourceGroupName internWorkspaces `
-Name internWorkspace
Option A is incorrect. Get-AzNetworkSecurityGroup cmdlet is used to retrieve the network security group(NSG) for which you want to enable resource logging.
Option B is correct. An existing Log Analytics workspace can be retrieved with the Get- AzOperationalInsightsWorkspace cmdlet.
Option C is incorrect. Retrieve-AzOperationalInsightsWorkspace is not the right cmdlet.
Option D is incorrect. Get-AzWorkspace is not the right command to retrieve the existing log analytics workspace.

Option E is incorrect. The new-AzOperationalInsightsWorkspace cmdlet is used to create a new workspace.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log?WT.mc_id=modinfra-33046-thmaure

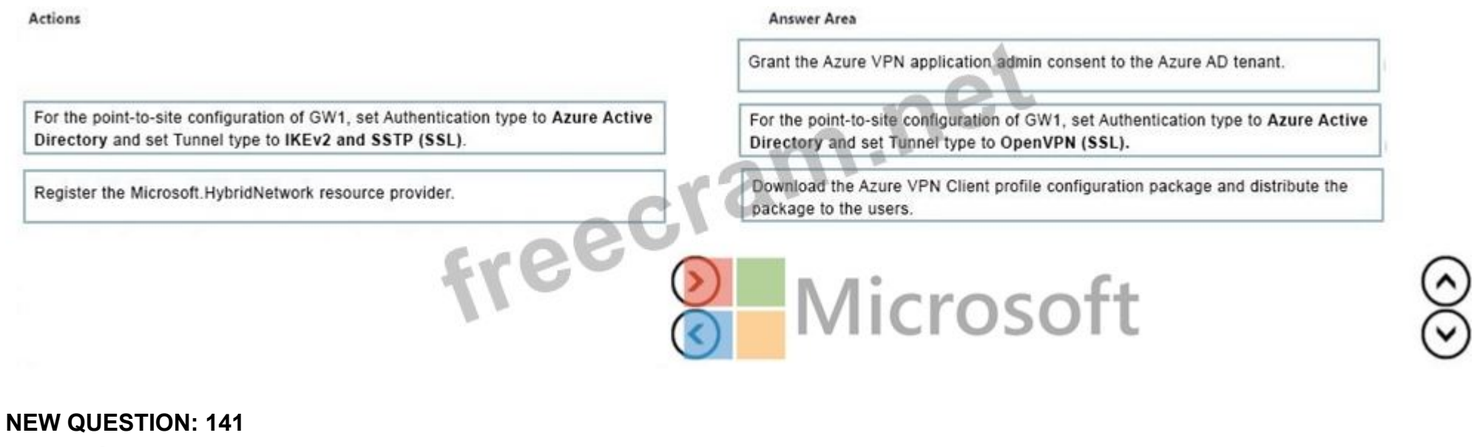
NEW QUESTION: 138
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a subnet named Subnet1.
You plan to add a private endpoint to Subnet.
You need to ensure that you can route traffic between the private endpoint and the Azure Private Link service by using a user-defined route.
What should you do first on Subnet1?
A. Enable delegation.
B. Enable network policy.
C. Create a service endpoint.
D. Provision a Standard Azure load balancer.
Answer: (SHOW ANSWER)

NEW QUESTION: 139
You have an Azure App Service that hosts your frontend application and is publicly accessible.
You also have some backend services in the same region deployed inside a Virtual Network (VNet). The backend services are private and not exposed outside the VNet.
You need to integrate your Azure Service with the VNet to establish a connection between the frontend and backend services.
Which two actions should you perform? Each correct answer presents part of the solution.
A. Create an Azure Virtual Network gateway.
B. Use the Premium App service plan.
C. Create an Integration subnet.
D. Use the Isolated App service plan.
E. Create a Network Security Group (NSG).
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 140
Drag and Drop Question
You have an Azure subscription that contains an Azure VPN gateway named GW1. GW1 provides Point-to-Site (P2S) VPN connectivity.
Users connect to GW1 from a Windows 11 device by using an SSTP connection.
You need to ensure that the P2S VPN connections support Azure AD authentication.
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.



Answer:



freecram.net

NEW QUESTION: 141

Hotspot Question

You have an on-premises server named Server1 that runs Windows Server and has the DNS Server role installed.

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2.

VNet1 contains an Azure Firewall instance named FW1. VNet1 peers with VNet2.

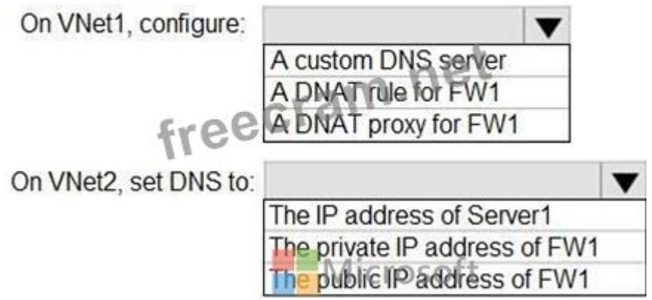
The on-premises network is connected to VNet1 by using ExpressRoute. The on-premises network is inaccessible from VNet2.

You need to ensure that virtual machines connected to VNet2 use Server1 to perform name resolution. The solution must minimize administrative effort.

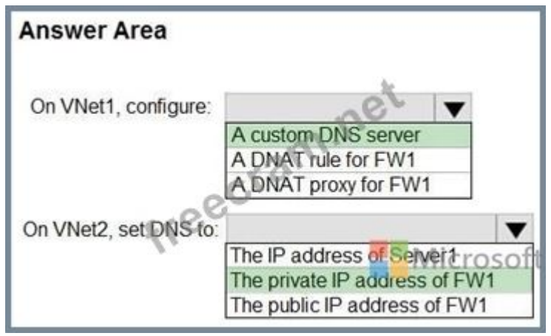
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area



Answer:



NEW QUESTION: 142

Hotspot Question

FirewallPolicy1 contains the following rules:

- Allow outbound traffic from Vnet1 and Vnet2 to the internet.
- Allow any traffic between Vnet1 and Vnet2.

No custom private endpoints, service endpoints, routing tables, or network security groups (NSGs) were created. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

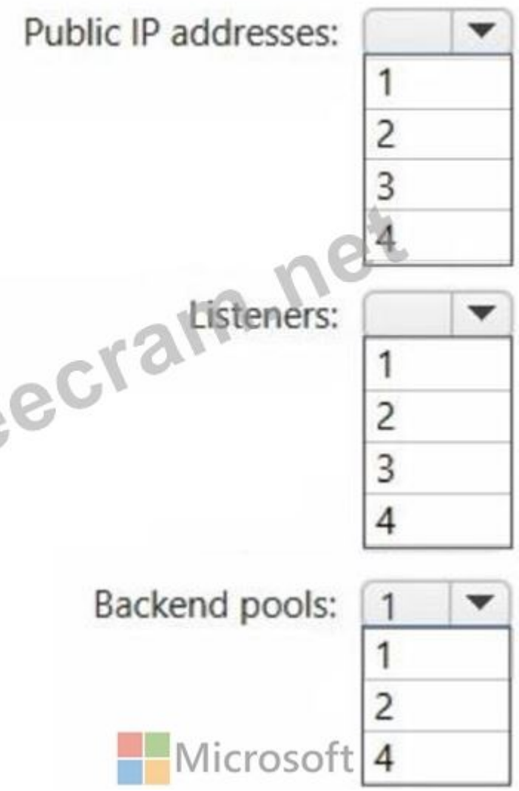
Statements	Yes	No
A routing table must be associated with Subnet1 and Subnet2 to ensure that all internet traffic for VM1 and VM2 is sent via Firewall1.	○	○
The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	○	○

Answer:

Statements	Yes	No
A routing table must be associated with Subnet1 and Subnet2 to ensure that all internet traffic for VM1 and VM2 is sent via Firewall1.	○	○
The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	○	○

NEW QUESTION: 143
Hotspot Question
You have an Azure subscription that contains an Azure application gateway named AG1 and two Azure App Service apps named App1 and App2 that have the following configurations:
- Both apps are accessible by using HTTP and HTTPS.
- HTTP host headers are used to route requests to the appropriate apps.
- Both apps are hosted in a single App Service Environment in the West
Europe Azure region.
You need to publish the apps by using AG1. The solution must ensure that AG1 provides both HTTP and HTTPS access.
What is the minimum number of resources required for AG1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



freecram.net

Microsoft

Answer:

Answer Area

Public IP addresses: 1 | 2 | 3 | 4

Listeners: 1 | 2 | 3 | 4

Backend pools: 1 | 1 | 2 | 4

Microsoft
freecram.net

NEW QUESTION: 144

Azure Private Endpoint acts as a network interface to connect you to a service powered by Azure Private Link in a private and secure manner. Being the Private Link resource owner, which of the following actions can you perform over a private endpoint connection?

A. Reviewing all private endpoint connection details.

B. Approving a private endpoint connection.

C. Rejecting a private endpoint connection.

D. Deleting a private endpoint connection from any state.

E. All the above

Answer: (SHOW ANSWER)

The private link resource owner can perform the below-given actions over a private endpoint connection:

- Review all private endpoint connections details.
- Approve a private endpoint connection. The corresponding private endpoint will be enabled to send traffic to the private link resource.
- Reject a private endpoint connection. The corresponding private endpoint will be updated to reflect the status.
- Delete a private endpoint connection in any state. The corresponding private endpoint will be updated with a disconnected state to reflect the action, the private endpoint owner can only delete the resource at this point.

Option A is incorrect. Besides reviewing all private endpoint connection details, the private link resource owner can approve, reject, and even delete a private endpoint connection.

Option B is incorrect. Besides approving a private endpoint connection, the private link resource owner can review, reject, and even delete a private endpoint connection.

Option C is incorrect. A private link resource owner can review, approve, reject and even delete a private endpoint connection.
Option D is incorrect. Besides deleting a private endpoint connection, the private link resource owner can review, approve, or even reject a private endpoint connection.
Option E is correct. A private link resource owner can perform all the given actions.
References:
https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview?WT.mc_id=modinfra-33046-thmaure

NEW QUESTION: 145
SIMULATION



Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
- If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You need to ensure that connections to the storage12345678 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name storage12345678.privatelink.blob.core.windows.net.
To complete this task, sign in to the Azure portal.
Answer:

Use private endpoints for Azure Storage
You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service.

Plan:
Stage 1: Create a virtual network and subnet
Stage 2: Create a private endpoint

Stage 1: Create a virtual network and subnet

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter Virtual network. In the search results, select Virtual networks.

Step 3: Select + Create in Virtual networks.

Step 4: In the Basics tab of Create virtual network, enter or select the following information.
Subscription -Select your subscription.
Resource group - Select Create new.
Enter SomeName in Name and select OK.
Instance details
Name - Enter myVNet for example
Region - Select West Europe.

Step 5: Select Next: IP Addresses or the IP Addresses tab.
Step 6: Select the IP Addresses tab or select Next: IP Addresses at the bottom of the page.
Step 7: In the IP Addresses tab, enter the following information:
* IPv4 address space - Enter 10.1.0.0/16

Step 8: Select Add subnet. In Edit subnet, enter the following information:
Subnet name - Enter mySubnet
Subnet address range - Enter 10.1.1.0/24 (as specified in the question)

Step 9: For the subnet: Select the Review + create tab or select the Review + create button.

Step 10: For the Virtual network: Select the Review + create tab or select the Review + create button.

Stage 2: Create a private endpoint
Step 1: In the search box at the top of the portal, enter Private endpoint. Select Private endpoints.

Step 2: Select + Create in Private endpoints.

Step 3: In the Basics tab of Create a private endpoint, enter or select the following information.

* Storage subresource - storage12345678.privatelink.blob.core.windows.net

* Private DNS integration.
Integrate with private DNS zone - Leave the default Yes.

* Private DNS Zone
Leave the default (New) privatelink.blob.core.windows.net.

Step 4: Select Next: Resource.

Step 5: In the Resource pane, leave the defaults.

Step 6: Select Next: Virtual Network.

Step 7: In Virtual Network, enter or select the following information.
Virtual network - Select the virtual network you created in stage 1.
Subnet - Select the subnet you created in stage 1.

Step 8: Select Next: DNS.
Step 9: Leave the defaults in DNS. Select Next: Tags, then Next: Review + create.
Step 10: Select Create.

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

NEW QUESTION: 146
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": "2021-06-02T18:15:45+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": "f7546159ylhjk7wall4568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```

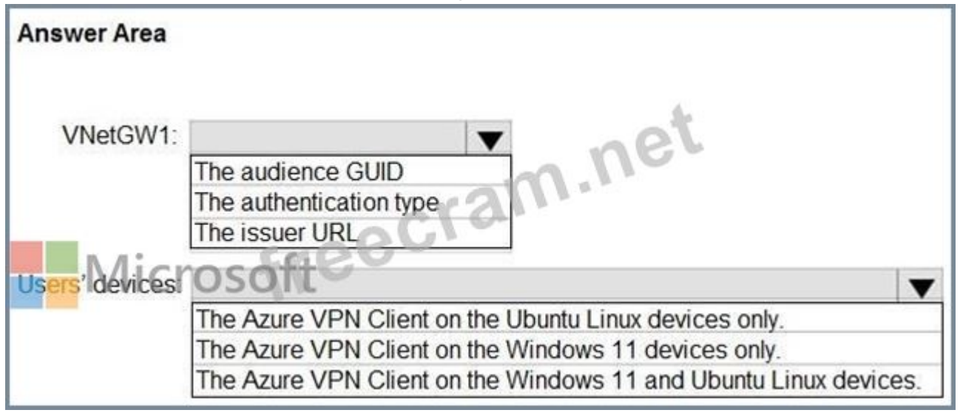

Microsoft freecram.net

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

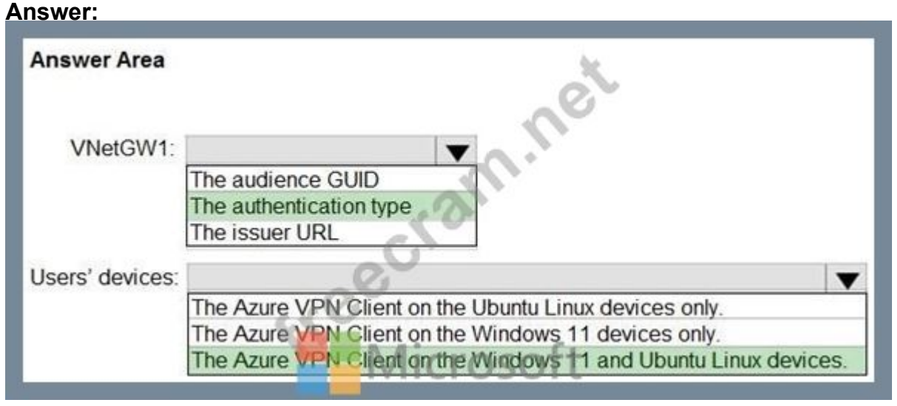
Solution: You add a rewrite rule for the host header.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
The log shows that WAF rule with ruleId 920300 was trigged. Instead we should disable the WAF rule that has a ruleId 920300.
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot

NEW QUESTION: 147
You have an Azure subscription that contains an Azure Front Door named FD1.
You plan to deploy an app named App1 by using Azure App Service. Users will access App1 by using FD1.
You need to provide FD1 with access to App1. The solution must meet the following requirements:
- Ensure that users can only access App1 by using FD1.
- Ensure that users cannot access App1 directly from the internet.
What should you create for App1?
A. an access restriction
B. a private endpoint
C. a subnet delegation
D. a service endpoint
Answer: A (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli

NEW QUESTION: 148
Hotspot Question
You have multiple remote users that have either a Windows 11 device or an Ubuntu Linux 22.04 device. Each device has a manually registered Azure VPN Client installed.
You have an Azure subscription that contains an Azure VPN gateway named VNetGW1.
The Windows 11 users establish Point-to-Site (P2S) VPN connections to VNetGW1 and authenticate by using their Microsoft Entra credentials. The Ubuntu Linux users cannot establish P2S VPN connections.
You need to ensure that the Ubuntu Linux users can establish P2S VPN connections to VNetGW1. The solution must minimize administrative effort and maximize security. To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 149

Drag and Drop Question

You have two Azure virtual networks named Hub1 and Spoke1. Hub1 connects to an on- premises network by using a Site-to-Site VPN connection.

You are implementing peering between Hub1 and Spoke1.

You need to ensure that a virtual machine connected to Spoke1 can connect to the on-premises network through Hub1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value 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.

Values

- -AllowForwardedTraffic
- -AllowGatewayTransit
- -UseRemoteGateways

Answer Area

```
$hub = Get-AZVirtualNetwork -ResourceGroup "RG1" -Name "Hub1"
$spoke = Get-AZVirtualNetwork -ResourceGroup "RG2" -Name "Spoke1"
Add-AZVirtualNetworkPeering -Name "Hub1-Spoke1" -VirtualNetwork $hub
      -RemoteVirtualNetworkId $spoke.id  [ Value ]
Add-AZVirtualNetworkPeering -Name "Spoke1-Hub1" -VirtualNetwork $spoke
      -RemoteVirtualNetworkId $hub.id    [ Value ]
```

Answer:



Microsoft
freecram.net

Explanation:

Box 1: -AllowGatewayTransit

Select Use this virtual network's gateway or Route Server:

- If you have a virtual network gateway attached to this virtual network and want to allow traffic from the peered virtual network to flow through the gateway.

Box 2: -UseremoteGateways

Select Use the remote virtual network gateway or Route Server:

- If you want to allow traffic from this virtual network to flow through a virtual network gateway attached to the virtual network you're peering with.

Box1: Hub told spoke to use hub's VPN gateway to reach on-premise network Box2: Spoke told hub to use hub's VPN gateway to reach on-premise network

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering

NEW QUESTION: 150

SIMULATION



Username and password

Use the following login credentials as needed:

- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

- Lab Instance: 12345678

You need to ensure that the owner of VNET3 receives an alert if an administrative operation is performed in the virtual network.

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

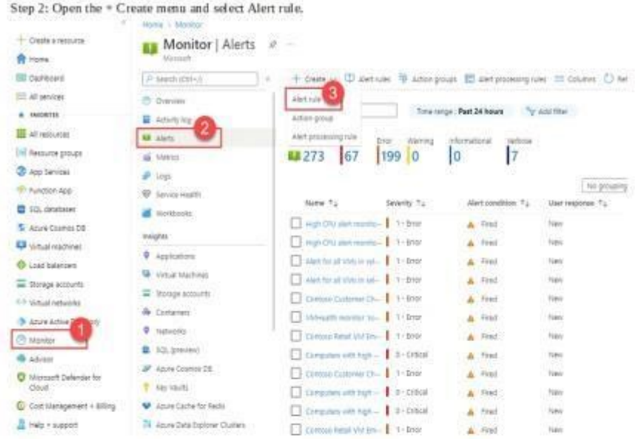
Answer:

Monitoring Azure virtual network
Alerts
Azure Monitor alerts proactively notify you when important conditions are found in your monitoring data. They allow you to identify and address issues in your system before your customers notice them. You can set alerts on metrics, logs, and the activity log.

Create a new alert rule in the Azure portal

Step 1: In the portal, select Monitor > Alerts.

Step 2: Open the + Create menu and select Alert rule.



Step 3: On the Select a resource pane, set the scope for your alert rule. You can filter by subscription, resource type, or resource location. We select Virtual Network.

The Available signal types for your selected resources are at the bottom right of the pane.

Step 4: Select Include all future resources to include any future resources added to the selected scope.

Step 5: Select Done.

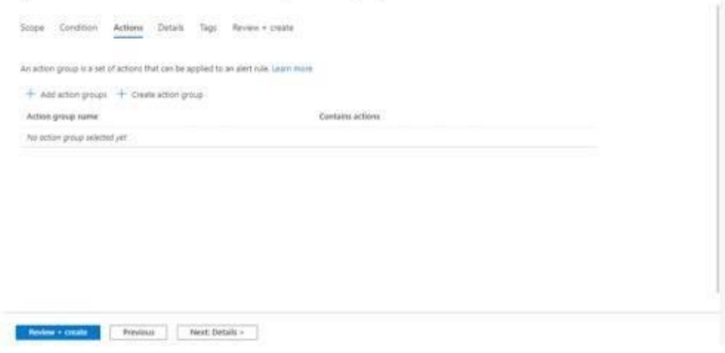
Step 6: Select Next: Condition at the bottom of the page.

Step 7: On the Select a signal pane, filter the list of signals by using the signal type and monitor service:

* Signal type: The type of alert rule you're creating.
We select Activity log

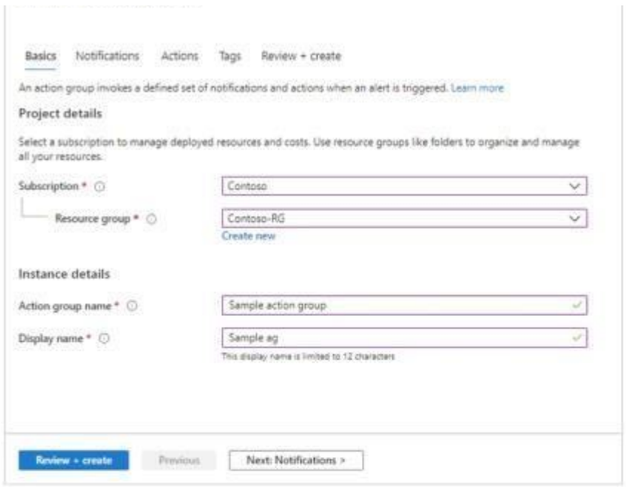
* Monitor service: The service sending the signal. This list is pre-populated based on the type of alert rule you selected.
We select Activity log – Administrative (The service that provides the Administrative activity log events)

Step 8: On the Actions tab, select to create the required action group.



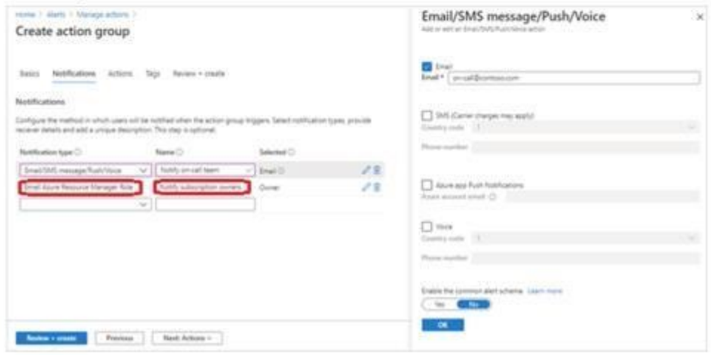
Step 9: Configure basic action group settings





Step 10: Configure notifications. To open the Notifications tab, select Next: Notifications.
Alternately, at the top of the page, select the Notifications tab.

Step 11: Define a list of notifications to send when an alert is triggered.
Notification: Email Azure Resource Manager Role
Name: Notify Owner



Step 12: Select OK.

Step 13: Finish the remaining steps in the wizard.

Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/monitor-virtual-network
https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule?tabs=metric#create-a-new-alert-rule-in-the-azure-portal

NEW QUESTION: 151

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

Name	Type	Location
VNet1	Virtual network	East US
storage1	Storage account	East US
storage2	Storage account	East US
storage3	Storage account	East US

VNet1 contains a subnet named Subnet.

You need to ensure that the resources connected to Subnet1 can access only storage1 and storage3. The solution must minimize administrative effort.

What should you configure?

A. an application security group
B. Azure Private Link
C. a service endpoint policy
D. a service tag
Answer: (SHOW ANSWER)
Service endpoint policies are allow policies, so apart from the specified resources, all other resources are restricted.
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies- overview

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
SIMULATION

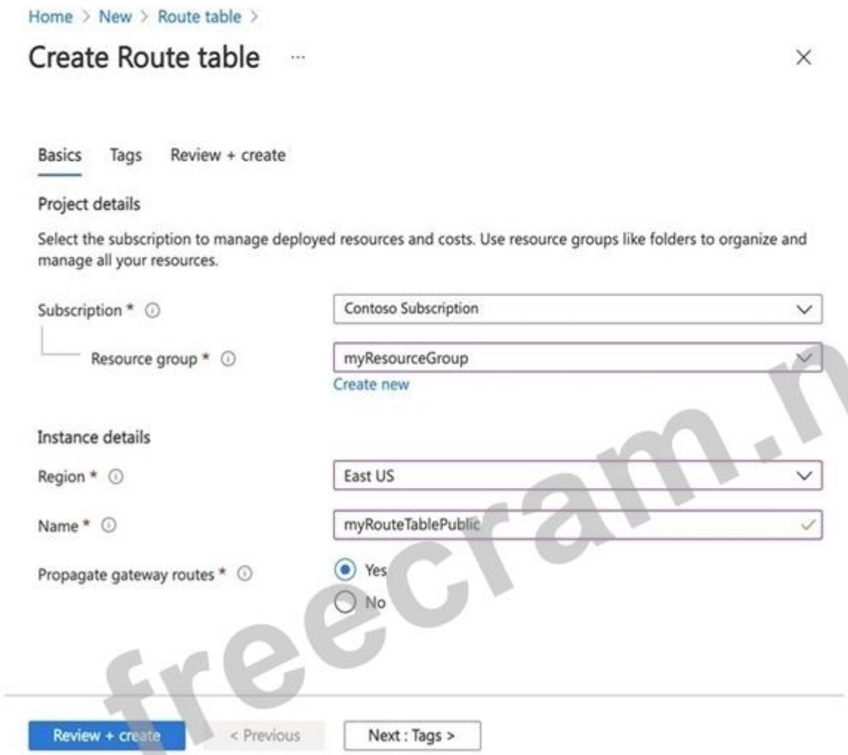

Username and password
Use the following login credentials as needed:
- To enter your password, place your cursor in the Enter password box and click on the password below.
- To enter your username, place your cursor in the Sign in box and click on the username below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
- If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You plan to deploy a firewall to subnet1-2. The firewall will have an IP address of 10.1.2.4.
You need to ensure that traffic from subnet1-1 to the IP address range of 192.168.10.0/24 is routed through the firewall that will be deployed to subnet 1-2. The solution must be achieved without using dynamic routing protocol.
To complete this task, sign in to the Azure portal.
Answer:
Custom routes, User-defined
You can create custom, or user-defined(static), routes in Azure to override Azure's default system routes, or to

add more routes to a subnet's route table. In Azure, you create a route table, then associate the route table to zero or more virtual network subnets. Each subnet can have zero or one route table associated to it.

Create a route table (Skip Step 1 to Step 4 if route table already present=
Step 1: From the Azure portal menu, select + Create a resource > Networking > Route table, or search for Route table in the portal search box.

Step 2: Select Create.

Step 3: On the Basics tab of Create route table, enter or select information:



Step 4: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Create a route
In this section, you'll create a route in the route table that you created in the previous steps.

Step 5: Select Go to resource or Search for myRouteTablePublic (The route table you created earlier) in the portal search box.

Step 6: In the myRouteTablePublic page, select Routes from the Settings section.

Step 7: In the Routes page, select the + Add button.

Step 8: In Add route, enter or select this information:
Route name: SomeName
Address prefix destination: Select IP Addresses.

freecram.net

Destination IP addresses/CIDR ranges: Enter 192.168.10.0/24 - The address range of to be routed from.
Next hop type: Select Virtual appliance.
Next hop address: Enter 10.1.2.4 (The address of the firewall in the sbunet1-2 subnet).

Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal

NEW QUESTION: 153
Your company has offices in New York and Amsterdam. The company has an Azure subscription.
Both offices connect to Azure by using a Site-to-Site VPN connection.
The office in Amsterdam uses resources in the North Europe Azure region. The office in New York uses resources in the East US Azure region.
You need to implement ExpressRoute circuits to connect each office to the nearest Azure region.
Once the ExpressRoute circuits are connected, the on-premises computers in the Amsterdam office must be able to connect to the on-premises servers in the New York office by using the ExpressRoute circuits.
Which ExpressRoute option should you use?
A. ExpressRoute Local
B. ExpressRoute FastPath
C. ExpressRoute Direct
D. ExpressRoute Global Reach
Answer: (SHOW ANSWER)
With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks. In the above example, with the addition of ExpressRoute Global Reach, your San Francisco office (10.0.1.0/24) can directly exchange data with your London office (10.0.2.0/24) through the existing ExpressRoute circuits and via Microsoft's global network.
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach

NEW QUESTION: 154
Hotspot Question
You have an Azure subscription that contains the resources shown in the following table.

Name	Description
VNet1	Virtual network that has an IP address space of 10.0.0.0/16
Subnet1	Subnet that has an IP address space of 10.0.0.0/24
Subnet2	Subnet that has an IP address space of 10.1.0.0/24
storage1	Storage account
storage2	Storage account
Policy1	Service endpoint policy

Policy1 has the following settings:
- Service: Microsoft Storage
- Allowed Resources: storage1
Subnet1 has the following settings:
- Name: Subnet
- Subnet address range: 10.0.0.0/24
- NAT gateway: None

- Network security group: None
- Route table: None
- Service Endpoints
- Services: Microsoft Storage
- Service endpoint policies: Policy1
- Delegate subnet to a service: None
- Subnet delegation

Subnet2 has the following settings:

- Name: Subnet2
- Subnet address range: 10.0.1.0/24
- NAT gateway: None
- Network security group: None
- Route table: None
- Service Endpoints
- 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.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Devices on Subnet1 can access storage1.	○	○
Devices on Subnet2 can access storage1.	○	○
Devices on Subnet1 can access storage2.	○	○

Answer:

Answer Area

Statements	Yes	No
Devices on Subnet1 can access storage1.	○	○
Devices on Subnet2 can access storage1.	○	○
Devices on Subnet1 can access storage2.	○	○

NEW QUESTION: 155

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

Answer: (SHOW ANSWER)
Both storage accounts require a single service endpoint for "Microsoft.Storage." The Azure SQL Database requires a service endpoint for "Microsoft.Sql."

NEW QUESTION: 156
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. peering
B. VNet-to-VNet VPN connections
C. service endpoints
D. route tables

Answer: (SHOW ANSWER)

NEW QUESTION: 157
Hotspot Question
You have an Azure subscription that contains a virtual network. The virtual network contains two subnets named Subnet1 and Subnet2. You have an instance of Azure Application Gateway v2 named AppGw1 that is connected to Subnet1.
You need to move AppGw1 to Subnet2. The solution must minimize downtime.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 158
SIMULATION



Username and password

Use the following login credentials as needed:

- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
- If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

- Lab Instance: 12345678

You need to ensure that hosts on VNET2 can access hosts on both VNET1 and VNET3. The solution must prevent hosts on VNET1 and VNET3 from communicating through VNET2.

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

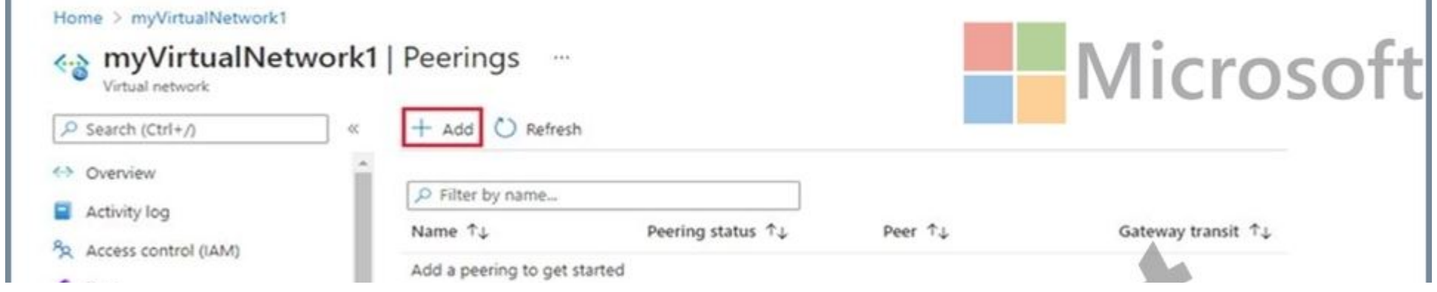
Answer:

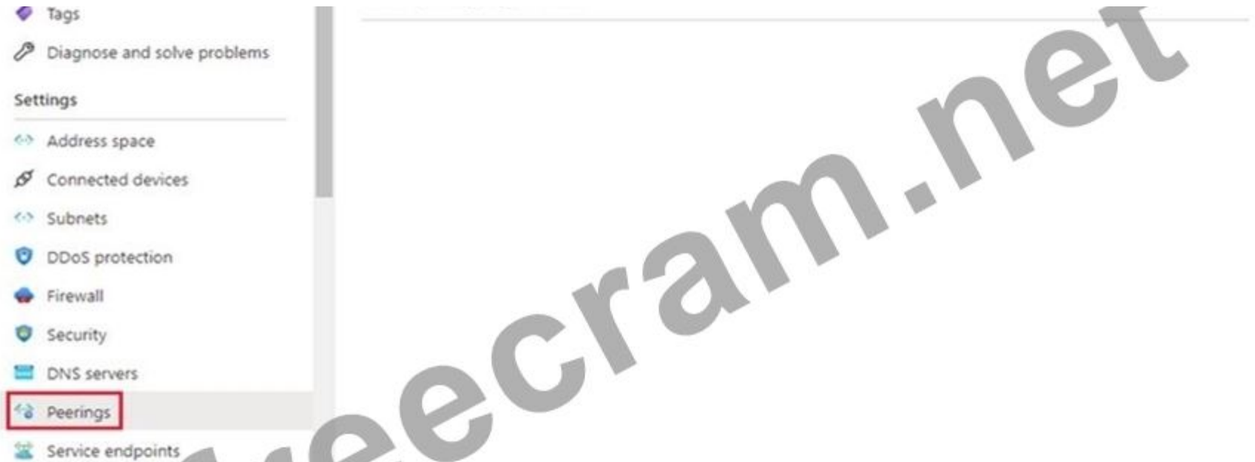
We use VNET2 as hub, and VNET1 and VNET3 as spokes.
The spoke virtual networks peer with the hub and can be used to isolate workloads.
A hub-spoke topology can be used without a gateway if you don't need cross-premises network connectivity.

Peer virtual networks

Step 1: In the search box at the top of the Azure portal, look for VNET2. When VNET2 appears in the search results, select it.

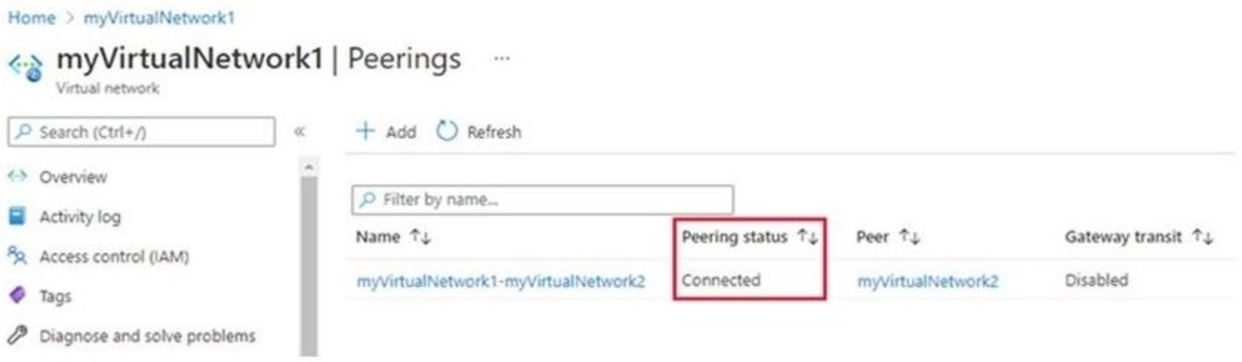
Step 2: Under Settings, select Peerings, and then select + Add, as shown in the following picture:





Step 3: Enter or select the following information, accept the defaults for the remaining settings, and then select Add.
* Virtual network - Select VNET1 for the name of the remote virtual network.

Step 4: In the Peerings page, the Peering status is Connected, as shown in the following picture:



Step 5: Repeat steps 1 to 4, but in Step 3 add VNET3 instead of VNET1.

Reference:
https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke

freecram.net

NEW QUESTION: 159
Hotspot Question
You configure a route table named RT1 that has the routes shown in the following table.

Name	Prefix	Next hop type	Next hop IP address
Route1	0.0.0.0/0	Network virtual appliance (NVA)	192.168.0.4
Route2	10.0.0.0/24	Network virtual appliance (NVA)	192.168.0.4

You have an Azure virtual network named Vnet1 that has the subnets shown in the following table.

Name	Prefix	Route table
DMZ	192.168.0.0/24	**None**
FrontEnd	192.168.1.0/24	RT1
BackEnd	192.168.2.0/24	**None**

You have the resources shown in the following table.

Name	IP address	Type
NVA1	192.168.0.4	NVA
VM1	192.168.1.4	Virtual machine
VM2	192.168.2.4	Virtual machine

Vnet1 connects to an ExpressRoute circuit. The on-premises router advertises the following routes:

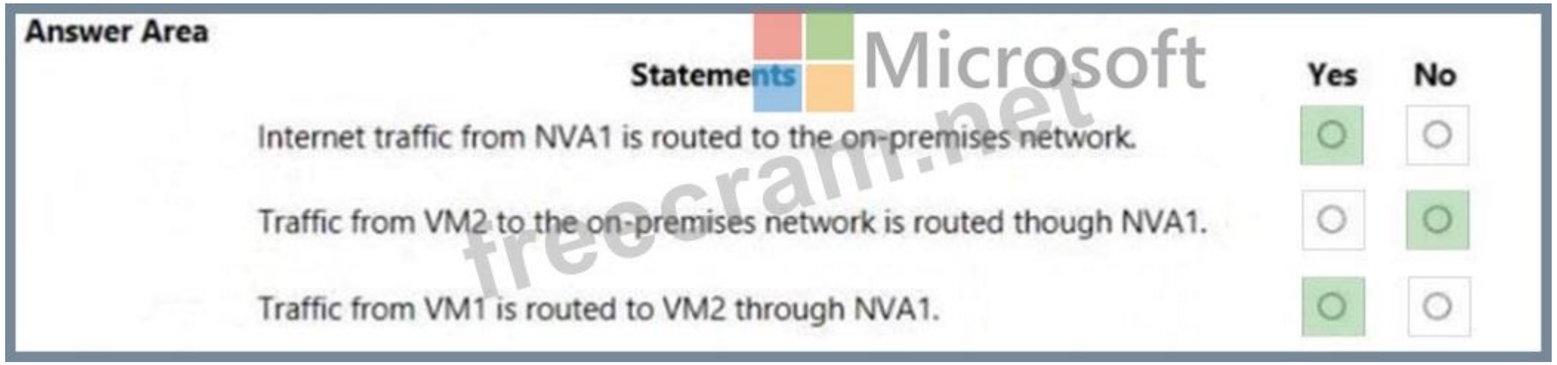
- 0.0.0.0/0
- 10.0.0.0/16

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Internet traffic from NVA1 is routed to the on-premises network.	○	○
Traffic from VM2 to the on-premises network is routed though NVA1.	○	○
Traffic from VM1 is routed to VM2 through NVA1.	○	○



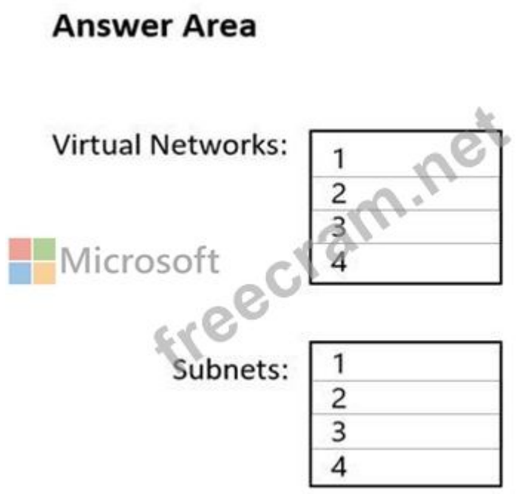
Explanation:
Box 1: Yes
NVA1 with IP (NVA-network virtual appliance) 192.168.0.4 is on the DMZ subnet. It will use route
10.0.0.0/16 to the on-premises network.
Box 2: No
VM2 has IP address 192.168.2.4 and is on the BackEnd subnet. VM2 will not use the RT1 route table, and will not reach the on-premises network through NVA1.
Box 3: Yes
VM1 with IP address 192.168.1.4 is on the FrontEnd subnet, and will use the RT1 routing table. It will use Route2 and Next Hop IP address 192.168.0.4, IP address of NVA1, to reach VM2.

NEW QUESTION: 160
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
Answer: (SHOW ANSWER)
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

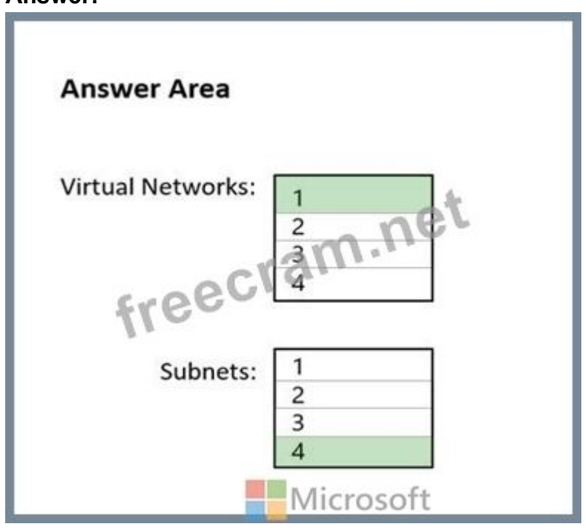
NEW QUESTION: 161
Hotspot Question

You are planning an Azure solution that will contain the following types of resources in a single Azure region:
- Virtual machine
- Azure App Service
- Virtual Network gateway
- Azure SQL Managed Instance

App Service and SQL Managed Instance will be delegated to create resources in virtual networks.
You need to identify how many virtual networks and subnets are required for the solution. The solution must minimize costs to transfer data between virtual networks.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



freecram.net

Explanation:
Answer should be 1 VNET and 4 subnet:
1 for VPN Gateway
1 for SQL managed instance
1 for App service/WebApp
VM is bound to have a separate subnet
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network

NEW QUESTION: 162
You plan to deploy an 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. VPN gateway
B. Azure Bastion
C. Azure Active Directory Domain Services (Azure AD DS)
D. Azure Application Gateway v2
E. Azure Private Link
Answer: A,B,D (LEAVE A REPLY)
Network Application Gateway- WAF-Dedicated Subnet-YES
VPN Gateway-Dedicated Subnet-YES
Azure Firewall-Dedicated Subnet-YES
Azure Bastion-Dedicated Subnet-YES
Network Virtual Appliances-Dedicated Subnet-NO
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure- services#services-that-can-be-deployed-into-a-virtual-network

NEW QUESTION: 163
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 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
Answer: (SHOW ANSWER)
WAF is for web application, while Azure Firewall is for VNETs which is needed for hub.

NEW QUESTION: 164

Your company has 40 branch offices that are linked by using a Software-Defined Wide Area Network (SD-WAN). The SD-WAN uses BGP.
You have an Azure subscription that contains 20 virtual networks configured as a hub and spoke topology. The topology contains a hub virtual network named Vnet1.
The virtual networks connect to the SD-WAN by using a network virtual appliance (NVA) in Vnet1.
You need to ensure that BGP route advertisements will propagate between the virtual networks and the SD-WAN. The solution must minimize administrative effort.
What should you implement?
A. An Azure VPN Gateway that has BGP enabled
B. a NAT gateway
C. Azure Traffic Manager
D. Azure Route Server
Answer: D (LEAVE A REPLY)
Azure Route Server is a fully managed service and is configured with high availability.
Azure Route Server simplifies dynamic routing between your network virtual appliance (NVA) and your virtual network.
When BGP Peering is set up with this, it eliminates the need to manually update routes across all connected networks.
https://learn.microsoft.com/en-us/azure/route-server/overview

NEW QUESTION: 165
Hotspot Question
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.



Answer:



Explanation:

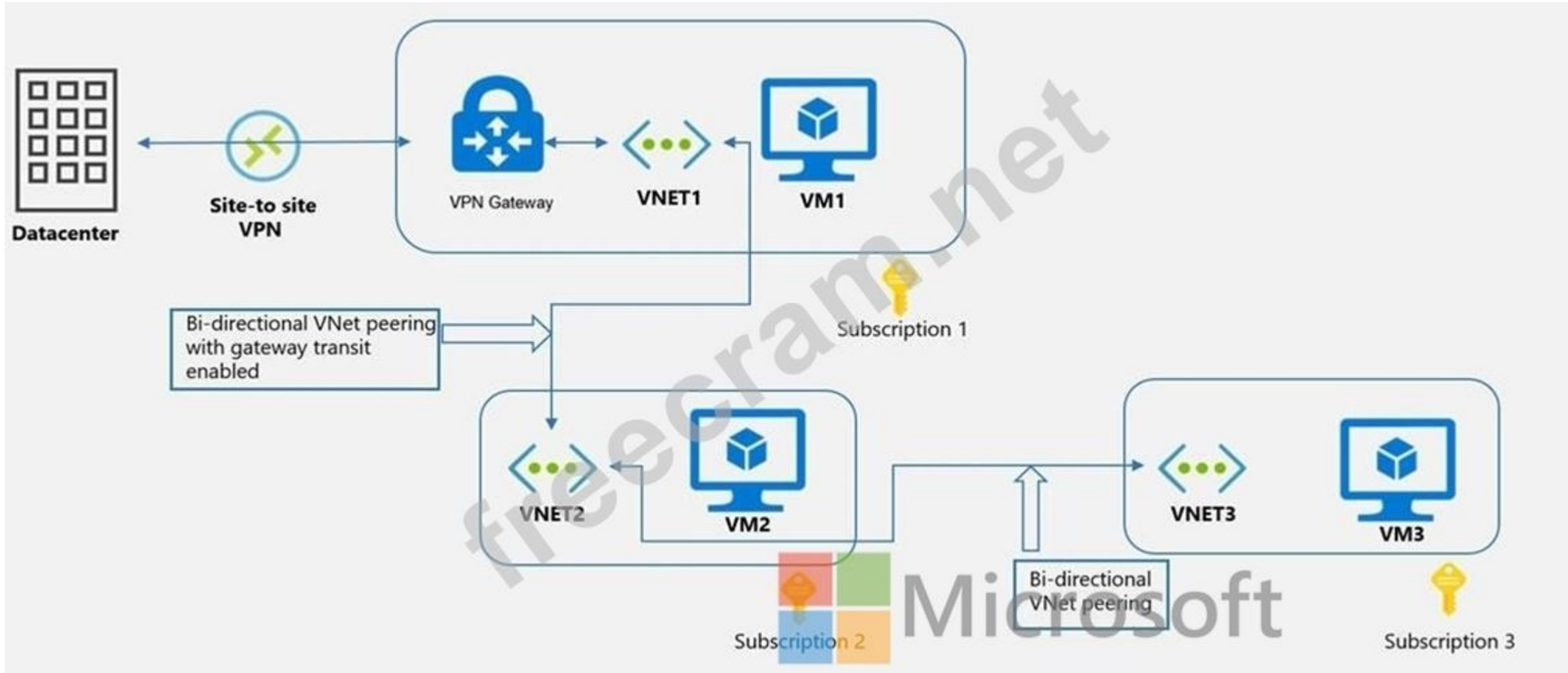
Say your application gateway has a global policy applied to it. Then you apply a different policy to a listener on that application gateway. The listener's policy now takes effect for just that listener. The application gateway's global policy still applies to all other listeners and path-based rules that don't have a specific policy assigned to them.

https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/policy-overview#per-site-waf-policy

NEW QUESTION: 166

Hotspot Question

You have the Azure environment shown in the following exhibit.



freecram.net
Microsoft

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.

Answer Area

VM1 can communicate with **(answer choice):**

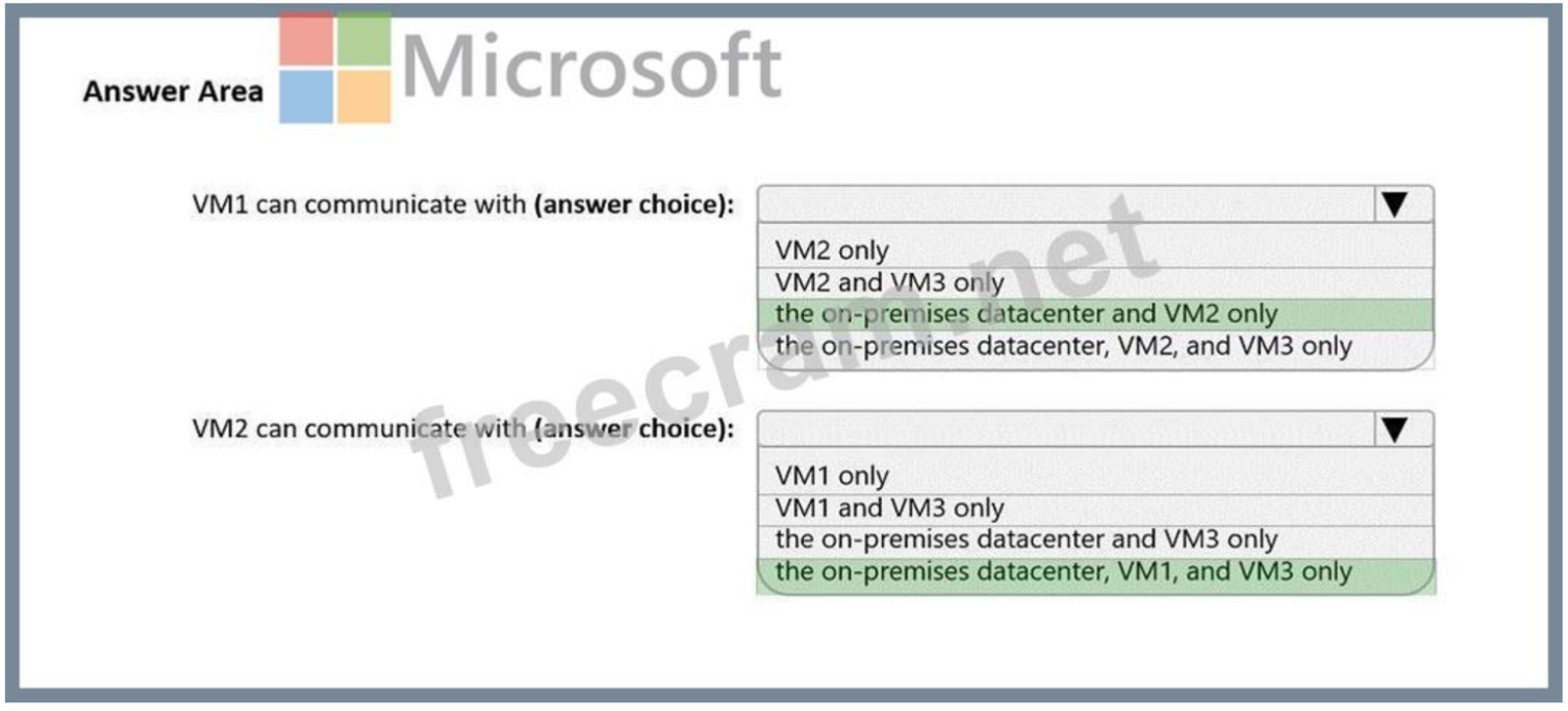
- VM2 only
- VM2 and VM3 only
- the on-premises datacenter and VM2 only
- the on-premises datacenter, VM2, and VM3 only

VM2 can communicate with **(answer choice):**

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

freecram.net

Answer:



Explanation:

Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity.
https://docs.microsoft.com/en-ca/azure/virtual-network/ip-services/ipv6-overview#capabilities

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

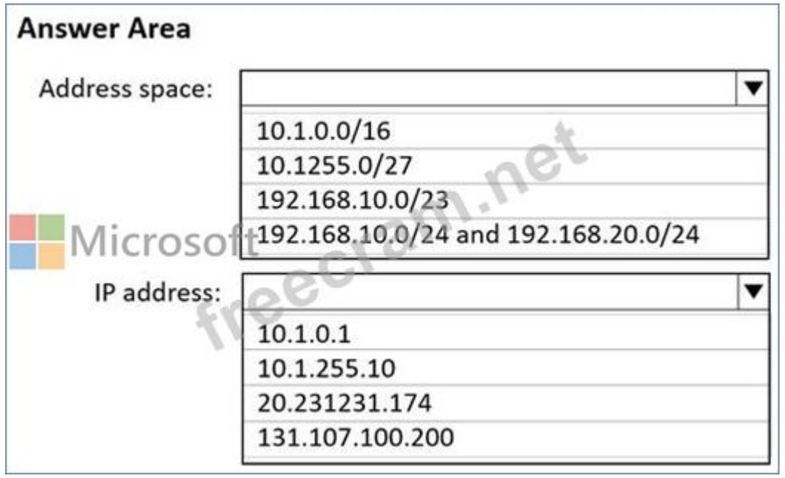
NEW QUESTION: 167
Hotspot Question
Your on-premises network contains the subnets shown in the following table.

Name	IPv4 network address
Subnet1	192.168.10.0/24
Subnet2	192.168.20.0/24

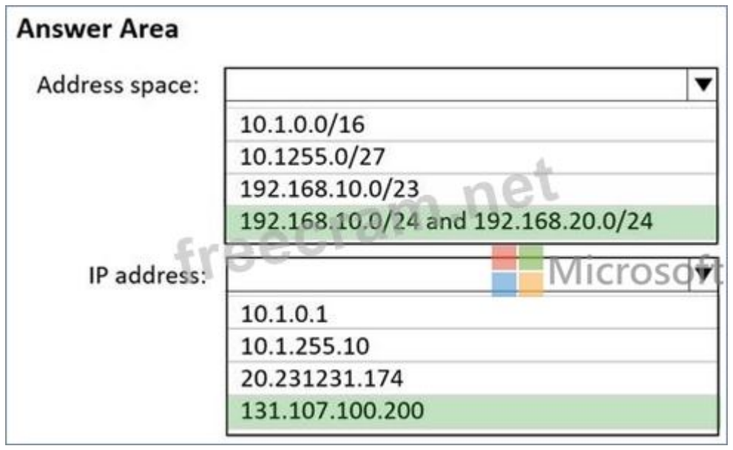
The network contains a firewall named FW1 that uses a public IP address of 131.107.100.200.
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNet1	Virtual network	Uses an address space of 10.1.0.0/16
GW1	Virtual network gateway	• Uses a public IP address of 20.231.231.174 • Uses a private IP address of 10.1.255.10
GatewaySubnet	Subnet	Uses an address space of 10.1.255.0/27
LNG1	Local network gateway	*None*

You plan to configure a Site-to-Site (S2S) VPN named VPN1 that will connect GW1 to FW1.
You need to configure LNG1 to support VPN1. The solution must meet the following requirements:
- Ensure that the resources on Subnet1 and Subnet2 can communicate with the resources on VNet1.
- Minimize administrative effort.
How should you configure LNG1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 168

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

RG1 contains an Azure Network Watcher instance named NW1.

You need to ensure that Admin1 can place a lock on NW1. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

A. User Access Administrator

B. Network Contributor

C. Resource Policy Contributor

D. Monitoring Contributor

Answer: (SHOW ANSWER)

To create or delete management locks, you need access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Only the Owner and the User Access Administrator built- in roles can create and delete management locks.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock- resources?tabs=json#who-can-create-or-delete-locks

NEW QUESTION: 169
You have Azure App Service apps in the West US Azure region as shown in the following table.

Name	App Service Plan	Number of instances
App1	ASP1	3
App2	ASP1	3
App3	ASP2	2
App4	ASP3	1

You need to ensure that all the apps can access the resources in a virtual network named VNet1 without forwarding traffic through the internet.
How many integration subnets should you create?
A. 0
B. 1
C. 2
D. 3
E. 6
Answer: (SHOW ANSWER)
One per App Service Plan: The feature supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can only use the same virtual network integration to a specific subnet. If you need an app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan.
The virtual interface used isn't a resource that customers have direct access to.
https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional- virtual-network-integration-works

NEW QUESTION: 170
Hotspot Question
You have an Azure subscription. The subscription contains 500 virtual machines that run either Windows 11 or Linux.
You need to identify which Linux virtual machines are accessible from the internet. The solution must minimize administrative effort.
What should you use, and what should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.





Explanation:

Microsoft Defender External Attack Surface Management (Defender EASM): Provides an inventory of all external-facing assets and determine which are accessible from the internet, including virtual machines. It minimizes administrative effort by automating discovery and categorization of resources.

Discovery group in Defender EASM: Enables identification and monitoring of external-facing assets based on the subscription and resource configuration, such as virtual machines.

https://learn.microsoft.com/en-us/azure/external-attack-surface-management/overview

https://learn.microsoft.com/en-us/azure/external-attack-surface-management/discovering-your-attack-surface

NEW QUESTION: 171

Hotspot Question

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 192.168.0.0/23
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

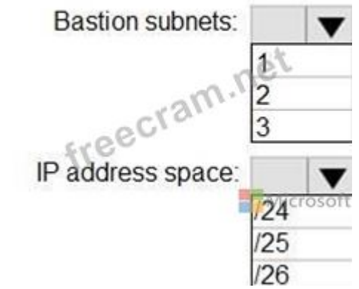
Each virtual network contains 20 virtual machines and a subnet that has an IP address space of /24.

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.

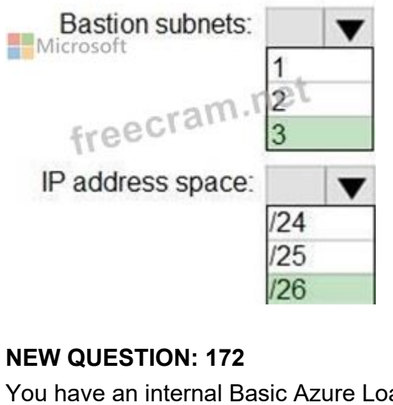
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



NEW QUESTION: 172

You have an internal Basic Azure Load Balancer named LB1 that has two frontend IP addresses.

The backend pool of LB1 contains two Azure virtual machines named VM1 and VM2.

You need to configure the rules on LB1 as shown in the following table.

Rule	Frontend IP address	Protocol	ILB1 port	Destination	VM port
1	65.52.0.1	TCP	80	IP address of the NIC of VM1 and VM2	80
2	65.52.0.2	TCP	80	IP address of the NIC of VM1 and VM2	80

What should you do for each rule?

A. Enable Floating IP.

B. Disable Floating IP.

C. Set Session persistence to Enabled.

D. Set Session persistence to Disabled.

Answer: (SHOW ANSWER)

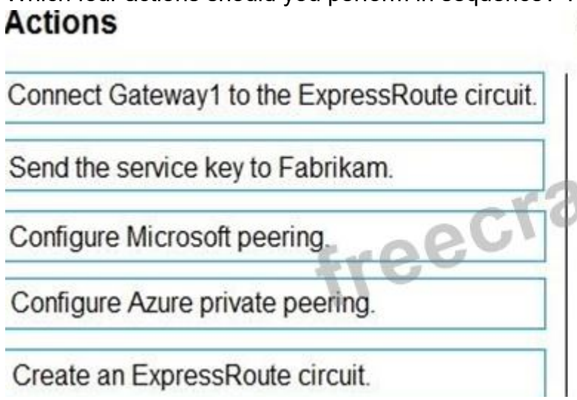
If you want to reuse same port for both load balancing rules then Floating IP needs to be enabled.

https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview#rule-type-2-backend-port-reuse-by-using-floating-ip

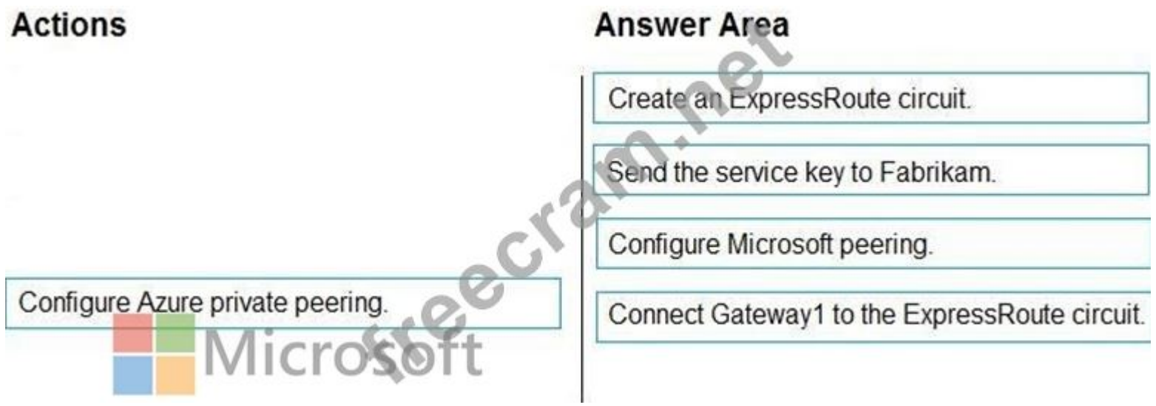
NEW QUESTION: 173

Drag and Drop Question

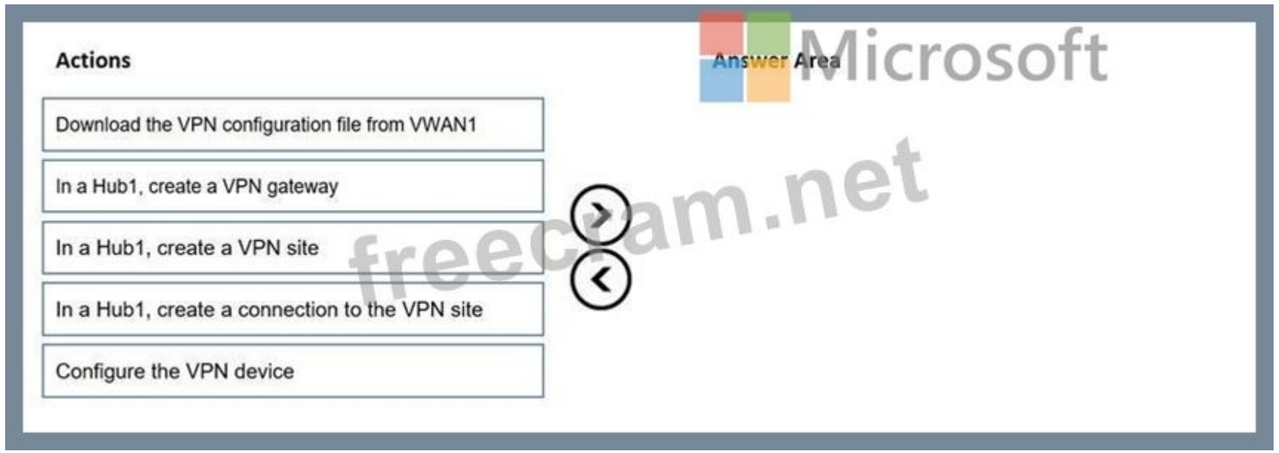
You have an on-premises network.
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains an ExpressRoute gateway named Gateway1.
You need to implement an ExpressRoute solution from a third-party provider named Fabrikam, Inc. The solution must ensure that devices on the on-premises network can connect to the Azure resources on VNet1.
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.



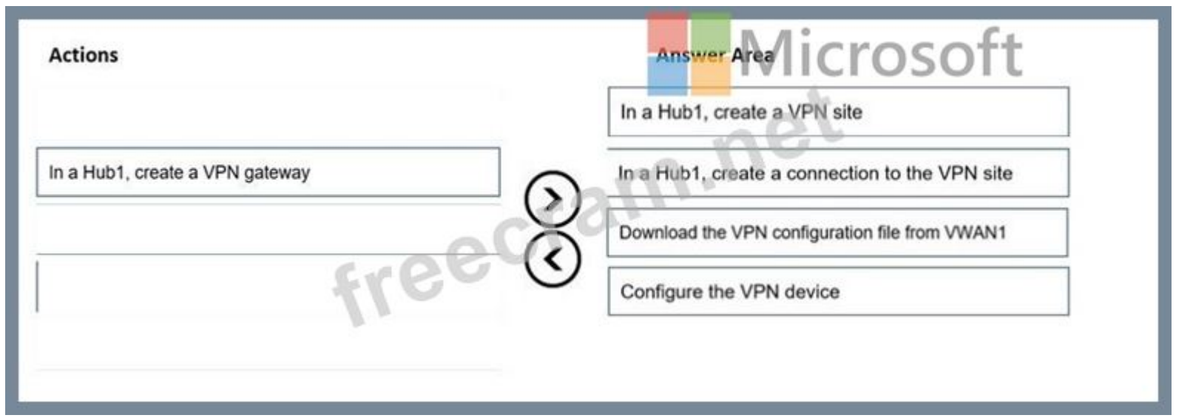
Answer:



NEW QUESTION: 174
Drag and Drop Question
You have three on-premises sites. Each site has a third-party VPN device.
You have an Azure virtual WAN named VWAN1 that has a hub named Hub1. Hub1 connects two of the three on-premises sites by using a Site-to-Site VPN connection.
You need to connect the third site to the other two sites by using Hub1.
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.



Answer:



Explanation:

You've already got the VPN infrastructure setup in Azure so you need to create the Site, Create the connection to the site, Download the stuff, then setup the on-prem side.

Make the site, connect to site, download the thing, config the on-prem.

https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal#vnet

NEW QUESTION: 175

Case Study 3 - Contoso, Ltd

Overview

Proseware, Inc. is a financial services company that has a main office in New York City and a branch office in San Francisco.

Existing Environment. Hybrid Environment

Proseware has an on-premises Active Directory Domain Services (AD DS) forest named corp.proseware.com that syncs with a Microsoft Entra tenant named proseware.com.

Proseware has an Azure subscription that is linked to proseware.com.

Proseware has an internal certification authority (CA).

Existing Environment. Network Infrastructure

The offices contain the resources shown in the following table.

Name	Type	Office	Description
NYCNet	On-premises network	New York City	IP address space of 192.168.0.0/22
SFONet	On-premises network	San Francisco	IP address space of 192.168.100.0/22
NYCDNS1	Server	New York City	DNS server that runs Windows Server 2019 and has an IP address of 192.168.0.100

NYCNet connects to Azure by using an ExpressRoute circuit.

SFONet connects to Azure by using a Site-to-Site (S2S) VPN.

Existing Environment. Azure Resources

The Azure subscription contains the virtual networks and subnets shown in the following table.

Name	Type	Location	Description
HubVNet	Virtual network	East US Azure region	IP address space of 10.0.0.0/20 peered to SpokeVNet
SpokeVNet	Virtual network	East US Azure region	IP address space of 10.0.16.0/20 peered to HubVNet
VPNGW1	Virtual network gateway	HubVNet	Active-passive resiliency, in the Generation 2, VpnGw3 SKU that has the default ASN connected to SFONet
SUBNET-PE	Subnet	HubVNet	Used for private endpoints
SUBNET-JUMPHOSTS	Subnet	HubVNet	Used for jump hosts
SUBNET-APPGW1	Subnet	SpokeVNet	Contains an Azure application gateway named APPGW1

The subscription contains four virtual machines named VM1, VM2, VM3, and VM4. VM1 and VM2 host an app named App1.

VM3 and VM4 host a web app named App2 that is accessed by using a FQDN of app2.proseware.com. Users access app2.proseware.com by using HTTP or HTTPS.

VM1, VM2, and VM4 are connected to SpokeVNet.

The subscription contains Application Gateway resources shown in the following table.

Name	Type	Location	Description
APPGW1	Application Gateway	SpokeVNet	In the Azure Web Application Firewall (WAF) V2 SKU Terminates HTTPS connections to a backend pool that contains VM3 and VM4
APPGW1-NSG1	Network security group (NSG)	East US region	Associated with SUBNET-APPGW1
APPGW1-WAFPolicy	Azure Web Application Firewall (WAF) policy	East US region	Applied to APPGW1

The subscription contains an Azure Front Door Standard profile named FD1. FD1 contains a single origin group that targets APPGW1 by using the default endpoint name.

HubVNet connects to NYCNet by using an ExpressRoute gateway named ERGW1.

Planned Changes and Requirements. Planned Changes
Proseware plans to implement the following changes:
- Deploy an Azure Private DNS Resolver named PRDNS1 to HubVNet and link PRDNS1 to SpokeVNet.
- Create a DNS forwarding ruleset named DNSRS1 and associate DNSRS1 with PRDNS1.
- Deploy Azure Virtual Network Manager and implement the following rules:
- Allow inbound connections on TCP port 3389 from the on-premises networks to SUBNET- JUMPHOSTS.
- Block inbound connections on TCP port 80 from the internet to SpokeVNet.
- Ensure that Azure Virtual Network Manager rules take precedence over conflicting NSG rules.
- Deploy two network virtual appliances (NVAs) named NVA1 and NVA2 to HubVNet.
- Deploy a gateway load balancer named LBGW1 to HubVNet.
- Configure LBGW1 to inspect traffic on TCP ports 443, 1433, and 1434 from LBS1 by using NVA1 and NVA2.
- Ensure that all the traffic to App2 is processed by using FD1.
Planned Changes and Requirements. Connectivity requirements
Proseware identifies the following connectivity requirements:
- Minimize the complexity of the Azure Virtual Network Manager deployment.
- Route traffic between NYCNet and SFONet via the ExpressRoute circuit and the S2S VPN.
- Ensure that remote users on Windows 11 devices can connect to HubVNet by using a Point-to- Site (P2S) VPN and their proseware.com credentials.
Planned Changes and Requirements. Security requirements
Proseware identifies the following security requirements:
- Whenever possible, use the internal CA.
- Ensure that all connections routed via APPGW1 use end-to-end encryption.
- Ensure that user connections to Azure-hosted apps use end-to-end encryption.
- Ensure that all inbound internet traffic to app2.proseware.com is routed via FD1.
- Prevent devices that connect to NYCNet from accessing Azure services that use private endpoints.
- Enable the virtual machines that connect to HubVNet and SpokeVNet to access Azure services that use private endpoints.
Planned Changes and Requirements. General requirements
Proseware identifies the following general requirements:
- Minimize the IP address space required to deploy platform-managed resources to the virtual networks.
- From SpokeVNet, resolve name resolution requests for the azure.proseware.com namespace and the corp.proseware.com namespace by using PRDNS1.
- Whenever possible, minimize administrative effort.
Hotspot Question
You need to configure connectivity between NYCNet and SFONet. The solution must meet the connectivity requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



For HubVNet:

- Configure a user-defined route (UDR).
- Deploy an Azure Route Server.
- Implement an Azure Virtual Network Manager connectivity configuration.

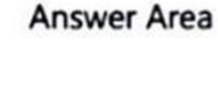
For VPNGW1:

- Change the ASN number.
- Configure active-active mode.
- Resize the SKU.

freecram.net

Answer:

Answer Area



For HubVNet:

- Configure a user-defined route (UDR).
- Deploy an Azure Route Server.
- Implement an Azure Virtual Network Manager connectivity configuration.

freecram.net



For VPNGW1:

- Change the ASN number.
- Configure active-active mode.
- Resize the SKU.

NEW QUESTION: 176

Hotspot Question

You have an Azure subscription that contains the route tables and routes shown in the following table.

Route table name	Route name	Prefix	Destination
RT1	Default Route	0.0.0.0/0	VirtualNetworkGateway
RT2	Default Route	0.0.0.0/0	Internet

The subscription contains the subnets shown in the following table.

Name	Prefix	Route table	Virtual network
Subnet1	10.10.1.0/24	RT1	Vnet1
Subnet2	10.10.2.0/24	RT2	Vnet1
GatewaySubnet	10.10.3.0/24	None	Vnet1

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

Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

The subscription contains the local network gateways shown in the following table.

Name	Prefix	Default site
New York	10.9.0.0/16	Yes
Seattle	10.8.0.0/16	No

There is a Site-to-Site VPN connection to each local network gateway.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	◯	◯
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	◯	◯
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	◯	◯

Answer:

Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	○	○

Microsoft
freecram.net

Explanation:

Box 1: No

All outbound traffic from VM2 is sent to the internet by default.

Box 2: No

The effective route table show the all the the subnet on the same VNET as a more specific one than the default route and Gateway routes. So subnets within a vnet can communicate can communicate directly.

Box 3: Yes

All outbound traffic from VM1 is sent to the VPN gateway.

https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm

NEW QUESTION: 177

Drag and Drop Question

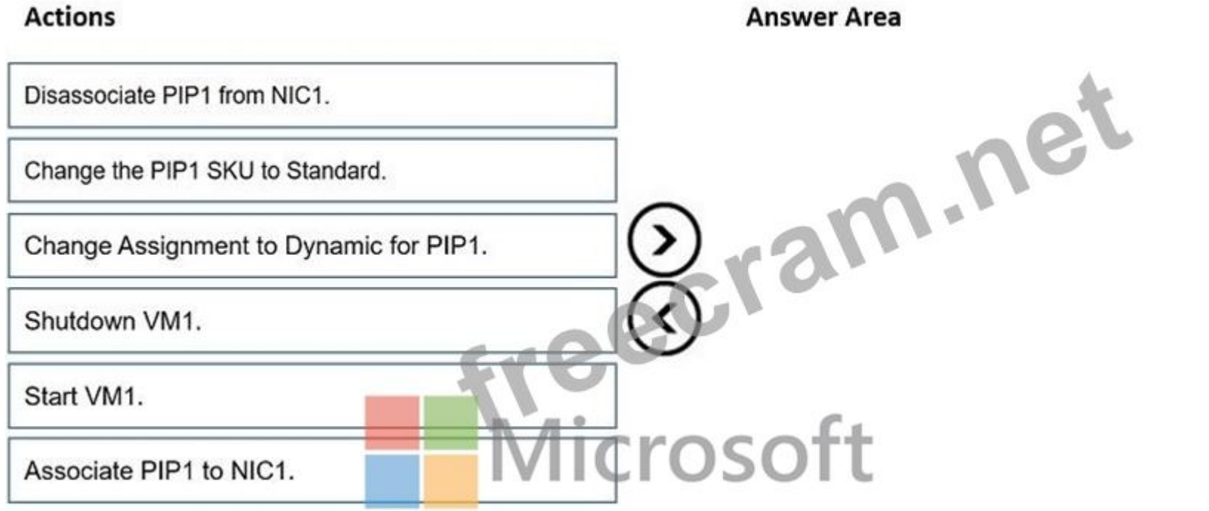
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
Gateway1	NAT gateway	Unconfigured
NIC1	Network interface	A network interface with a statically assigned public IP address named PIP1
PIP1	Public IP address	A Basic SKU public IP address
VNet1	Virtual network	Contains a subnet named Subnet1
Subnet1	Virtual subnet	Part of VNet1
VM1	Virtual machine	Connected to Subnet1 via NIC1

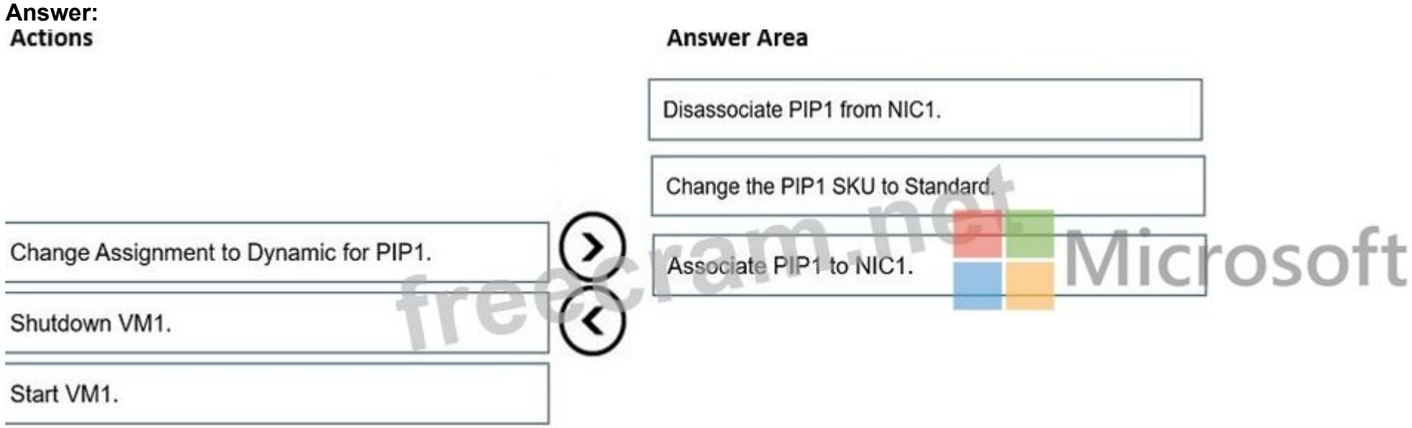
Microsoft
freecram.net

You need to associate Gateway1 with Subnet1. The solution must minimize downtime on VM1.

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.



Answer:

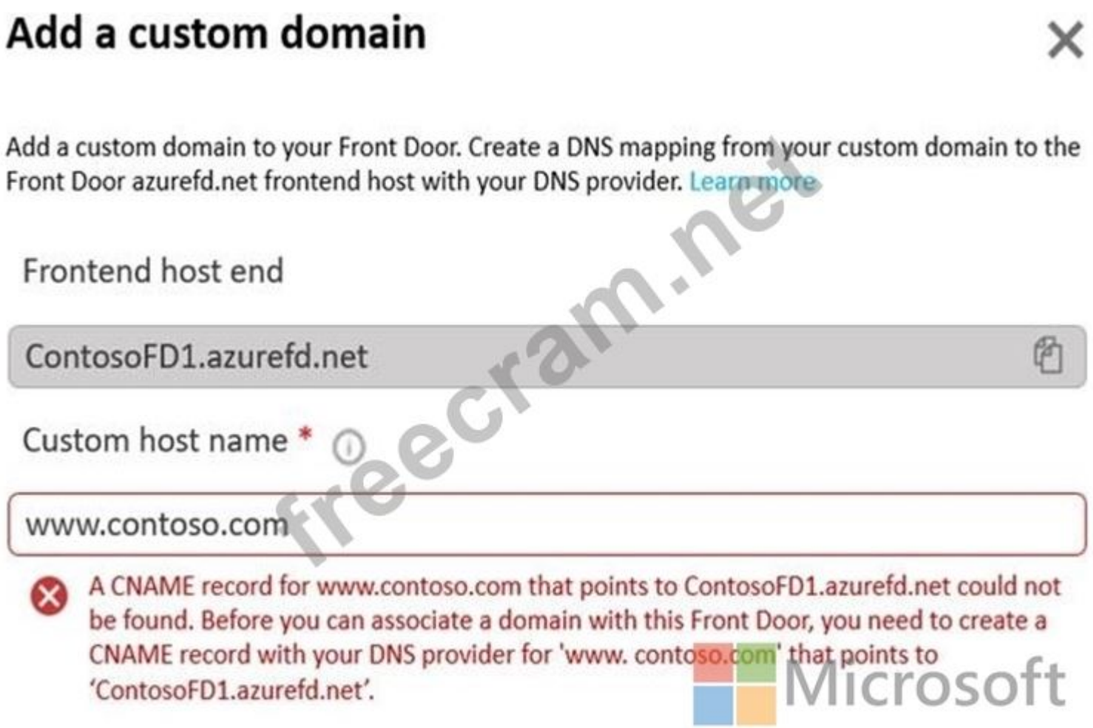


Explanation:
https://learn.microsoft.com/en-us/azure/nat-gateway/tutorial-migrate-ilip-nat

NEW QUESTION: 178
You decide to create a Point-to-Site VPN connection to connect you to your virtual network from home. In this case, Point-to-Site VPN can use any of the following protocols except:
A. SSTP
B. OpenVPN
C. IPSecright
D. IKEv2 VPN
Answer: (SHOW ANSWER)
Point-to-Site (P2S) VPN can use any one of the below-given protocols:
OpenVPN Protocol, an SSL/TLS based VPN protocol.

SSTP (Secure Socket Tunneling Protocol), a proprietary TLS-based VPN protocol.
IKEv2 VPN, a standards-based IPsec VPN solution.
Option A is incorrect. SSTP can be used by a P2S VPN.
Option B is incorrect. P2S VPN can use any one of these three: SSTP, OpenVPN or IKEv2 VPN.
Option C is correct. IPSec protocol can't be used by P2S VPN.
Option D is incorrect. P2S VPN can use any one of these three: SSTP, OpenVPN, or IKEv2 VPN.
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

NEW QUESTION: 179
You have a website that uses an FQDN of www.contoso.com. The DNS record tor www.contoso.com resolves to an on-premises web server.
You plan to migrate the website to an Azure web app named Web1. The website on Web1 will be published by using an Azure Front Door instance named ContosoFD1.
You build the website on Web1.
You plan to configure ContosoFD1 to publish the website for testing. When you attempt to configure a custom domain for www.contoso.com on ContosoFD1, you receive the error message shown in the exhibit.



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 www.contoso.com to ContosoFD1.azurefd.net
B. a CNAME record that maps www.contoso.com to Web1.contoso.com
C. a CNAME record that maps afdverify.www.contoso.com to ContosoFD1.azurefd.net
D. a CNAME record that maps afdverify.www.contoso.com to afdverify.ContosoFD1.azurefd.net

Answer: (SHOW ANSWER)

This is to map the custom domain while regsitering to the Azure portal without affecting Web traffic traffic ...

With this method, users can access your domain without interruption while the DNS mapping occurs.

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#map-the-temporary- afdverify-subdomain%20Community%20vote%20distribution

NEW QUESTION: 180

Hotspot Question

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

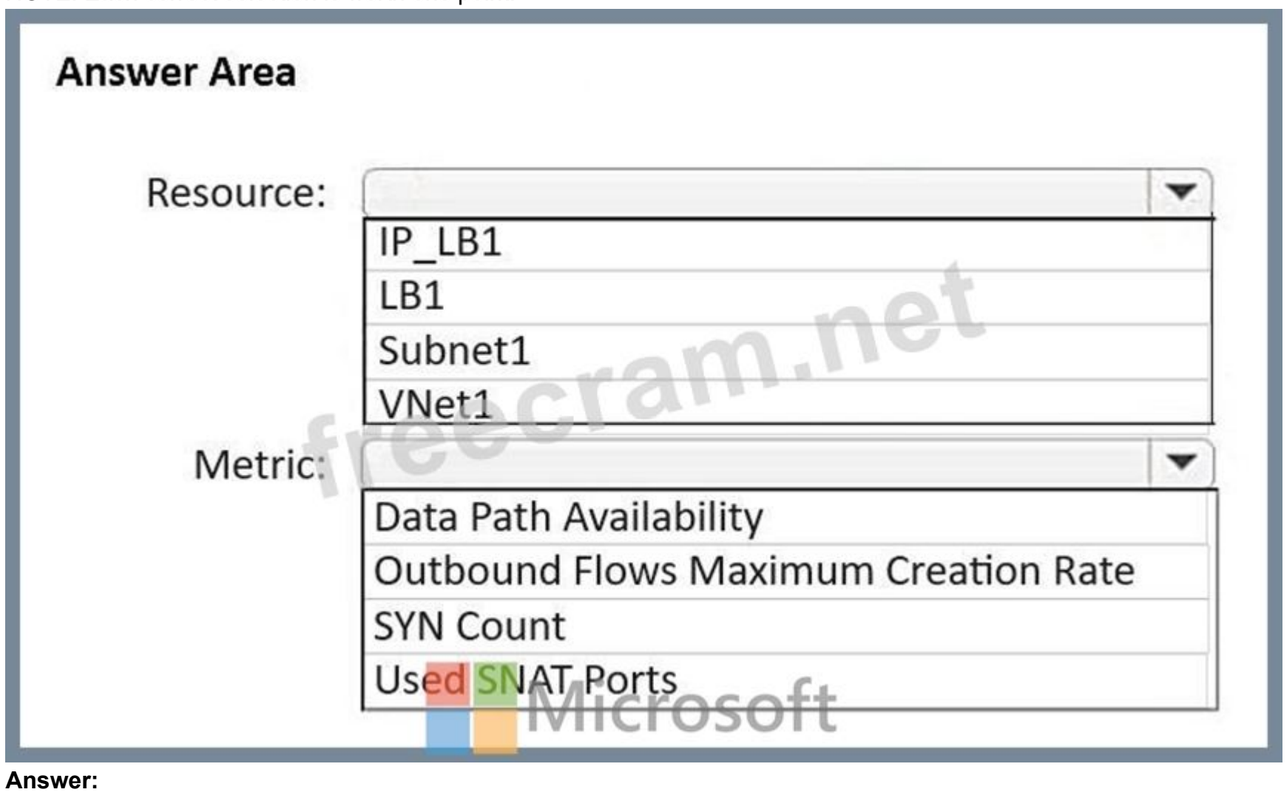
Name	Description
VNet1	Virtual network
Subnet1	Subnet on VNet1 Contains 350 virtual machines that connect to the internet by using LB1
LB1	Public load balancer connected to Subnet1
IP_LB1	Public IP address of LB1

freecram.net Microsoft

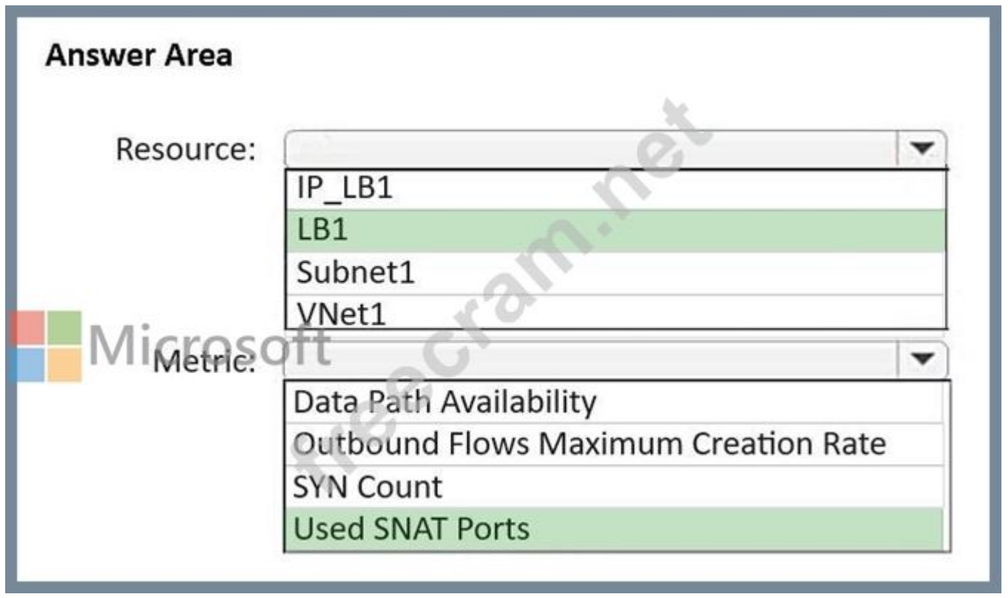
You need to identify the number of established outbound connections from the virtual machines.

Which resource and metric should you review? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections

NEW QUESTION: 181
You need to configure a security policy. As a process, first you find the name for the resource group containing Front Door profile with the help of Get-AzResourceGroup. Now, which of the following cmdlet would you use to configure a security policy in the identified resource group?
A. New-AzFrontDoorWafPolicy
B. Set-AzFrontDoorWafPolicy
C. New-AzFrontDoorPolicry
D. New-AzureFrontDoorWafPolicy
Answer: (SHOW ANSWER)
New-AzFrontDoorWafPolicy cmdlet is used to configure a security policy with already created rules in the specific resource group containing the Front Door profile.
Option A is correct. New-AzFrontDoorWafPolicy is the right command.
Option B is incorrect. Set-AzFrontDoorWafPolicy is not the right command to configure the security policy.
Option C is incorrect. New-AzFrontDoorPolicy is not the right command.
Option D is incorrect. New-AzureFrontDoorWafPolicy is not a valid command in Azure PowerShell.
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-custom-rules- powershell?WT.mc_id=modinfra-33046-thmaure

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 182
Case Study 3 - Contoso, Ltd

Overview

Proseware, Inc. is a financial services company that has a main office in New York City and a branch office in San Francisco.

Existing Environment. Hybrid Environment

Proseware has an on-premises Active Directory Domain Services (AD DS) forest named corp.proseware.com that syncs with a Microsoft Entra tenant named proseware.com.

Proseware has an Azure subscription that is linked to proseware.com.

Proseware has an internal certification authority (CA).

Existing Environment. Network Infrastructure

The offices contain the resources shown in the following table.

Name	Type	Office	Description
NYCNet	On-premises network	New York City	IP address space of 192.168.0.0/22
SFONet	On-premises network	San Francisco	IP address space of 192.168.100.0/22
NYCDNS1	Server	New York City	DNS server that runs Windows Server 2019 and has an IP address of 192.168.0.100

NYCNet connects to Azure by using an ExpressRoute circuit.

SFONet connects to Azure by using a Site-to-Site (S2S) VPN.

Existing Environment. Azure Resources

The Azure subscription contains the virtual networks and subnets shown in the following table.

Name	Type	Location	Description
HubVNet	Virtual network	East US Azure region	IP address space of 10.0.0.0/20 peered to SpokeVNet
SpokeVNet	Virtual network	East US Azure region	IP address space of 10.0.16.0/20 peered to HubVNet
VPNGW1	Virtual network gateway	HubVNet	Active-passive resiliency, in the Generation 2, VpnGw3 SKU that has the default ASN connected to SFONet
SUBNET-PE	Subnet	HubVNet	Used for private endpoints
SUBNET-JUMPHOSTS	Subnet	HubVNet	Used for jump hosts
SUBNET-APPGW1	Subnet	SpokeVNet	Contains an Azure application gateway named APPGW1

The subscription contains four virtual machines named VM1, VM2, VM3, and VM4. VM1 and VM2 host an app named App1.

VM3 and VM4 host a web app named App2 that is accessed by using a FQDN of app2.proseware.com. Users access app2.proseware.com by using HTTP or HTTPS.

VM1, VM2, and VM4 are connected to SpokeVNet.

The subscription contains Application Gateway resources shown in the following table.

Name	Type	Location	Description
APPGW1	Application Gateway	SpokeVNet	In the Azure Web Application Firewall (WAF) V2 SKU Terminates HTTPS connections to a backend pool that contains VM3 and VM4
APPGW1-NSG1	Network security group (NSG)	East US region	Associated with SUBNET-APPGW1
APPGW1-WAFPolicy	Azure Web Application Firewall (WAF) policy	East US region	Applied to APPGW1

freecram.net

The subscription contains an Azure Front Door Standard profile named FD1. FD1 contains a single origin group that targets APPGW1 by using the default endpoint name.

HubVNet connects to NYCNet by using an ExpressRoute gateway named ERGW1.

Planned Changes and Requirements. Planned Changes

Proseware plans to implement the following changes:

- Deploy an Azure Private DNS Resolver named PRDNS1 to HubVNet and link PRDNS1 to SpokeVNet.
- Create a DNS forwarding ruleset named DNSRS1 and associate DNSRS1 with PRDNS1.
- Deploy Azure Virtual Network Manager and implement the following rules:
- Allow inbound connections on TCP port 3389 from the on-premises networks to SUBNET- JUMPHOSTS.
- Block inbound connections on TCP port 80 from the internet to SpokeVNet.
- Ensure that Azure Virtual Network Manager rules take precedence over conflicting NSG rules.
- Deploy two network virtual appliances (NVAs) named NVA1 and NVA2 to HubVNet.
- Deploy a gateway load balancer named LBGW1 to HubVNet.
- Configure LBGW1 to inspect traffic on TCP ports 443, 1433, and 1434 from LBS1 by using NVA1 and NVA2.
- Ensure that all the traffic to App2 is processed by using FD1.

Planned Changes and Requirements. Connectivity requirements

Proseware identifies the following connectivity requirements:

- Minimize the complexity of the Azure Virtual Network Manager deployment.
- Route traffic between NYCNet and SFONet via the ExpressRoute circuit and the S2S VPN.
- Ensure that remote users on Windows 11 devices can connect to HubVNet by using a Point-to- Site (P2S) VPN and their proseware.com credentials.

Planned Changes and Requirements. Security requirements

Proseware identifies the following security requirements:

- Whenever possible, use the internal CA.
- Ensure that all connections routed via APPGW1 use end-to-end encryption.
- Ensure that user connections to Azure-hosted apps use end-to-end encryption.
- Ensure that all inbound internet traffic to app2.proseware.com is routed via FD1.
- Prevent devices that connect to NYCNet from accessing Azure services that use private endpoints.
- Enable the virtual machines that connect to HubVNet and SpokeVNet to access Azure services that use private endpoints.

Planned Changes and Requirements. General requirements

Proseware identifies the following general requirements:

- Minimize the IP address space required to deploy platform-managed resources to the virtual networks.
- From SpokeVNet, resolve name resolution requests for the azure.proseware.com namespace and the corp.proseware.com namespace by using PRDNS1.
- Whenever possible, minimize administrative effort.

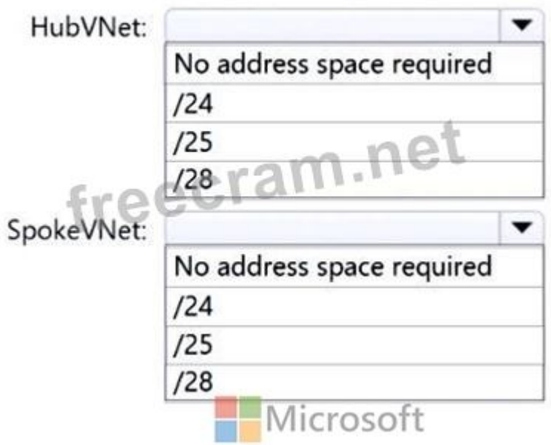
Hotspot Question

You need to identify which IP address space to allocate for the planned deployment of PRDNS1 to HubVNet and SpokeVNet. The solution must meet the general requirements.

What should you identify for each virtual network? To answer, select the appropriate options in the answer area.

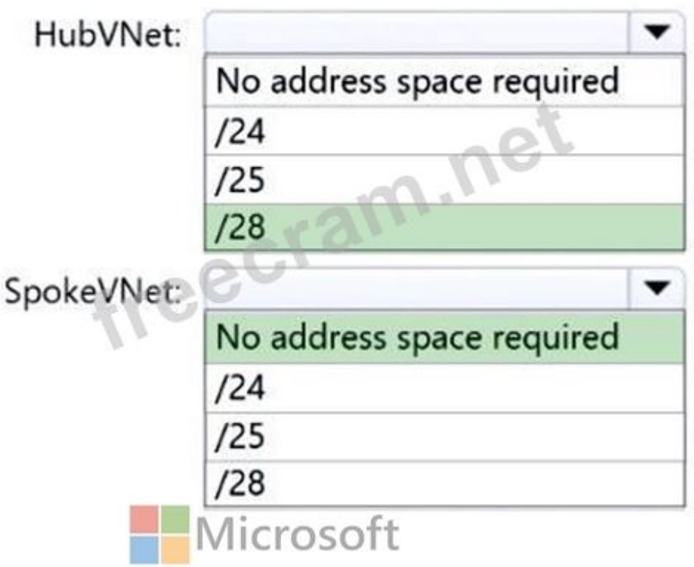
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

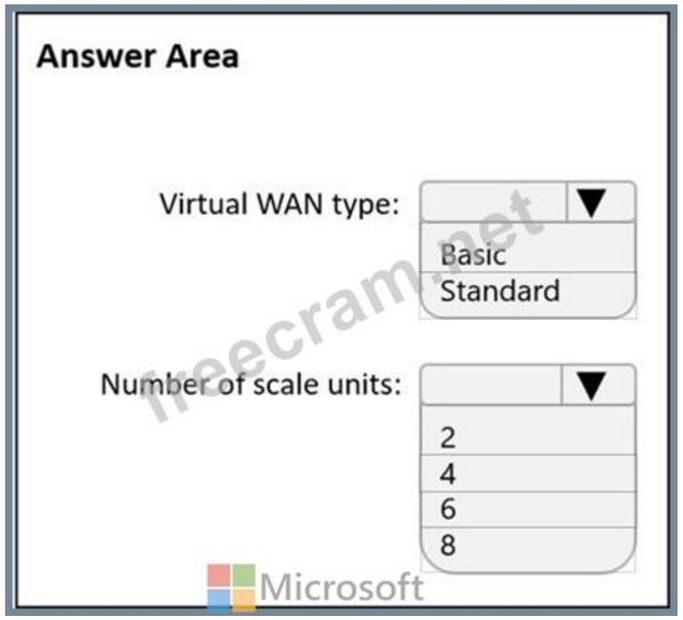
Answer Area



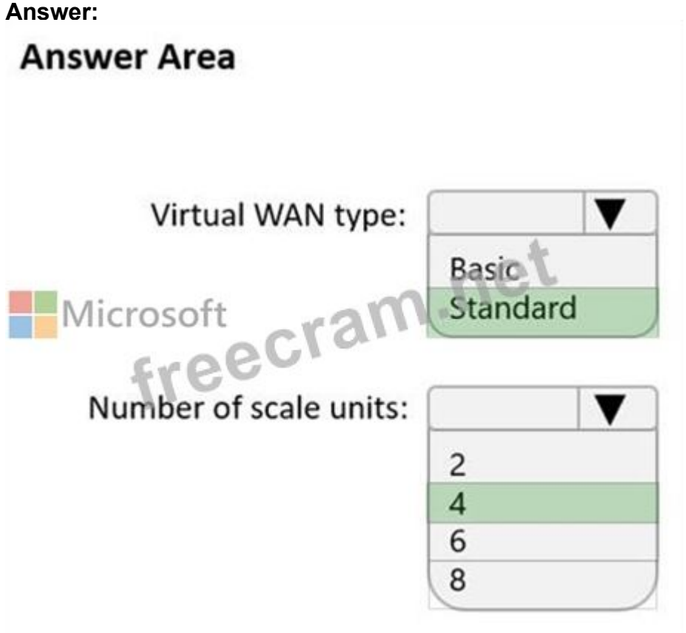
NEW QUESTION: 183

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The subscription contains the following resources:
- An Azure App Service app named App1
- An Azure DNS zone named contoso.com
- An Azure private DNS zone named private.contoso.com
- A virtual network named Vnet1
You create a private endpoint for App1. The record for the endpoint is registered automatically in Azure DNS.
You need to provide a developer with the name that is registered in Azure DNS for the private endpoint.
What should you provide?
A. app1.privatelink.azurewebsites.net
B. app1.contoso.com
C. app1.contoso.onmicrosoft.com
D. app1.private.contoso.com
Answer: (SHOW ANSWER)
When you use Private Endpoint for Web App, the requested URL must match the name of your Web App. By default mywebappname.azurewebsites.net.
By default, without Private Endpoint, the public name of your web app is a canonical name to the cluster. For example, the name resolution will be:
DNS
Name Type Value
mywebapp.azurewebsites.net CNAME clustername.azurewebsites.windows.net
clustername.azurewebsites.windows.net CNAME cloudservicename.cloudapp.net cloudservicename.cloudapp.net A 40.122.110.154 When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net. For example, the name resolution will be:
DNS
Name Type Value Remark
mywebapp.azurewebsites.net CNAME mywebapp.privatelink.azurewebsites.net mywebapp.privatelink.azurewebsites.net CNAME clustername.azurewebsites.windows.net clustername.azurewebsites.windows.net CNAME cloudservicename.cloudapp.net cloudservicename.cloudapp.net A 40.122.110.154
https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint

NEW QUESTION: 184
Hotspot Question
You plan to deploy Azure Virtual WAN.
You need to deploy a virtual WAN hub that meets the following requirements:
- Supports 10 sites that will connect to the virtual WAN hub by using a Site-to-Site VPN connection
- Supports 8 Gbps of ExpressRoute traffic
- Minimizes costs
What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Box1: Standard
Basic virtual WAN supports Site-to-site VPN only
Standard virtual WAN supports
ExpressRoute
User VPN (P2S)

VPN (site-to-site)
Inter-hub and VNet-to-VNet transiting through the virtual hub
Azure Firewall
NVA in a virtual WAN
Box 2: 4
8 Gig Express Route. 2 GB per ER scale unit. Therefore number of scale units = 8/2 = 4 Express Route Scale Units and Connectivity: Similar in concept to VPN scale units, customers seeking to deploy Express Route connectivity into their Virtual WAN Hubs will incur costs for the scale units provisioned in that hub, with options ranging from 1 to 10 with each representing
2Gbps of ER throughput.
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about
https://www.wwt.com/article/microsoft-azure-virtual-wan-cloud-networking-architecture

NEW QUESTION: 185
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
Answer: (SHOW ANSWER)
Another concept to make use of in constructing effective Custom Rules is compound conditions.
Rules can be created with a single condition, or you can add multiple conditions that must be satisfied to constitute a match. When adding multiple conditions, they are added as an AND statement, so all conditions must be met for the Action to take place. If you need to construct a rule with OR logic, it is best to create multiple rules with the same Action.
https://techcommunity.microsoft.com/t5/azure-network-security-blog/azure-waf-custom-rule-samples-and-use-cases/ba-p/2033020

NEW QUESTION: 186
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. On FW1, create an outbound service tag rule for AzureCloud.
B. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).

C. Deploy a NAT gateway.
D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.
Answer: (SHOW ANSWER)
The Azure Windows VMs need to connect to the Azure KMS server for Windows activation. The activation requires that the activation request come from an Azure public IP address.
To resolve this problem, use the Azure custom route to route activation traffic to the Azure KMS server.
Reference:
https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/custom-routes-enable-kms-activationwvd/

NEW QUESTION: 187
SIMULATION



Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You plan to use VNET4 for an Azure API Management implementation.
You need to configure a policy that can be used by an Azure application gateway to protect against known web attack vectors. The policy must only allow requests that originate from IP addresses in Canada. You do NOT need to create the application gateway to complete this task.
To complete this task, sign in to the Azure portal.
Answer:

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

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

Plan:
Stage 1: Create a WAF policy
Stage 2: Create a custom WAF Geo location rule that blocks all traffic outside Canada
Stage 3: Create a custom WAF Geo location rule that allows traffic from Canada

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

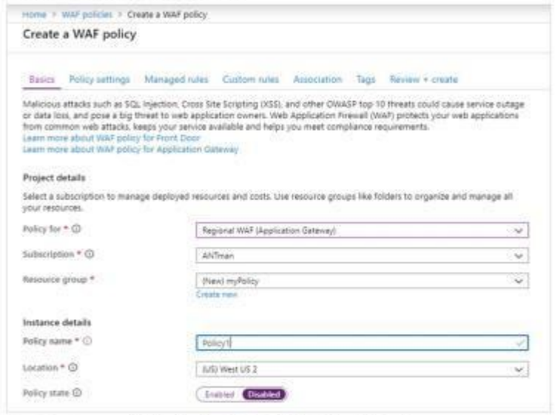
Step 1: On the upper left side of the portal, select Create a resource. Search for WAF, select Web Application Firewall, then select Create.

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

* details omitted *

Step 3: On the Association tab, select Add association, then select one of the following settings:
Application Gateway: Select the application gateway, and then select Add.
HTTP Listener: Select the application gateway, select the listeners, then select Add.
Route Path: Select the application gateway, select the listener, select the routing rule, and then select Add.

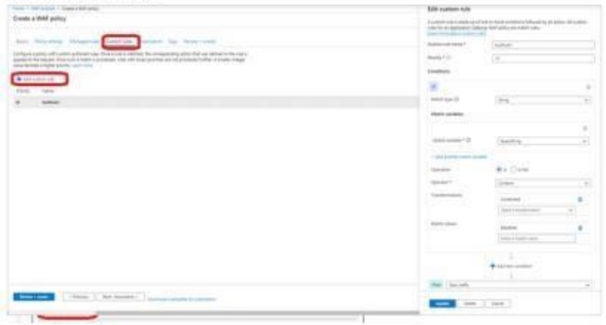
Step 4: Select Review + create, then select Create.



Stage 2: Create a custom WAF Geo location rule that blocks all traffic outside Canada
Configure WAF rules :
When you create a WAF policy, by default it is in Detection mode. In Detection mode, WAF doesn't block any requests. Instead, the matching WAF rules are logged in the WAF logs. To see WAF in action, you can change the mode settings to Prevention. In Prevention mode, matching rules defined in the CRS Ruleset you selected are blocked and/or logged in the WAF logs.

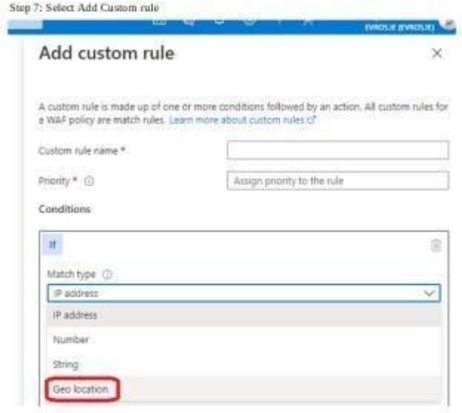
Custom rules

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



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

Step 7: Select Add Custom rule



Step 8: Select Geo location

Create your Custom Rule with an appropriate name and priority, then choose 'Geo location' from the Match type drop down as above. Next, you'll want to ensure you choose RemoteAddr as the match variable, and decide what logic you want to apply. By logic I mean the pattern that will fire

the rule. In this example, I want all traffic except Ireland blocked. So I will choose the Operation 'Is not', then location Ireland, then Deny. If I wanted all traffic allowed and Ireland blocked, I would simply choose the Operation 'Is'. I recommend figuring out your pattern then working your way through the final section of the CR.

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

Conditions



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

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

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

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

NEW QUESTION: 188
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 v2
C. Azure Application Gateway v1
D. Azure Standard Load Balancer
Answer: (SHOW ANSWER)

NEW QUESTION: 189
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
Answer: (SHOW ANSWER)
https://azure.microsoft.com/en-us/pricing/details/ddos-protection/

NEW QUESTION: 190



Username and password
Use the following login credentials as needed:
- To enter your username, place your cursor in the Sign in box and click on the username below.
- To enter your password, place your cursor in the Enter password box and click on the password below.
- Azure Username: User-12345678@cloudslice.onmicrosoft.com
- Azure Password: xxxxxxxxxx
- If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support purposes only:
- Lab Instance: 12345678
You are preparing to connect your on-premises network to VNET4 by using a Site-to-Site VPN.
The on-premises endpoint of the VPN will be created on a firewall named Firewall1.

The on-premises network has the following configuration:
- internal address range: 10.10.0.0/16
- Firewall1 internal IP address: 10.10.1.1
- Firewall public IP address: 131.107.50.60
BGP is NOT used.
You need to create the object that will provide the IP addressing configuration of the on-premises network to the Site-to-Site VPN. You do NOT need to create a virtual network gateway to complete this task.
To complete this task, sign in to the Azure portal.
Answer:

Create a site-to-site VPN connection in the Azure portal
We only create a local network gateway

The local network gateway is a specific object that represents your on-premises location (the site) for routing purposes. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you'll create a connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. If your on-premises network changes or you need to change the public IP address for the VPN device, you can easily update the values later.

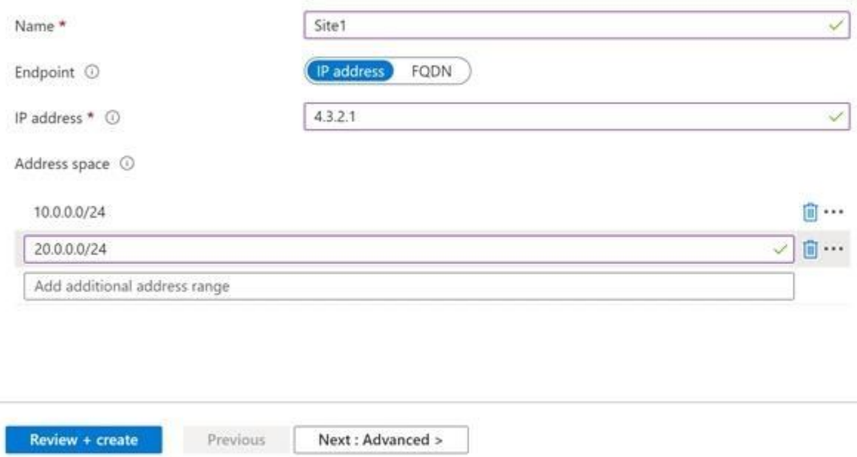
Step 1: From the Azure portal, in Search resources, services, and docs (G+/) type local network gateway. Locate local network gateway under Marketplace in the search results and select it. This opens the Create local network gateway page.

Step 2: On the Create local network gateway page, on the Basics tab, specifiy the values for your local network gateway.

* Select Endpoint type: IP address
* Endpoint: Enter 131.107.50.60 (The Firewall public IP address)
(IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device, select the IP address option and fill in the IP address as shown in the example. This is the public IP address of the VPN device that you want Azure VPN gateway to connect to. If you don't have the IP address right now, you can use the values shown in the example, but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure won't be able to connect.)
* Address Space: Enter 10.10.0.0/16 (The internal address range)

Select the endpoint type for the on-premises VPN device - IP address or FQDN (Fully Qualified Domain Name).
IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device.





Step 3: On the Advanced tab, you can configure BGP settings if needed. Skip this.

Step 4: When you have finished specifying the values, select Review + create at the bottom of the page to validate the page.

Step 5: Select Create to create the local network gateway object.

Reference:
https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal

NEW QUESTION: 191
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.
Answer: (SHOW ANSWER)
Virtual Wan requires a Wan Hub Gateway, so Gateway1 should be deleted (after the new gateway is connected).
https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology#step-5-transition-connectivity-to-virtual-wan-hub

Valid AZ-700 Dumps shared by ExamDiscuss.com for Helping Passing AZ-700 Exam! ExamDiscuss.com now offer the **newest AZ-700 exam dumps**, the ExamDiscuss.com AZ-700 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com AZ-700 dumps with Test Engine here: https://www.examdiscuss.com/Microsoft/exam/AZ-700/premium/ (**335** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)