Microsoft.AZ-700-KR.v2026-08-22.q200

□□□□:	AZ-700-KR
□□□□:	Designing and Implementing Microsoft Azure Networking Solutions (AZ-700 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	200
□□:	v2026-08-22
# □□ □:	230
# □□ □□□:	2000
https://www.krdump.com/Microsoft.AZ-700-KR.v2026-08-22.q200.html	

NEW QUESTION: 1
□□□ □ □□ □□
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.
VNet1□ VNet2□ □□ □□□□□ □□□□. Subnet1□□ VM1□ □□□□ □□□□.

Name	Type	Description
VNet1	Virtual network	Has an IP address space of 10.0.0.0/20 that contains two subnets named Subnet11 and Subnet12
Subnet1	Virtual network subnet	Has an IP address range of 10.0.1.0/24
Subnet2	Virtual network subnet	Has an IP address range of 10.0.2.0/24
VNet2	Virtual network	Has an IP address space of 172.16.0.0/20 that contains one subnet named Subnet21
Subnet21	Virtual network subnet	Has an IP address range of 172.16.0.0/24
VM1	Virtual machine	Hosts a legacy app named App1 that is hardcoded to use an IP address of 10.0.1.4

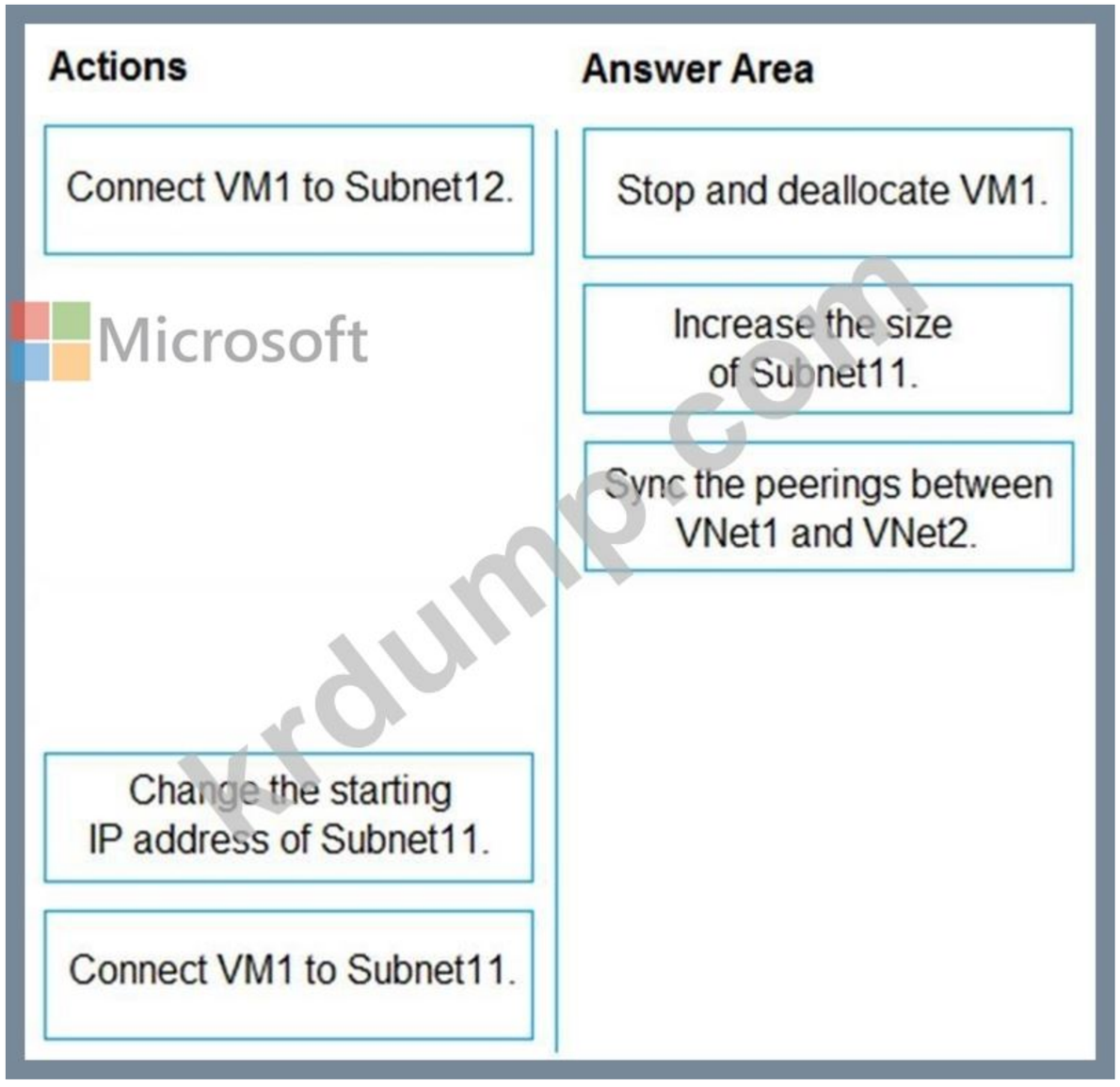
□□□11□ 500□□ IP □□□ □□□□□ □□□□ □□□. □□□□ □□ □□□□ VNet1□ VNet2 □□ □□□□□ □□□□ App1□ □□□□ □ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.

Actions

- Connect VM1 to Subnet12.
- Increase the size of Subnet11.
- Sync the peerings between VNet1 and VNet2.
- Stop and deallocate VM1.
- Change the starting IP address of Subnet11.
- Connect VM1 to Subnet11.

Answer Area

Answer:



NEW QUESTION: 2

□□ □□□ Azure Traffic Manager □□□□ □□ □□□□.

Name	Routing method
Profile1	Performance
Profile2	Multivalue

□□ □□ □□□ □□□□□□ □□□ □□□□□.

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

Profile2□ □□ □□□□□□ □□□ □ □□□?

A. Endpoint1 □ Endpoint4□

B. Endpoint1, Endpoint2, Endpoint3 □ Endpoint4

C. Endpoint1□

D. Endpoint2 □ Endpoint3□

E. Endpoint3□

Answer: E (LEAVE A REPLY)

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: 3

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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*

HP1 □□□□ https://app1.contoso.com URL□ □□□□ App1□ □□□□□.

FW1□ IDPS□ HP1□□ Server1□□ □□□□ □□ □□□ □□□ □ □□□ □□□□ □□□.

□□ □ □□ □□□ □□ □□□? □ □□□ □□□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

A. FW1□ □□ TLS □□□ □□□□□□.

B. □□ □□□□ KV1□□ □□□□□.

C. FW1□ □□ □□ □□□□□□ □□□□□□.

D. HP1□ □□□□□□ □□□ □□□□□.

E. FW1□ □□ □□ □□□□□ □□□□□.

Answer: A,B (LEAVE A REPLY)

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: 4
□□□ □□
□□□ Azure □□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	Connected to
VM1	Vnet1/Subnet1
VM2	Vnet1/Subnet2

Subnet1□ Subnet2□ □□□ □□ □□□□□ □□□ □□ NSG1□□□ □□□□ □□ □□(NSG)□ □□□□ □□□□.
□□□□: 100
□□: □□ □□
□□□□: Any
□□: Any
□□□: □□□
□□: □□
□□□ □□ □□□ □□ □□□ □□□□□□ □□□□□.
□□: Private1
□□□ □□: Microsoft.Storage/storageAccounts
□□□: storage1
□□ □□ □□□: blob
□□ □□□□: Vnet1
□□□: □□□1
□□ □ □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:
Service Tag "storage" represents Azure Storage Accounts and can only be applied on the Outbound direction.
Here the NSG is denying the access to any Storage account (direction is Outbound, read well) and it is applied on the Subnet level not on the NIC level.
Box 1: No
VM2 being on the subnet 2 not on subnet 1 will be deny.
Box 2: Yes
VM1 and Private 1 are in the same subnet so VM1 will have access.
Box 3: No

VM2 has been denied the access by the NSG

NEW QUESTION: 5
□□ □□ □□□ Azure □□ □□□□□ □□□□.

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

Azure Firewall□ Vnet3□ □□□□□.
□□□1-1□□ □□□2-1□ □□ □□□□ □□□□ □□□□□ □□ □□□.
□□□ □□□□ □□□?
A. Vnet1□ Vnet2 □□ □□□ □□
B. □□□1-1 □ □□□2-1□ □□□ □□□ □□□
C. Azure □□□□ DNS □□
D. AzureFirewallSubnet□ □□□ □□□ □□□
Answer: B (LEAVE A REPLY)
1. You have to create a route table first
2. Next you create the route in the table like this
Route name: toFW
Destination type: IP Addresses
Destination IP addresses/CIDR ranges: 0.0.0.0/0
Next hop type: Virtual appliance
Next hop address: Firewall IP
3. Go to Subnets
Select the Vnet
Associate Subnet1-1 and Subnet2-1
https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route

NEW QUESTION: 6
Azure □□ □□□□□ □□□□ □□ IP □□ □□□ □□□□ □□□□.
□□□□□ IP □□□ □□□ □□□ □□□ □□□□□?
A. □□□ □□□□□ □□
B. Azure □□ □□□□ NAT
C. □□ □□ □□□
D. □□ □□□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 7
□□□ □□

Network1□ Network2□□ □ □□ □□□□□ □□□□□ □□□□. Network1□□ 10.0.0.0/23 IP □□ □□□ □□□□ □□, Network2□□ 10.10.0.0/24 IP □□ □□□ □□□□ □□□□. □ □□□□□ □□□□□□ □□ □ □ VPN □□□ □□□□ □□□□.

Azure □□□□ VNet1□ VNet2□□ □ □□ □□ □□□□□ □□□□ □□□□.

VNet1□□ 192.168.0.0/22 IP □□ □□□ □□□□□□□. VNet2□□ 172.16.0.0/24 IP □□ □□□ □□□□□□□. VNet1□ VNet2□ □□□□□□.

□□ □□ □□□ □□□□□ □□□ □□□□ □□□.

- Network1□□ VNet1 □ VNet2□ □□□ □□□□ □ □□□ □□□.
- Network2□□ VNet1 □ VNet2□ □□□ □□□□ □ □□□ □□□.
- □□□ □□□ □□□□□□.
- □□□ □□□□□□□.

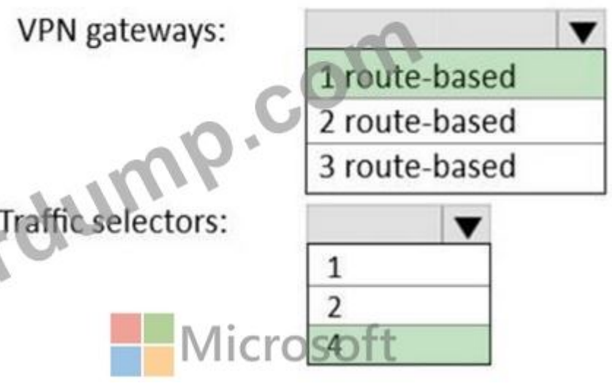
Azure VPN □□□□□ □ □□□ □□□□ □□ □□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area



NEW QUESTION: 8

□□ □□ 2 - □□□ □□□□

□□

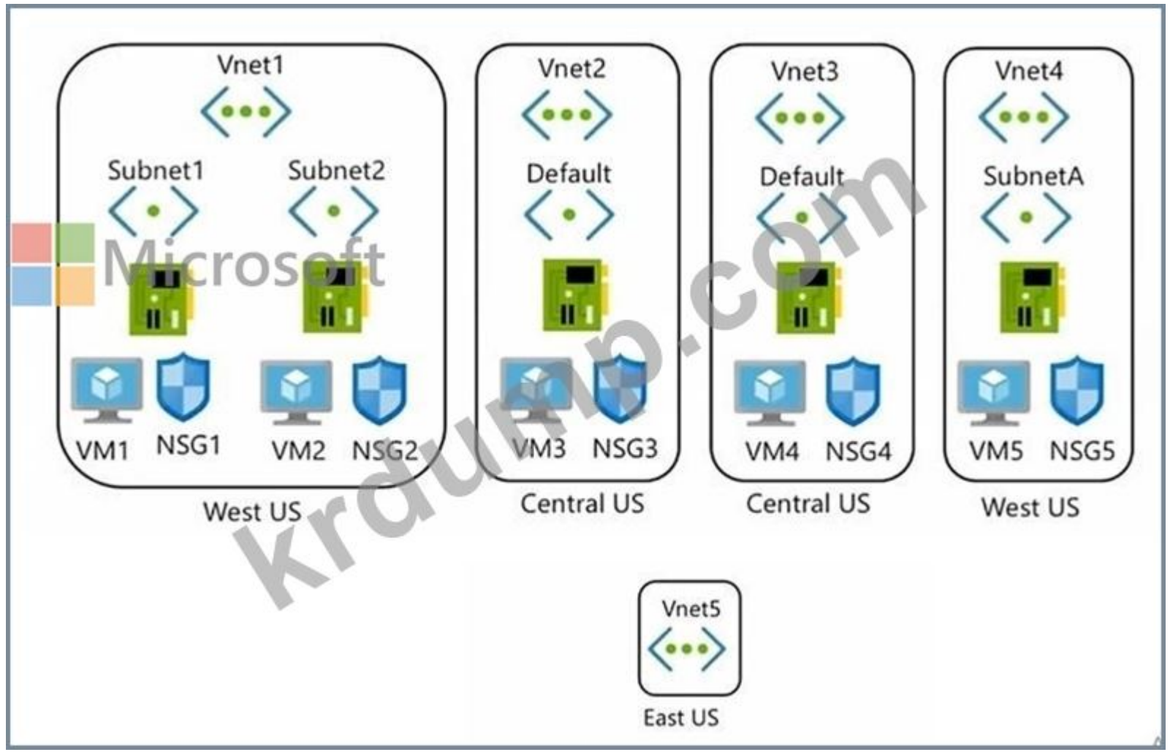
□□□ □□□□□ □□□□□□□ □□□ □□ □□□□ □□□ □ □□□ □□□□□.
Contoso□ □□ Azure □□□ □□□□□ Azure□□ □ □□ □□ □□□□□ □□□□ □□□□.
□□ □□:
Azure □□□□ □□□
Contoso□ contoso.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. □□ Azure □□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

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□□ GW1□□□ □□□ □□ □□□□ □□□□□□ □□□□ □□□□.
Azure □□ □□
Azure □□□□ □□ □□ □□□ □□□ Windows Server 2019□ □□□□ □□ □□□ □□□□ □□□□.

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

NSG(□□□□ □□ □□)□ □□ □□□ □□□□ □□□□□□ □□□□ □□□□. □ NSG□□ □□□□□ RDP □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□□. □ □□ □□□ □□□□ ICMP □□□□ □□□□ □.
ASG1□□□ □□□□□□ □□ □□□ VM1□ □□□□ □□□□□□ □□□□ □□□□.
Azure □□□□ □□□ □□□□□



Azure □□□□ DNS □□

Azure □□□□ □□ □□ □□□ Azure □□□□ DNS □□□ □□□□ □□□□.

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

Zone1.contoso.com□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

□□ Azure □□□

Azure □□□□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.

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

□□ □□:

□□ □□□□ □□ □□
Contoso□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□.
- □□ □□ □□□ Vnet6□□□ □□□ □□ □□□□□ □□□□, □□ □□□□□ □□ □□□□ □□□ □□□□□□□.
Vnet6□ □□□□ □ □□ □□□□ □□
Vnet6□ □□□ □ □□ □□ □□
Vnet6□ □□ VPN □□ □□□ □□□□□.
Vnet6□ □□□□ KeyVault1, DB1 □ Vnet1□ □□□□ □ □□□ □□□□□.
□□□□□□□ □□ □□□□
- Vnet4□ Vnet5□ □□ □□□□ □□ □□□ □ □□□ □□□.
□□□□□□□ □□ □□□□□ □□.
- VM-Analyze□□ □□□ □□ □□□ Subnet1□ □□□□□. VM-
Analyze□ Subnet2□□ □□□ □□□□ □□□□ □□□□ □□□.
□□□.
□□□□ □□ □□ □□
Contoso□ □□□ □□ □□□□ □□ □□ □□□ □□□ □□□□.
- P2S(Point-to-Site) VPN □□□□ □□ Azure Active Directory(Azure AD) □□□ □□□□□.
- NSG3 □ NSG4□ □□ NSG □□ □□□ □□□□□□.
- Vnet1/Subnet1□ □□□ NSG10□□□ □□□ NSG□ □□□□□.
□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.
□□□.

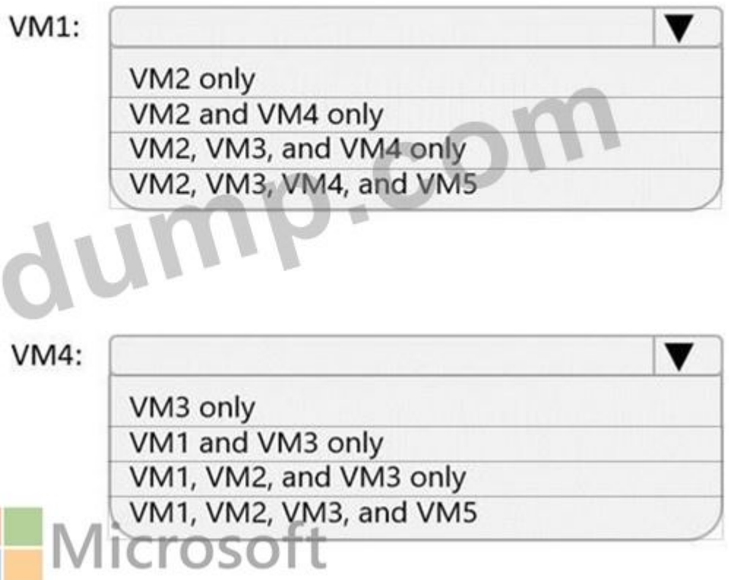
Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

- Vnet1/Subnet2□ □□□ NSG11□□□ □□□ NSG□ □□□□□.
□□□ □□ □□ □□□ □□□ □□ □□□□□ □□ □□□ □□□□□.

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

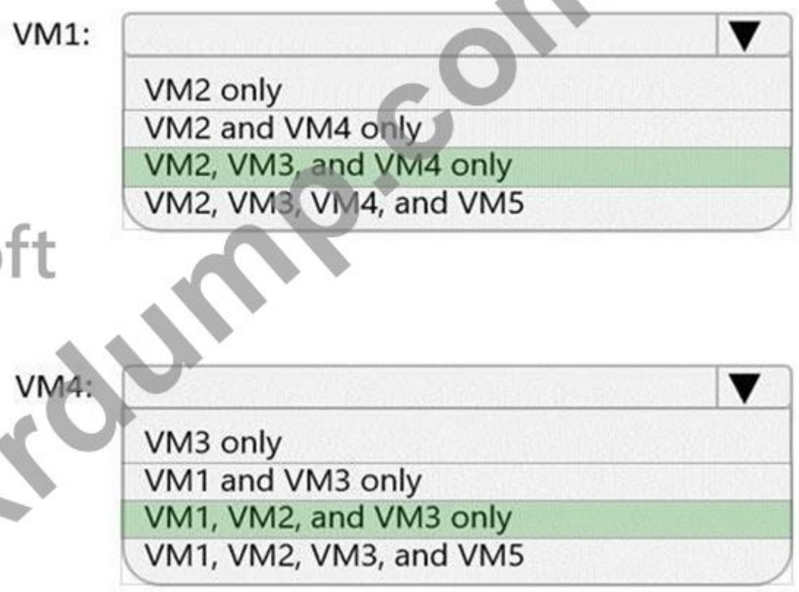
□□□ □□
VM1□ VM4□ □□ □□ □□□ □□□□□ ping□ □□ □ □□□□? □□□ □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



Explanation:
Box 1: VM2, VM3 and VM4.
VM1 is in VNet1/Subnet1. VNet1 is peered with VNet2 and VNet3. There are no NSGs blocking outbound ICMP from VNet1. There are no NSGs blocking inbound ICMP to VNet1/Subnet2, VNet2 or VNet3. Therefore, VM1 can ping VM2 in VNet1/Subnet2, VM3 in VNet2 and VM4 in VNet3.
Box 2:
VM4 is in VNet3. VNet3 is peered with VNet1 and VNet2. There are no NSGs blocking outbound ICMP from VNet3. There are no NSGs blocking inbound ICMP to VNet1/Subnet1, VNet1/Subnet2 or VNet2 from VNet3 (NSG10 blocks inbound ICMP from VNet4 but not from VNet3). Therefore, VM4 can ping VM1 in VNet1/Subnet1, VM2 in VNet1/Subnet2 and VM3 in VNet2.

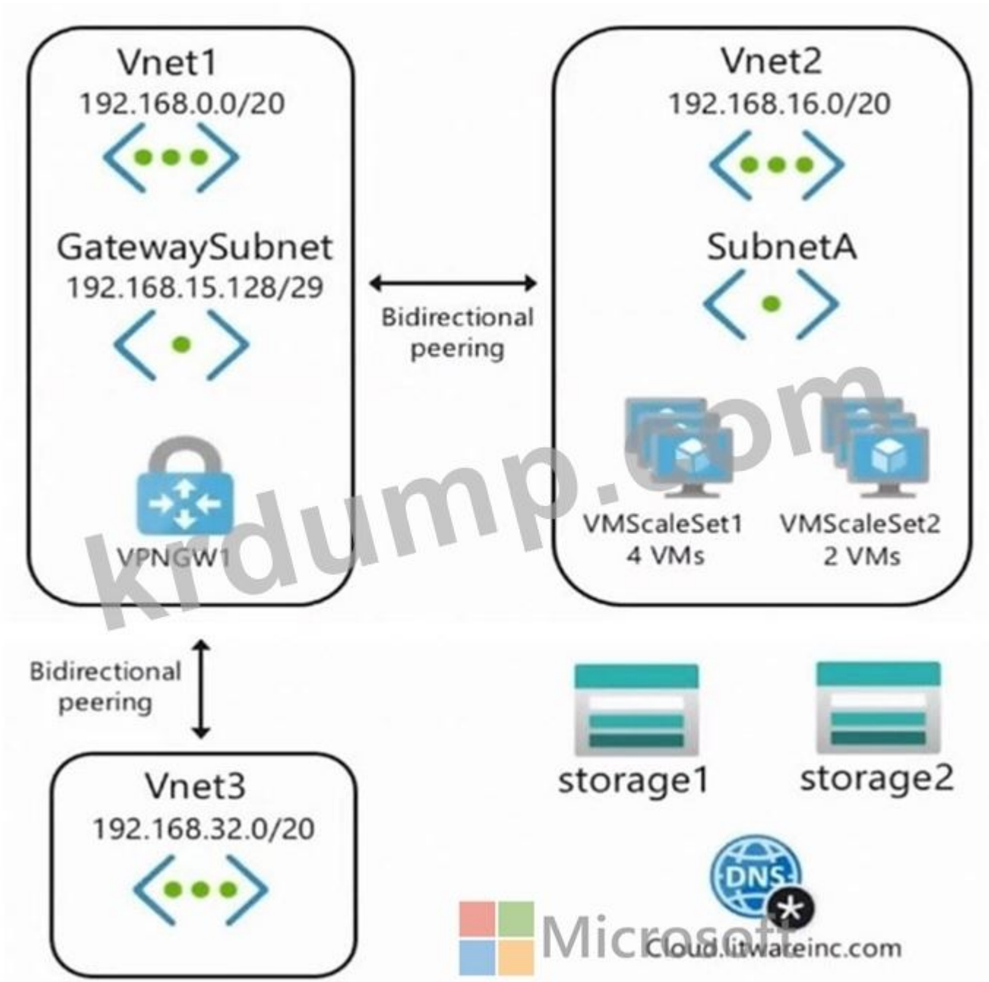
NEW QUESTION: 9
Azure □□ □□□□□ □□□ □□□□□.
□□□□ □□□□ □□□.
□□ □□□□ □□□ □ □□ □□□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. VPN □□□□□
B. Azure □□
C. Azure Active Directory □□□ □□□(Azure AD DS)

D. Azure □□□□□□ □□□□□ v2
E. Azure □□ □□
Answer: (SHOW ANSWER)
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: 10
□□ □□ 1 - Litware. Inc.
□□
Litware Inc.□ □□□□ □□ □□□□□□ □□ □□ □□□ 20□□ □□□ □□□ □□ □□□□□. □□□□□ □□□□□, iOS □ □□□ 10 □□□ □□□□□.
□□ □□:
□□□□□ □□
□□□□□ □□□□□□ litwareinc.com□□□ □□□ Active Directory □□□□□ □□□, Azure AD Connect□ □□□□ litwareinc.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□□□.
□□ □□□□ □□□ □ VPN □□□ □□□□ Vnetl□□□ □□ □□□□□ □□□□□.
Azure □□
Litware□ litwareinc.com Azure AD □□□□ □□□ Sub1□□□ Azure □□□ □□□□ □□□□. Sub1□□ □□ □□ □□□ □□□ □□ □□ Azure □□□ □□□□ □□□□ □□□□.

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

□□ □□ Azure □□□ □□□ □□□□□□ □□□□ □□□□□□ □□ □□□□.
Vnet1□ Vnet2 □□□□ □□□ □□□□ □□□□ □□□□. Vnet1□ Vnet3 □□□□ □□□ □□□□ □□□□ □□□□. □□ Vnet2□ Vnet3□ □□ □□□ □ □□□□.
Azure □□ □□□□□



□□ □□:

□□□□ □□□□

Litware□ □□ □□ □□ □□□ □□□□ □, □□□ □ □□□ □□□□□□ □□□.

□□ □□□□ □□ □□

Litware□ □□□ □□ □□ □□□□ □□ □□□ □□□□□.

- Vnet2 □ Vnet3□ □□ □□□ 0.0.0.0/0□ □□□□ □□□□□.

ExpressRoute □□□ □□ □□□ □□□□□□ □□□□□.

- cloud.litwareinc.com □□□ □□□□ □□□ □□□□□ □□□□□□.

□□□□□ □□□□ □□□□□□□.

- Azure □□ □□□ DNS □□□ cloud.litwareinc.com □□□ □□□□ □□□□□.
- □□□ □□ □□□ □□□□ □□□□ □□□ □□□□□□.

□□□.

- VMScaleSet1□□ VMScaleSet2□□ TCP □□ 443□ □□ □□□□ □□□□□.

□□.
□□□□□ □□□□ □□ □□
Litware□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□□.
- □□□□ □□□□ □□□ □ P2S(Point-to-Site) VPN□ □□□□ Vnet1□ □□□ □ □□□ □□□. □□□ Azure AD□ □□ □□□□□ □□□.
- □□□ □□□□□□ □□ □□ □ □□□ □□ □□
□□ □□□□□ □□□□□ □□□.
- □□□ □□□□□□ Azure □□ □□□□□ □□□□ □□□.
ExpressRoute FastPath □□□ □□□□□.
- Vnet2□ Vnet3 □□ □□□□ Vnet1□ □□ □□□□□□ □□□.
PaaS □□□□ □□ □□
Litware□ □□□□ □□□(PaaS)□ □□□ □□□□ □□ □□□ □□□ □□ □□□□□.
- storage1 □□□ □□□□□□ □□ □□□ □□ □□□□ □□□.
storage1□ □□ □□□□□□ □□□□ □□ □□□ □□□ □ □□□□.
- storage2 □□□ Vnet2 □ Vnet3□□ □□ □□□□ □□□.
storage2□ □□ □□□□□□ □□□□□.
Vnet2□ Vnet3□ □□ □□□ □□□□ □□□. □□□□ □□ □□□□ □□ □□□ □□□□ □□□.
□□ □□□ □□□□□ □□□ □□□□ □□□?
A. Vnet2 □ Vnet3□ GatewaySubnet□ □□□ □□□ □□ □□
B. Vnet1□ GatewaySubnet□ □□□ □□□ □□ □□
C. BGP □□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
You must use BGP to advertise on-premises routes to the Microsoft Edge router. You cannot create user-defined routes to force traffic to the ExpressRoute virtual network gateway if you deploy a virtual network gateway deployed as type: ExpressRoute Source: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr- overview#border-gateway-protocol

NEW QUESTION: 11
Subnet1□ Subnet2□□ □ □□ □□□□ □□□ Azure □□ □□□□□ □□□□.
□□□ 1□□ VM1□□□ □□ □□□ □□□□. □□□ 2□□ VM2□□ □□ □□□ □□□□.
NSG1□ NSG2□□ □ □□ □□□□ □□ □□(NSG)□ □□□□. NSG1□□ 100□□ □□□□ □□ □□□ □□□ VM1□ □□□□ □□□□. NSG2□□ 200□□ □□□□ □□ □□□ □□□ Subnet1□ □□□□ □□□□.
VM2□ VM1□ □□□ □ □□□□.
NSG □□□ □□□ □□□□□ □□□□□.
□□ □□□ □□□ □□□□□ □□□□ □□□. □□□ □□□ □□ □□□□ □□□.
□□ Azure Network Watcher □□□ □□□□ □□□?
A. □□□□ □□ □□
B. NSG □□ □□
C. □□ □□ □□
D. NSG □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.

Azure WAF(□ □□□□□□ □□□)□ □□□□ Azure □□□□□□ □□□□□□ □□□□.

□□□□□□ □□□□□□ □□□□□□ □□□□□□ URL□ □□□□ □□□□□ □□□□□□.

□□□□□□ □□□□□□ □□ URL□ □□□ □ □□□ □□□□ □□□.

□□ □□: ruleId□ 920300□ WAF □□□ □□□□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: B (LEAVE A REPLY)

NEW QUESTION: 13

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□ □ □□□□.

□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.

Azure □□□ VWAN1□□□ □□□ Azure □□ WAN□ □□□□. VWAN1□□ Hub1□□□ □□□ □□□ □□□□.

Hub1□ □□ □□□ '□□□□ □□'□□□.

Hub1□ □□ □□□ '□□□'□□ □□□□ □□□ □□□□ □□□.

□□ □□: Azure Firewall□ □□□□□.

□□□ □□ □□□ □□□□□?
A. □□□
B. □
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
Azure PowerShell□ □□□□ □□ □□□ □□□ □□ □□□ □□□ □□□□□. □□□ □□□ □□□ □□□□□ □□ □□□ □□□□ □□□ □□□□□. □□□□ □□□ Azure PowerShell □□□ □□□□□ □□ cmdlet □ □□ □□ □□□□ □□□?
A. Get-Module -ListAvailable Az
B. Get-Module -AzList
C. Retrieve-Module -ListAvailable Az
D. Retrieve-Module -AzList
Answer: A (LEAVE A REPLY)
PowerShell cmdlets are updated regularly; if you have not installed the latest version or used the earlier versions, the values defined in the instructions might fail. You can run Get-Module - ListAvailable Az cmdlet to know the version of Azure PowerShell installed on your computer.
Option A is correct. Get-Module -ListAvailable Az is the right cmdlet to be used to know the version of Azure PowerShell installed on the system.
Option B is incorrect. Get-Module-AzList is not the right cmdlet.
Option C is incorrect. There is no command like Retrieve-Module -ListAvailable Az.
Option D is incorrect. There is no such cmdlet in Azure PowerShell.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/diagnose-network-routing-problem?WT.mc_id=modinfra-33046-thmaure
https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-how-to-radius-ps?WT.mc_id=modinfra-33046-thmaure

NEW QUESTION: 15
□□□□□


□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678
□□□ □□ Azure □□□ Azure □□ □□□ □□□ □ □□□ □□□□ □□□. □□□□ □□□ □□ □□□ □□ □□□ IP □□ □□□ 10.5.1.0/24□ □□□□ □□□□□ □□□ □□□□ □□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.
Answer:

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

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

Network interfaces
IP addresses
Virtual network and subnets

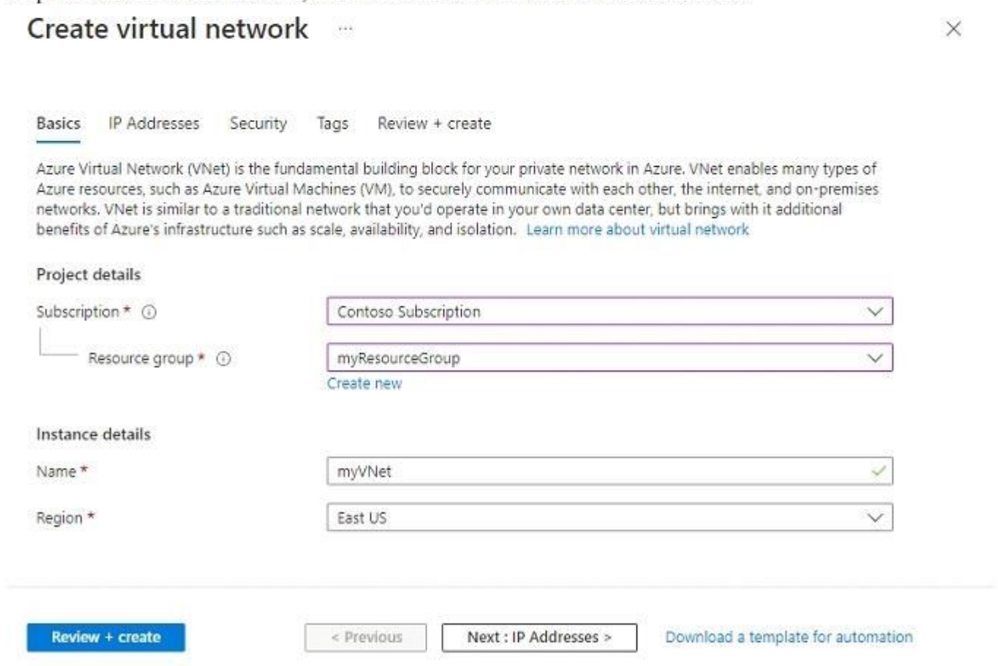
Create a virtual network

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

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

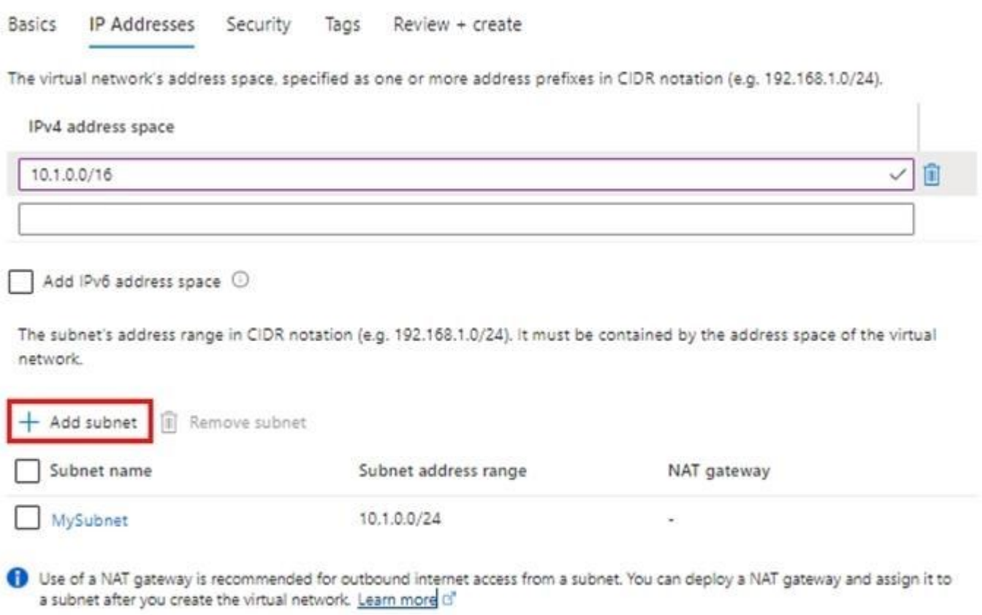
Step 3: In the Virtual Network page, select Create.

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



Step 5: Enter Region: `France Central`

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



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

Step 8: Click Add subnet

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

Step 10: Finish the wizard.

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

NEW QUESTION: 16

□□□ □□

Sub1□□□ Azure □□□ □□□, □ □□□ Tenant1□□□ Microsoft Enterprise □□□□ □□□□ □□□□. Sub1□□ VNetGW1□□□ Azure VPN □□□□□□ □□□□ □□□□.

□□□1□ Azure VPN □□□□□□ □□□□ □□□□□.

VNetGW1□ □□□□ P2S(Point-to-Site) VPN □□□ □□ Microsoft Entra □□□ □□□□ □□□. □□□□ □□□□ Azure VPN □□□□□□ □□□□ P2S VPN □□□ □□□ □ □□□ □□□□ □□□.

VNetGW1□ □□ □ □□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□?

□□□□□ □□□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Tenant:
- https://graph.microsoft.com/<Tenant1-GUID>
- https://login.microsoft.com/<Tenant1-GUID>
- https://sts.windows.net/<Tenant1-GUID>

Issuer:
- https://graph.microsoft.com/<Tenant1-GUID>
- https://login.microsoft.com/<Tenant1-GUID>
- https://sts.windows.net/<Tenant1-GUID>

Answer:

Answer Area

Tenant:
- https://graph.microsoft.com/<Tenant1-GUID>
- https://login.microsoft.com/<Tenant1-GUID>
- https://sts.windows.net/<Tenant1-GUID>

Issuer:
- https://graph.microsoft.com/<Tenant1-GUID>
- https://login.microsoft.com/<Tenant1-GUID>
- https://sts.windows.net/<Tenant1-GUID>

NEW QUESTION: 17

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.

- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx

Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

- □ □□□□: 12345678

VNET1□ □□ □□□□ □□ □□□□ □□□ □□□□□□ □□□.

□ □□□ □□□□□ Azure □□□ □□□□□□.

Answer:

Monitoring Azure virtual network
Azure virtual network uses Azure Monitor.

Data platform
Azure Monitor stores data in data stores for each of the pillars of observability: metrics, logs, distributed traces, and changes. Each store is optimized for specific types of data and monitoring scenarios.

Retention of metrics
You can send platform metrics for Azure Monitor resources to a Log Analytics workspace for long-term trending.

Send to Azure Storage
Send resource logs to Azure Storage to retain them for archiving. After you've created the diagnostic setting, a storage container is created in the storage account as soon as an event occurs in one of the enabled log categories.

Create a diagnostic setting to send resource logs to a Log Analytics workspace or to a Storage Account.

Archiving logs and metrics to a Storage account is useful for audit, static analysis, or backup. Compared to using Azure Monitor Logs or a Log Analytics workspace, Storage is less expensive, and logs can be kept there indefinitely.

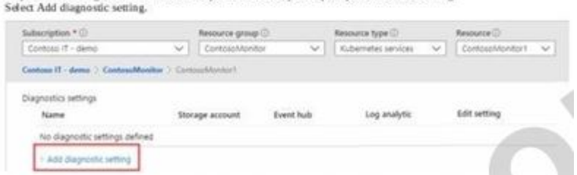
Create diagnostic settings

You can configure diagnostic settings in the Azure portal either from the Azure Monitor menu or from the menu for the resource.

Step 1: Select the Virtual Network VNET1.

Step 2: Select Diagnostic settings under Monitoring on the resource's menu.

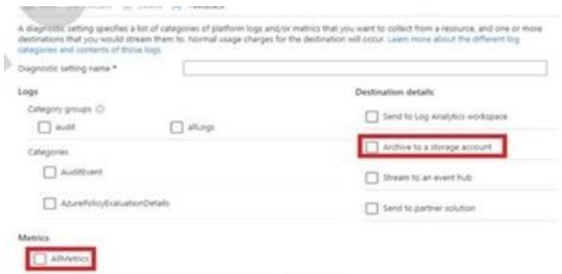
Step 3: If no settings exist on the resource you've selected, you're prompted to create a setting. Select Add diagnostic setting.



If there are existing settings on the resource, you see a list of settings already configured. Select Add diagnostic setting to add a new setting. Or select Edit setting to edit an existing one. Each setting can have no more than one of each of the destination types.

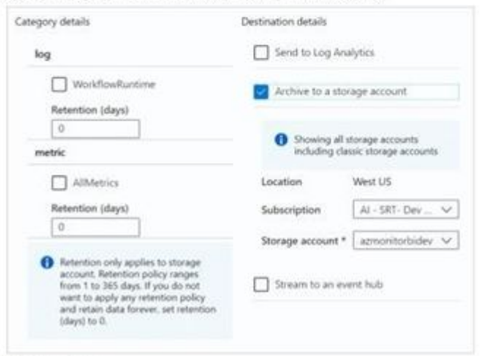
Step 4: Give your setting a name if it doesn't already have one.

Step 5: Logs and metrics to route: Select AllMetrics if you want to store metrics in Azure Monitor Logs too.



Step 6: Destination details. Select Archive to a storage account

Step 7: Storage: Select the Subscription, Storage account, and Retention policy.



Step 8: Select Save.

Reference

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-platform-metrics

NEW QUESTION: 18

□□□ □□□□□ □□□□□ □□□□ □□□□.

VNet1□□□ □□ □□□□□ AKS1□□□ □□□□ Azure Kubernetes Service(AKS) □□□□□ □□□ Azure □□□ □□□□. VNet1□ Azure ExpressRoute □□□ □□ □□□□□ □□□ □□□□ □□□□. AKS1□ VNet1 □ □□□□ □□□□.

AKS1□ □□ □□□□ □□□□ □□□□□ □□□□ □□□. □ □□□□ □□□□□ □□□□ AKS1□□ □□□□□ □□□□□□ □□□□□□ □□□ □□□□ □□□.

□□ Azure □□□□ □□□□ □□□?

A. Azure Application Gateway

B. □□□ □□□

C. Azure Traffic Manager

D. Azure □□ □□□

Answer: A (LEAVE A REPLY)

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: 19

□□□□ □+□□□□ □□□□□ Subscription1, Subscription2, Subscription3□□□ □ □□ Azure □□□ □□□□.

□□ □□ □□□ □□ □□□ □□□□□ Azure □□□ □□□□□.

Department	Subscription
IT	Subscription1
Research	Subscription1
Development	Subscription2
Testing	Subscription2
Distribution	Subscription3

□□□ □□ □□□□ □□ □□ Azure □□ □□ □□ □□ 2 Azure □□□ □□□□.
ExpressRoute□ □□□□ □□ □□□ □□□□□ □□□□□ □□□ □□□□□.
ExpressRoute □□□ □□ □□□ □□□□□?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: (SHOW ANSWER)

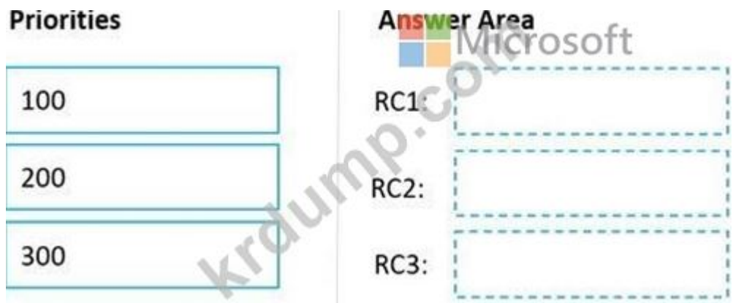
Managing Authorization
https://azure.microsoft.com/en-us/blog/enable-multiple-subscription-expressroute/#:~:text=The%20circuit%20owner%20can%20share,the%20authorization%20at%20any%20time.
The circuit owner can share a circuit with up to 10 Azure subscriptions. The circuit owner can view who has been authorized to the circuit. The owner can revoke the authorization at any time.

NEW QUESTION: 20

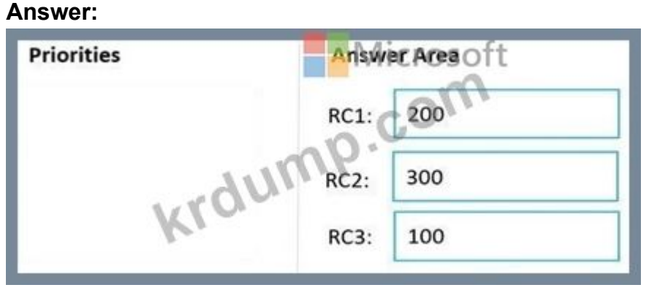
□□□ □ □□ □□: FWP1□□□ □□□ Azure Firewall Premium □□□ □□□ Azure □□□ □□□□.
FWP1□ □□ □□ □□□ □□ □□□ □□□ □□□□□.

Name	Type
RC1	Network
RC2	Application
RC3	DNAT

□ □□ □□□ □□ □□□□□ □□□□ □□□? □□□ □□□□ □□□ □□□□ □□ □□ □□ □□□□ □□□□□□. □ □□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□.
□□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □ □□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

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

NEW QUESTION: 21

□□□ □□

AppGW1□□□ Azure □□□□□□ □□□□□□ □□□, □ □□□□□□ □□ □□□□ □□ □□□□ □□□□□.

- www.adatum.com
- www.contoso.com
- www.fabrikam.com

AppGW1□□ □□ □□ □□□ □□□□ □□□□.

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

□□ □□ □□□ □□ AppGW1□ □□ Azure □ □□□□□□ □□□(WAF) □□□ □□□□□.

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

□□ □ □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

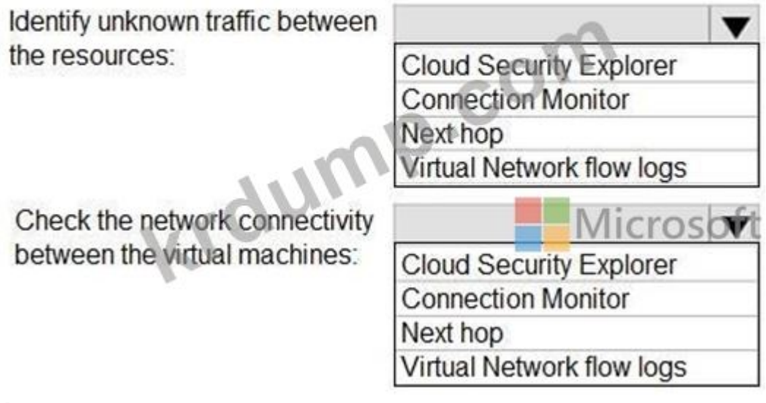
Answer:

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

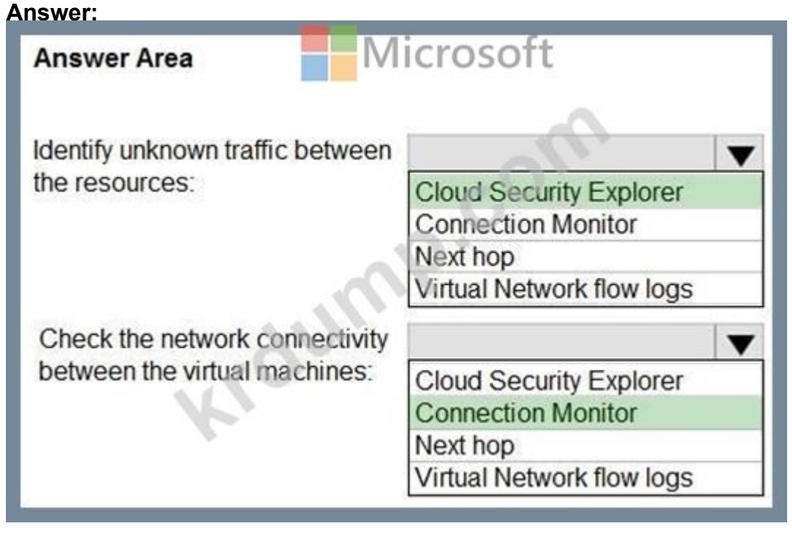
NEW QUESTION: 22
□□□ □□

□□ □□□□, □□□□ □□ □□(NSG) □ □□ □□□ □□□ Azure □□□ □□□□.
□□ □□□ □□□□ □□□.
- □□□ □□ □ □ □□ □□□□ □□□□□.
- □□ □□ □□ □□□□ □□ □□□ □□□□□□.
□ □□□ □□□□□ □□□ □□□□ □□□? □□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

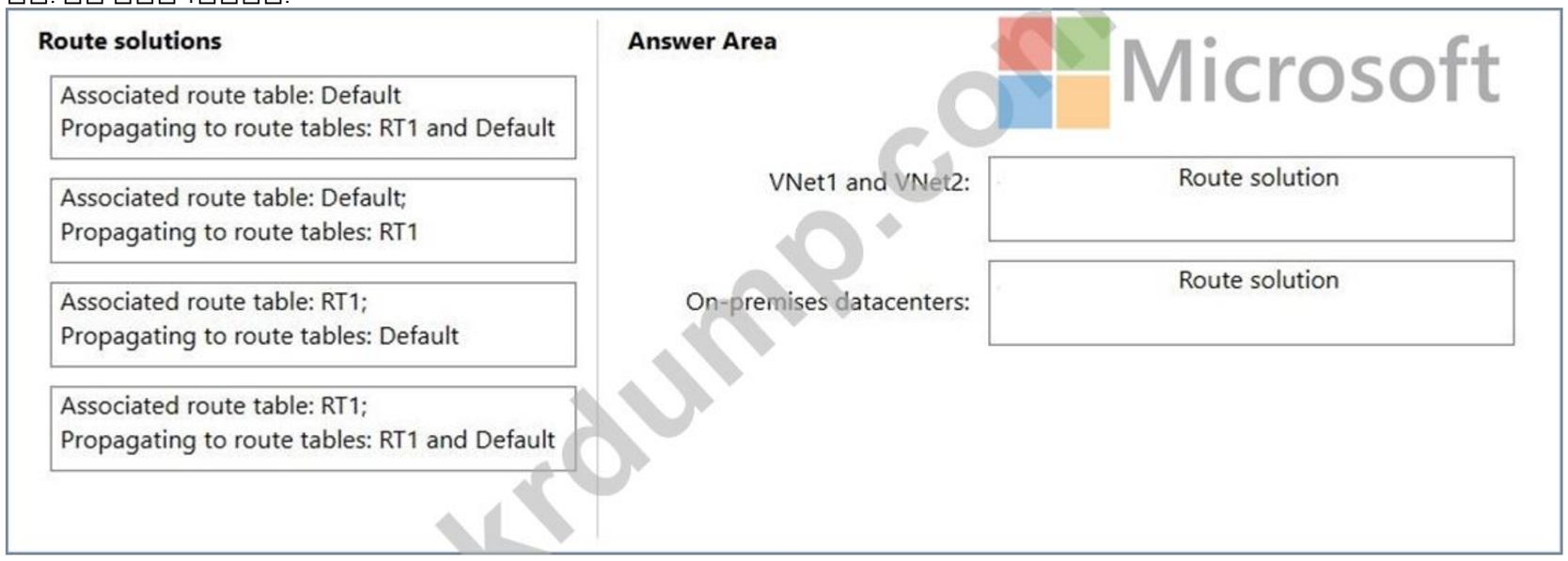


Answer:



NEW QUESTION: 23
□□□ □ □□ □□
□□□ □□□□□ □□□□□□ □ □ □□□□ □□□□.
VNet1, VNet2, VNet3, VNet4□□ □□□ □□ □□□□ 4□□ □□□ Azure □□□ □□□□.
VWAN1□□□ □□□ Azure □□ WAN□ □□□□□. VWAN1□□ □□□□□ □□□ □□□ □□ □□ □□□□□ □□□ □□ □□ □□□ □□□□ □□□, □ □□□ □ □□ □□□□□ □□□□□.

RT1□□□ □□□ □□□ □□□□ □□□□□.
VWAN1□ □□ □□ □□□ □□ □□□□ □□□.
- VNet1□ VNet2, □□□ □ □□□□□ □□□□□ □□ □□□ □□□□□ □□□.
- VNet3□ VNet4, □□□ □ □□□□□ □□□□□ □□ □□□ □□□□□ □□□.
- VNet1□ VNet2□ VNet3 □ VNet4□ □□□□□ □□□.
VNet1□ VNet2, □□□ □ □□□□□ □□□□□ □□□ □□ □□□□ □□□ □□□□ □□□?
□□□ □□□□□ □□□ □□□ □□□□ □□□ □□□ □□ □□□ □□ □□ □□□□ □□□□□□□. □ □□□ □□□□ □□□ □□□ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □ □□□□.
□□: □□ □□□ 1□□□□.



Answer:

Route solutions

Associated route table: Default;
Propagating to route tables: RT1

Associated route table: RT1;
Propagating to route tables: RT1 and Default

Answer Area

VNet1 and VNet2: Associated route table: RT1;
Propagating to route tables: Default

On-premises datacenters: Associated route table: Default
Propagating to route tables: RT1 and Default

NEW QUESTION: 24
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type	Description
Vnet1	Virtual network	In the US East Azure region
LB1	Load balancer	Basic SKU
VM1	Virtual machine	Connected to Vnet1 Member of the backend pool of LB1
VM2	Virtual machine	Connected to Vnet1 Member of the backend pool of LB1

□□ □□ □□□ Vnet2□□ □□□ □□ □□□□□ □□□□□.
Vnet1□ Vnet2 □□ □□□□ □□□□ □□□□□.
Vnet2□ □□□ □□ □□□ LB1□ □□ VM1 □ VM2□ □□□ □ □□□ □□□□ □□□.
□□□ □□ □□□?
A. Vnet2□ □□□ □□□□ □□ □□ □□□□□□ □□□□ □□□□ □□□□ □□□□□.
B. LB1□ □□□ IP □□□ □□□□□.
C. Vnet1□ □□□ □□□□ □□ □□ □□□□□□ □□□□ □□□□ □□□□ □□□□□.
D. LB1□ SKU□ □□□□□.
Answer: D (LEAVE A REPLY)
Global VNet Peering Support Standard ILB is supported via Global VNet Peering Not supported.
https://learn.microsoft.com/en-us/azure/load-balancer/skus#skus

NEW QUESTION: 25
Azure App Service □□ □□□ Azure □□□ □□□□. □□ □□ URL□ □□□□□.
https://www.contoso.com.
Azure Front Door□□ www.contoso.com□ □□□ □□ □□□□ □□□□ □□□. □□□ □□ □□□□ □□□ □□ □□(CA)□ □□□□ □□□□ □□□.
□□□□ □□□ □□□□ □□□?
A. Azure Active Directory(Azure AD)□ □□□□□□ □□□□□□
B. Active Directory □□□ □□□(AD CS)
C. Azure □ □□□
D. Azure □□□□□□ □□□□□
Answer: C (LEAVE A REPLY)
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

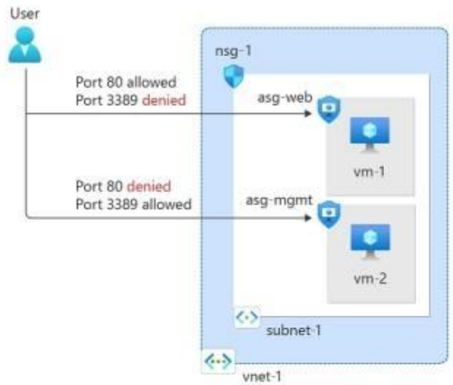
NEW QUESTION: 26
□□□□□


□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxx
Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678
□□□3-2□ □□□3-1□ □□□□□ □□□ □ □□□ □□ □□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.
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.

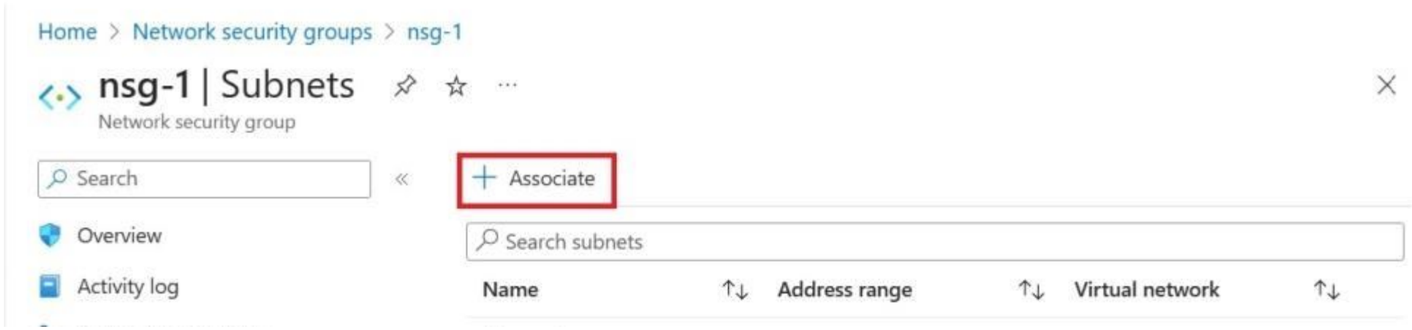
Stage 2
Associate network security group to subnet
In this section, you associate the network security group with the subnet of the virtual network you created earlier.

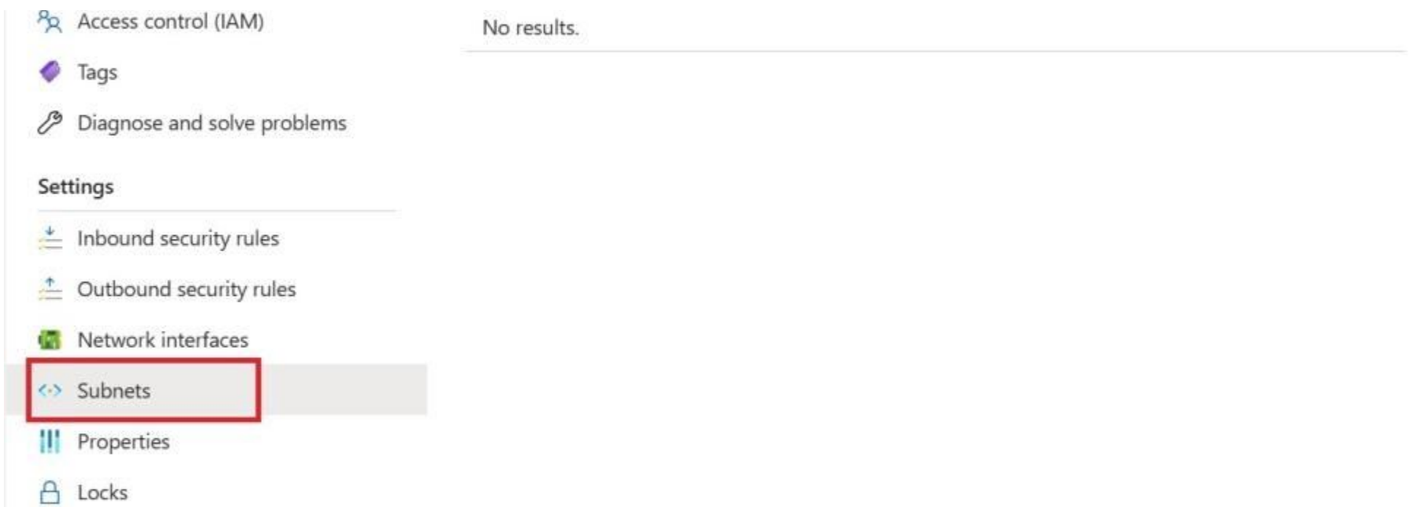
Step 1: In the search box at the top of the portal, enter Network security group. Select Network security groups in the search results.

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.

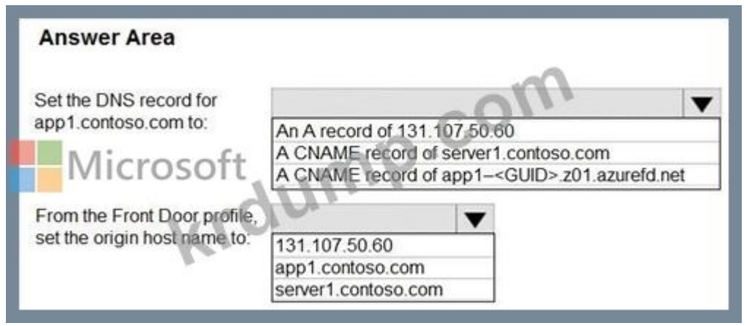
Step 2: In Outbound security rules page, select + Add.

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

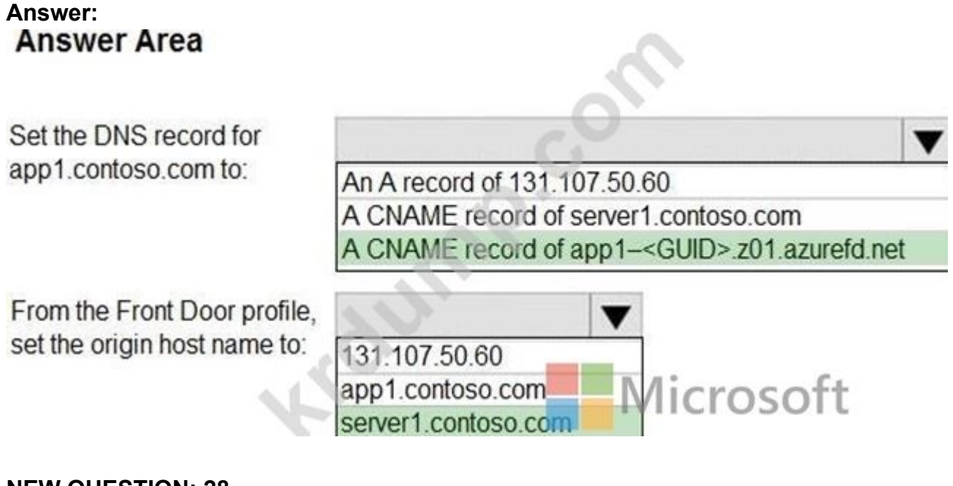
Step 4: Select Add.

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

NEW QUESTION: 27
□□□ □□
□□□□ App1□□□ □ □□□□□□□ □□□□□ □□□□□ □ □□□ □□□, □□ □□□ □□□ □□ □□□ □□□ □□□□.
- IP □□: 131.107.50.60
- FQDN: server1.contoso.com
Azure □□□ □□□□ □□□□.
Azure Front Door□ □□□□ App1□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□ □□□□ FQDN□ □□□□ App1□ □□□ □ □□□ □□□□.
app1.contoso.com.
- □□□ □□□ □□□ □□ □□□ □□□□□□□.
Server1□ Azure□ □□□□□□□□□□□.
□□□□ □□□ □□□□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 28

□□□ □ □□ □□

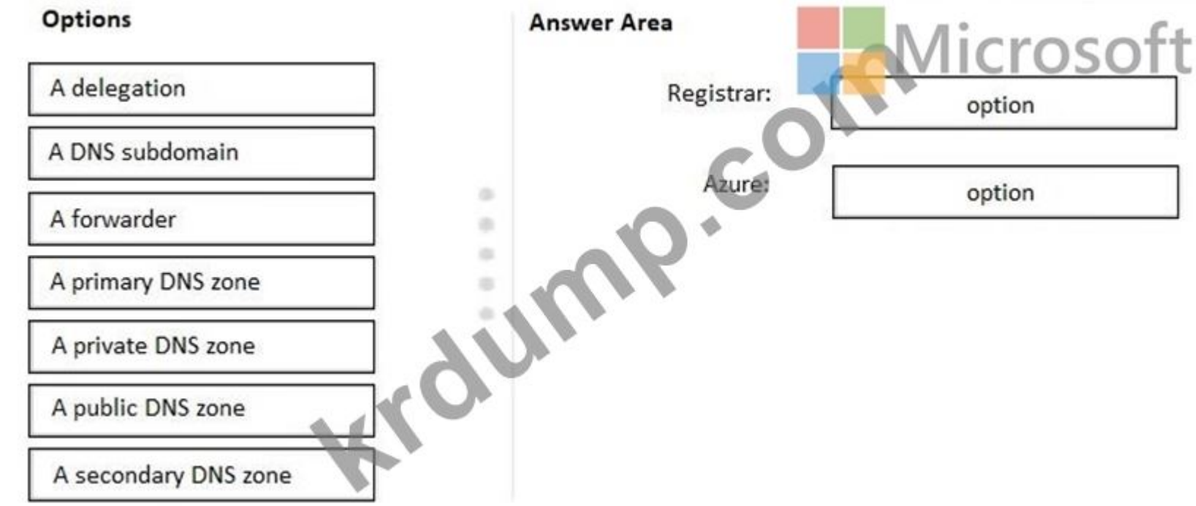
□□□ □□ □□□ □□ □□□□ □□□□□ contoso.com□□□ DNS □□□□ □□□□ □□□□.

contoso.com □□□□□ □□ □□ DNS □□□ Azure DNS□ □□□□ □□□□□ □□ □□□.

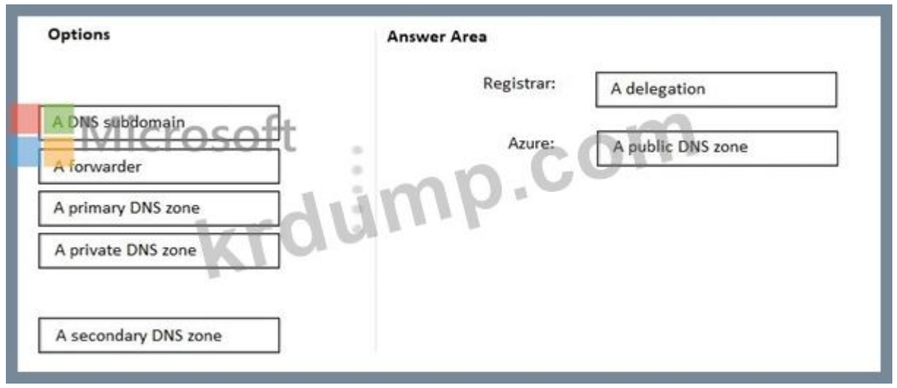
Azure □□□□ □□□□□ □□□□□.

□□□□□□ □□□ □□□□ □□, Azure□□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□ □□□□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □ □ □□□ □□□□□□ □□□□□ □ □□ □□□□.

□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 29

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type	Description
VNet1	Virtual network	Contains a subnet named Subnet1
storage1	Storage account	Located in the East US Azure region and geo-replicated to the paired region

Subnet1□ Policy1□□□ □□□ □□□□□ □□□ □□□□ □□□□. Policy1□ storage1□ □□□□ □□ □□□□ □□□□□.

Subnet1□ Pool1□□□ □□□ Azure Batch □□ □□□□□.

Pool1□ □□□ □□□□ storage1□ □□□□ □ □□□ □□ □□□.
□□□ □□ □□□?

A. Policy1□ □□□□ □□□□□.

B. Policy1□ □□□ □□□□□.

C. Subnet1□ □□□□ □□□□ □□□□ □□□□□□ □□□□□.

D. Subnet1□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Adding an alias is used when referencing services using specific names (e.g., DNS names), but in this case, you need to add the actual resource (storage1) to the policy, not just an alias.

NEW QUESTION: 30
□□□ □□□□ □□ □□ □□□□ □ □□ □□□ □□ □□□□□□ □ □□□□ □□ □□□ □□□□ □□, □□ □ □□□□ □□□. □□ □□□ □ □□ □□□□ □□□□□□□□?
A. □□□ □□□
B. Azure □□□
C. Azure Private Link
D. Azure DNS
E. Azure DDoS □□
Answer: B (LEAVE A REPLY)
Azure Firewall is one of the cloud-based, managed network security services which protects Azure Virtual Network resources. This service can be used to centrally create/develop, enforce, and log applications and network connectivity policies across virtual networks and subscriptions.
Option A is incorrect. Azure Front Door is an application delivery network that offers global load balancing and site acceleration services for web applications.
Option B is correct. Azure Firewall can be used centrally to create/develop, enforce, and log applications and network connectivity policies across virtual networks and subscriptions.
Option C is incorrect. Azure Private Link allows you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure-hosted customer-owned/partner services over a private endpoint in your virtual network.
Option D is incorrect. Azure DNS offers name resolution with the help of Microsoft Azure infrastructure.
Option E is incorrect. Azure DDoS Protection offers protection against DDoS threats.
Reference:
https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview?WT.mc_id=modinfra-33046-thmaure#firewall

NEW QUESTION: 31
Azure WAF(□ □□□□□□ □□□)□ □□□□ □□□□ FD1□□□ Azure Front Door □□□□□ □□□□.
FD1□ app1.contoso.com□□□ □□□□□ □□□□ □□□□ □□ □□ Azure □□□ □□ □□ Azure □□□ □□□□ Azure □□□ □□ □□□□ □□□□□.
□□ □□ □□ □□□□ app1.contoso.com□ □□ □□□ □□□□□ FD1□ □□□□ □□□.
WAF □□□ □□□ □□□□ □□□?
A. □□□□□ □□□ □□
B. □□□□ □□ □□
C. □□ □□ □□□ □□□□ □□□ □□ □□
D. □□ □□□ □□□□ □□□ □□ □□
Answer: D (LEAVE A REPLY)
Custom rules allow you to create tailored rules to suit the exact needs of your applications and security policies. Now, you can restrict access to your web applications by country/region. As with all custom rules, this logic can be compounded with other rules to suit the needs of your application.
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.

NEW QUESTION: 32

□□□□□

□□□ □□□ □□□□

□□□ □□ □□ □□□ □□ □□□ □□□□□□.

- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx

Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

- □ □□□□: 12345678

□□□2-1□ DNS □□ □ □□ □□□ □□□□□. □ □□□ fabrikam.com□ □□ DNS □□□ □□□□□□. DNS □□□□ □□□□□ □□□□□ □□□□ □□□□□. DNS □□□ IP □□□ 10.2.1.4□ 10.2.1.5□□□.

VNET2□ □□ □□□ fabrikam.com□ □□ □□□□□ □□□ □□□ □□□ □ □□□ □□□□ □□□.

□ □□□ □□□□□ Azure □□□ □□□□□□

Azure DNS Private Resolver

The Azure DNS Private Resolver is a service that can resolve on-premises DNS queries for Azure DNS private zones. Previously, it was necessary to deploy a VM-based custom DNS resolver, or use non-Microsoft DNS, DHCP, and IPAM (DDI) solutions to perform this function.

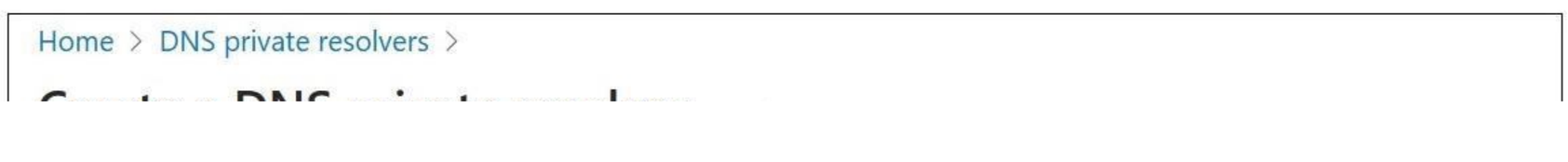
Create a DNS resolver inside the virtual network

Step 1: In the Azure portal, search for DNS Private Resolvers.

Step 2: Select DNS Private Resolvers, select Create, and then on the Basics tab for Create a DNS Private Resolver enter the following:

Subscription
Resource group:
Name: Enter a name for your DNS resolver (ex: mydnsresolver).
Region: Choose the region you used for the VNET2 virtual network.
Virtual Network: Select VNET2.

Don't create the DNS resolver yet.



Create a DNS private resolver ...

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

Azure DNS private resolver bridges on-premises DNS namespaces with private DNS zones hosted on Azure DNS without the burden of deploying VM-based custom DNS servers. You can resolve DNS queries from on-premises networks and do conditional forwarding to on-premises DNS zones. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ: _mysubscription

Resource group * ⓘ: myresourcegroup

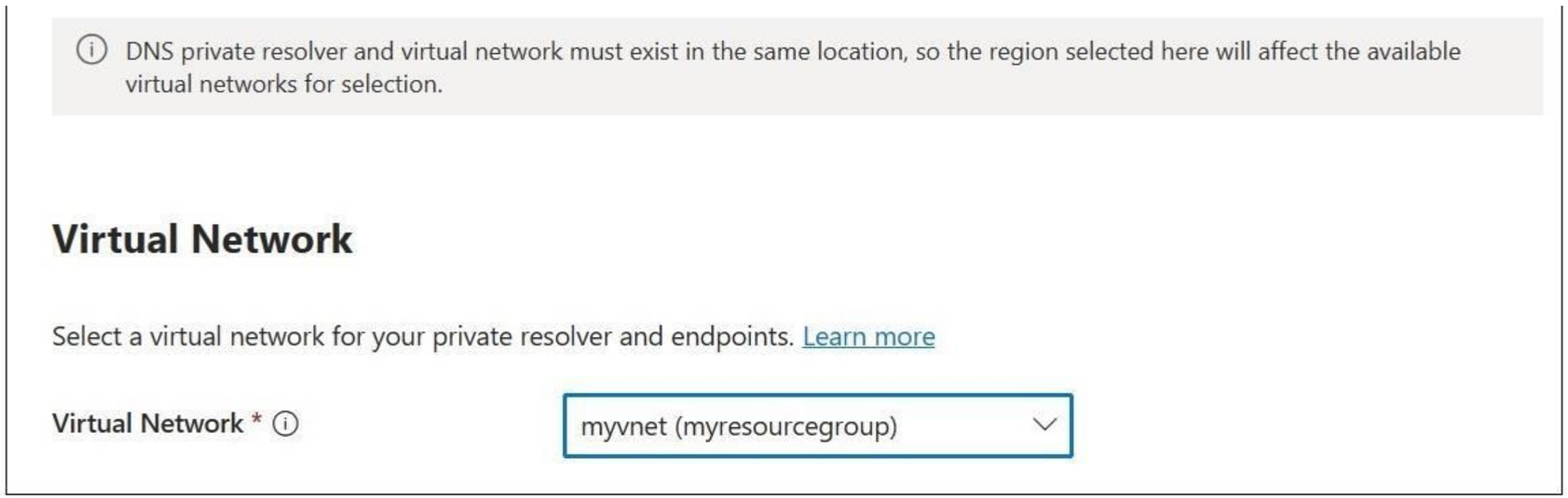
Create new

Instance details

Private resolver is a regional service. Only virtual networks and rulesets in the same region can use this private resolver.

Name *: mydnsresolver

Region *: (US) West Central US



Add rules to the forwarding ruleset
Add two new conditional forwarding rules to the ruleset.

Step 3: On the myruleset | Rules page, select Add, and enter the following rule data:

Rule Name: Internal
Domain Name: internal.fabrikam.com. (fabrikam.com domain in the question)
Rule State: Enabled
Under Destination IP address enter 10.2.1.4, and then select Add.

Question has the IP address of the DNS servers will be 10.2.1.4 and 10.2.1.5.

Step 4: On the myruleset | Rules page, select Add, and enter the following rule data:

Rule Name: Internal
Domain Name: internal.fabrikam.com. (fabrikam.com domain in the question)
Rule State: Enabled
Under Destination IP address enter 10.2.1.5, and then select Add.

Reference:
https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-get-started-portal

NEW QUESTION: 33
□□□ □□
VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□. VNet1□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

AG1□ https://app1.contoso.com URL□ □□□□ App1□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- TLS □□□ AG1□□ □□□□□ □□□.
- AG1□ □□□ □□ □□ □□ □□ □□□□□□.
- □□□ SSL □□□ □□ □□ □□□□□□.

□1.
□□□□ □□□ □□□ □ □□□, AG1□ □□□ □□ □□□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Certificates: 1 2 3 4 5

Backend pool targets: 1 2 3 4

Answer:

Answer Area

Certificates: 1 2 3 4 5

Backend pool targets: 1 2 3 4

NEW QUESTION: 34
Policy1□ "string1"□ □□□□□ □□□□ □□ □□□□ □□□□□ □□□□□□□□.
Frontend1□□□□ □□ □□□□□□□□ Policy1□□□□ Azure WAF(□ □□□□□□□□□ □□□) □□□ □□ Azure Front Door □□□□□ □□□□.
https://www.contoso.com/redirect1. Policy1□ Frontend1□ □□□□ □□□□.
□□ □□□□ □□□ □□□□ □□□.
"string2"□ □□□□ □□□ □□ Frontend1□ □□ □□□ □□□□ □□□□□□□ □□□.
https://www.contoso.com/redirect2.

□□ □ □□ □□□ □□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□□ □□ □□□ □□□□.
B. □□□□ □□□ □□□□□.
C. □□□□□ □□□□ □□□□□.
D. □□□ □□□□.
E. □□□□ □□□□□.
F. Policy1□ □□□ □□ □□□ □□□□□.
Answer: A,D,E (LEAVE A REPLY)
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: 35
□□ □□ 3 - □□□ □□□□
□□
□□□□□(Proseware, Inc.)□ □□□□ □□□ □□ □□□□□□□ □□□ □ □□ □□□ □□□□□.
□□ □□. □□□□□ □□
Proseware□ corp.proseware.com□□□ □□□ □□□□□ Active Directory Domain Services(AD DS) □□□□□ □□□□ □□□, □ □□□□□ proseware.com□□□ □□□ Microsoft Entra □□□□ □□□□□□.
Proseware□ proseware.com□ □□□ Azure □□□ □□□□ □□□□.
Proseware□ □□ □□ □□(CA)□ □□□□ □□□□.
□□ □□. □□□□ □□□
□□ □□□□□ □□ □□ □□□ □□ □□□□ □ □□□□ □□□□ □□□□.

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□ ExpressRoute □□□ □□□□ Azure□ □□□□□.
SFONet□ □□□ □(S2S) VPN□ □□□□ Azure□ □□□□□.
□□ □□. Azure □□□
Azure □□□□ □□ □□ □□□ □□ □□□□ □ □□□□ □□□□ □□□□.

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

□□□□ VM1, VM2, VM3, VM4□□ □□□ □□ □□ 4□□ □□□□ □□□□. VM1□ VM2□ App1□□□ □□ □□□□□□.

VM3 □ VM4□ app2.proseware.com□□□ FQDN□ □□□□ □□□□ □ □□ App2□□ □ □□□□□□□ □□□□□□. □□□□ HTTP □□ HTTPS□ □□□□ app2.proseware.com□ □□□□□□.

VM1, VM2, VM4□ SpokeVNet□ □□□□ □□□□.

□□□□ □□ □□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □□□□.

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

□□□□ FD1□□□ Azure Front Door Standard □□□□ □□□□ □□□□. FD1□□ □□ □□□□□ □□□ □□□□ APPGW1□ □□□□ □□ □□ □□ □□□ □□□□ □□□□.

HubVNet□ ERGW1□□□ ExpressRoute □□□□□□ □□□□ NYCNet□ □□□□□.

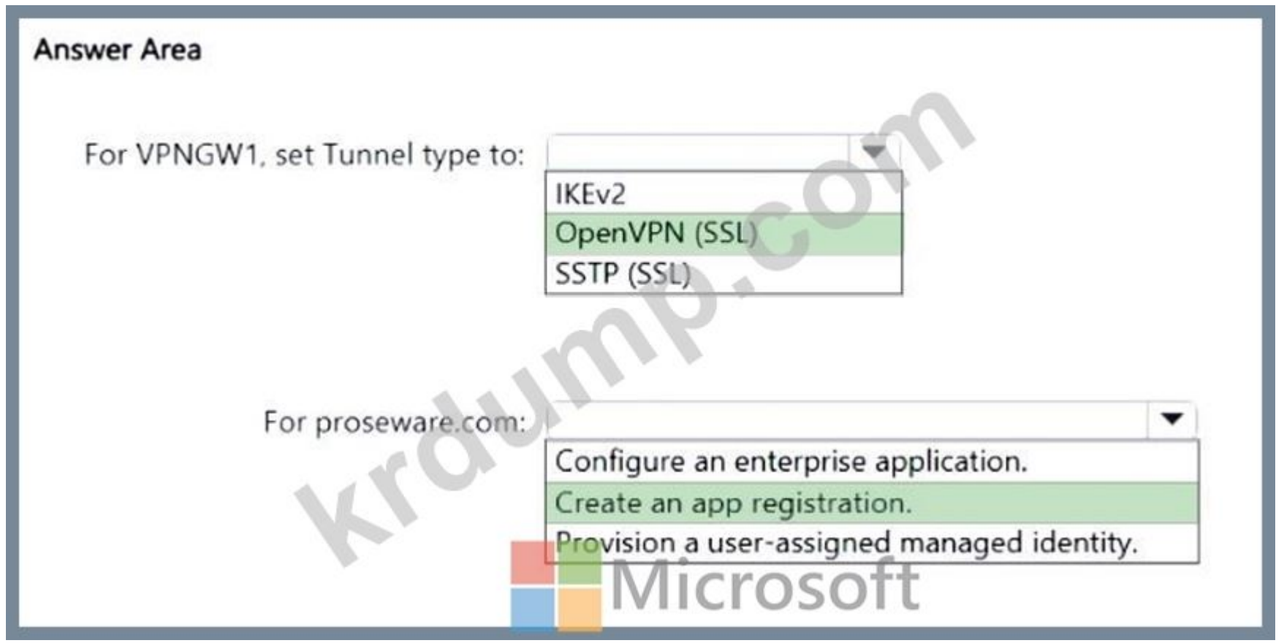
□□□ □□ □□ □ □□ □□. □□□ □□ □□

Proseware□ □□□ □□ □□ □□□ □□□ □□□□□.

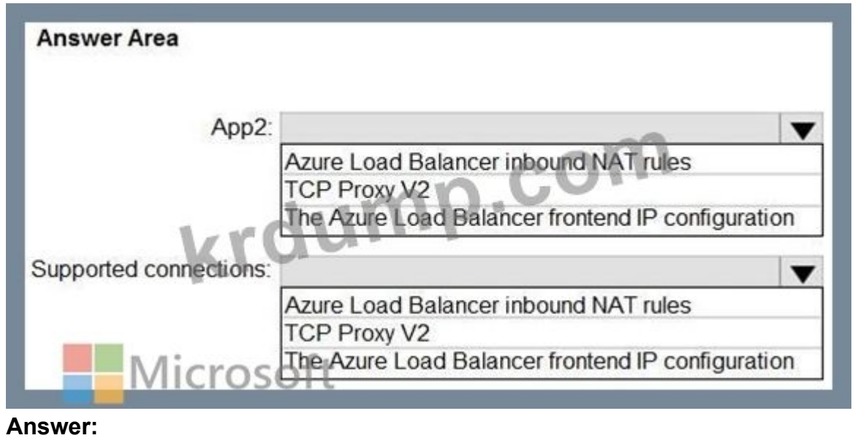
- PRDNS1□□□ □□□ Azure □□□□ DNS □□□□ HubVNet□ □□□□ PRDNS1□ SpokeVNet□ □□□□□.
- DNSRS1□□□ □□□ DNS □□□ □□ □□□ □□□□, DNSRS1□ PRDNS1□ □□□□□.
- Azure □□ □□□□ □□□□ □□□□ □□ □□□ □□□□□.
- □□□□□ □□□□□□ SUBNET-JUMPHOSTS□ TCP □□ 3389□ □□ □□□□ □□□ □□□□□.
- □□□□□ SpokeVNet□□ □□□□ TCP □□ 80 □□□ □□□□□.
- Azure Virtual Network Manager □□□ □□□□ NSG □□□□ □□ □□□□□ □□□.
- HubVNet□ NVA1 □ NVA2□□ □□□ □□□□ □□ □□□□□□(NVA) □ □□ □□□□□.
- HubVNet□ LBGW1□□□ □□□ □□□□□ □□ □□□□ □□□□□.
- NVA1 □ NVA2□ □□□□ LBGW1□ LBS1□□ TCP □□ 443, 1433 □ 1434□ □□□□ □□□□□ □□□□□.

- App2□ □□□ □□ □□□□ FD1□ □□□□ □□□□□ □□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□ □□ □□□ □□□□□.
- Azure Virtual Network Manager □□□ □□□□ □□□□□□.
- NYCNet□ SFONet □□ □□□□ ExpressRoute □□ □ S2S VPN□ □□ □□□□□□.
- Windows 11 □□□ □□ □□□□ P2S(Point-to-Site) VPN□ proseware.com □□ □□□ □□□□ HubVNet□ □□□ □ □□□ □□□□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□ □□ □□□ □□□□□.
- □□□ □ □□ CA□ □□□□□□.
- APPGW1□ □□ □□□□□ □□ □□□ □□ □ □□□□ □□□□□ □□□□.
- Azure□□ □□□□□ □□ □□ □□□ □□□ □□ □ □□□□ □□□□□ □□□□□□.
- app2.proseware.com□□ □□□□ □□ □□□ □□□□ FD1□ □□ □□□□□□ □□□□.
- NYCNet□ □□□□ □□□ □□ □□□□□□ □□□□ Azure □□□□ □□□□□ □□□□ □□□.
- HubVNet □ SpokeVNet□ □□□□ □□ □□□ □□□□ □□□□□□ □□□□ Azure □□□□ □□□□ □ □□□ □□□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□□□ □□ □□□ □□□□□.
- □□□□□ □□□□ □□□□ □□ □□□□□ □□□□ □ □□□ IP □□ □□□ □□□□□□.
- SpokeVNet□□ azure.proseware.com □□□□□□□ corp.proseware.com □□□□□□□ □□ □□ □□ □□□ PRDNS1□ □□□□ □□□□□.
- □□□ □ □□□ □□□ □□□□□□□.
□□□ □□
□□ □□ □□□ □□□□□ P2S VPN□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

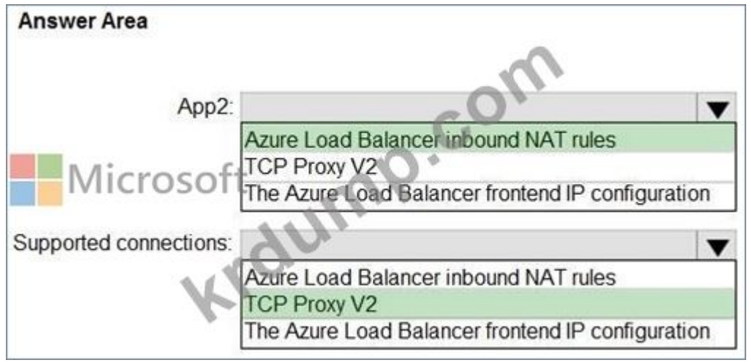
Answer:



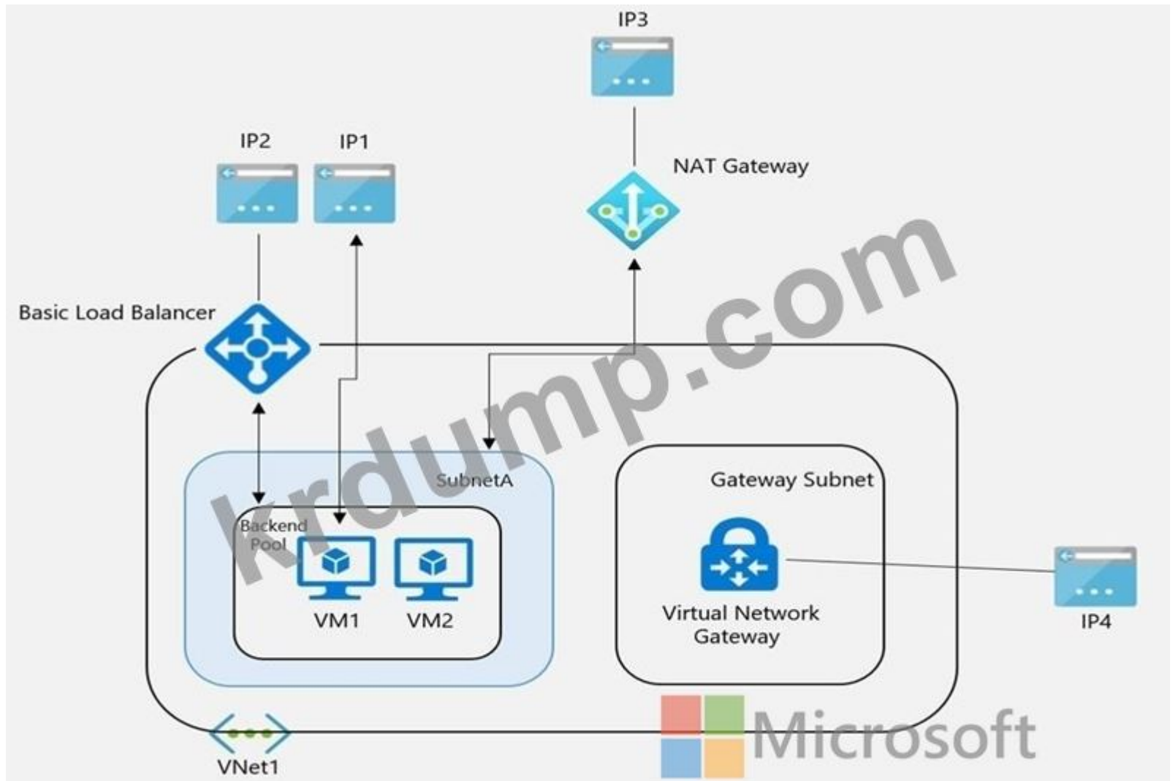
NEW QUESTION: 36
□□□ □□
Azure □□□ □□□□. □ □□□□ App1□ App2□□ □ □□ □□ □□□□□ □ □□ □□ □□ □□ □□, PLS1□□□ Azure Private Link □□□, □□□ LB1□□□ Azure □□ □□□□ □□□□ □□□□. PLS1□ LB1□ □ □□□ TCP Proxy V2□ □□□□□□ □□□□. PLS1□ App1□□ □□□□ □□□□□.
□□ □□□ □□□□ □□□.
- App1□ App2□ □□ □□ □□□ □□□□□□.
- □□□□ □□ □□□□□ □□ □□ □□□□.
App2□ □□□ □ □□□ □□□ □□□ □□□□ □□, □□□□ □□ □□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 37
□□□□ Azure □□□ □□ □□□□.



VM1□ □□□□ □□ □□ IP □□(ILPIP)□ □□ □□ □□□□□.
□□ □□ □□□□ □□ IP □□□ □□□□□. VM1□ VM2□ □□□ □□ □□□□.
NAT □□□□□□ SubnetA□ □□□ IP3□□□ □□ IP □□□ □□□□□.
VNet1□□ IP4□□ □□ IP □□□ □□ □□ □□□□ □□□□□□ □□□□.
VM1□□ □□□□□ □□□□□ □□□□ □□□ □ □□ □□ □□□ □□□□□?
A. IP1

B. IP2
C. IP3
D. IP4
Answer: C (LEAVE A REPLY)
On a subnet with a NAT gateway, all outbound to Internet scenarios are superseded by the NAT gateway.
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat- and-vm-with-instance-level-public-ip-and-public-load-balancer

NEW QUESTION: 38
Azure □□□ VNet1□□□ □□ □□□□□ □□□□. VNet1□□ Subnet1□□□ □□□□ □□□□.
Subnet1□ AppGw1□□□ □□□ Azure Application Gateway v2 □□□□□ □□□□□. NSG1□□□ □□□ □□□□ □□ □□(NSG)□ □□□□ NSG1□ Subnet1□ □□□□□.
AppGw1□ VNet1□□ □□□□ □□□□ □□ □□□□□□ □□ □□□. □□, □ □□□□ AppGw1□ □□□ □□□ □□□ □□□□□ □□□.
NSG1□ □□□ □□□□ □□□?
A. □□□□□ 4096□□ □□ □□□ □□□□ □□□□ □□□□□ □□
B. □□□□□ 100□□ □□ □□□ □□□□ □□□□ □□□□ □□
C. □□□□□ 4096□□ □□ □□□ □□□□ □□□□ □□□□ □□
D. □□□□ 100□□ □□ □□□ □□□□ □□□□ □□□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 39
□□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
- Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678

VNET2□ □□□□ VNET1□ VNET3□ □□□ □□□ □□□ □ □□□ □□ □□□. □, VNET1□ VNET3□ □□□□ VNET2□ □□ □□□□ □□ □□□□ □□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.

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

NEW QUESTION: 40
OpenVPN□ □□□□ Azure □□ □(P2S) VPN□ □□□□ □□□□. □□□□ □-□□□□ Active Directory □□□□ □□□□ □□□□□.
VPN □□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□?
A. □□ □□(CA)
B. RADIUS □□
C. Azure □ □□□
D. Azure Active Directory(Azure AD) □□□□□□ □□□
Answer: B (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

NEW QUESTION: 41
□□□ □□
□□□ DC1□□□ □□□□□ □□□□□□ □□□□ □□□□. DC1□ □□□ □□□ □□ IPv4 □ IPv6 □□ □□□ □□□□ □□□□ □□□□□□.
□□□□ Azure□ □□□□□□□ □□□□□□.
□□□ Azure □□□ □□□□□.
□□□ □□ □□ □□ IP □□□ □□□□□□□ □□□.
□ IP □□ □□□ □□□ □ □□ □□ □□ IP □□ □□□□ □□□□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

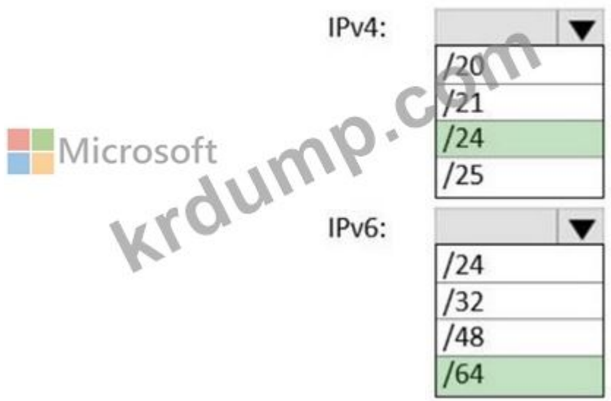
Answer Area

Microsoft

IPv4:
- /20
- /21
- /24
- /25

IPv6:
- /24
- /32
- /48
- /64

Answer Area



NEW QUESTION: 42

□□□ □□

□□□ □□ □□□ □□□□ □□ Azure □□□ □□□□ Azure □□□□ □□□ □□□□□.

- □□ □□
- Azure □ □□□
- □□ □□□□ □□□□□
- Azure SQL □□□ □□□□

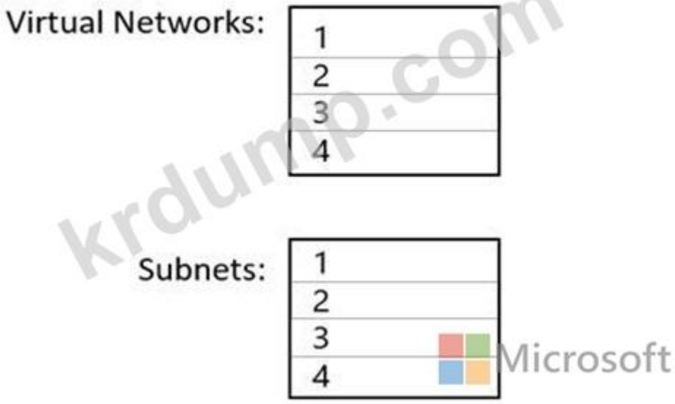
App Service□ SQL Managed Instance□ □□ □□□□□ □□□□ □□□□ □□□ □□□□ □□□.

□□□□ □□□ □□ □□□□ □ □□□□ □□ □□□□ □□□. □□ □□□□ □□ □□□□ □ □□□ □□ □□□ □□□□□ □□□.

□□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.

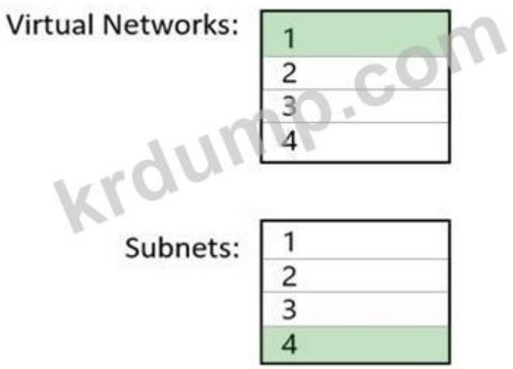
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



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: 43

□□□ □□

□□□□□ □□□□□□ Windows Server 2022□ □□□□ DNS1□□□ □□□ □□□□.

DNS1□ DNS □□ □□□ □□ IP □□□ 10.1.0.1□□□. □□□□□□ DNS1□ □□□□ □□□ □□□□ □□□□ □□□□.

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

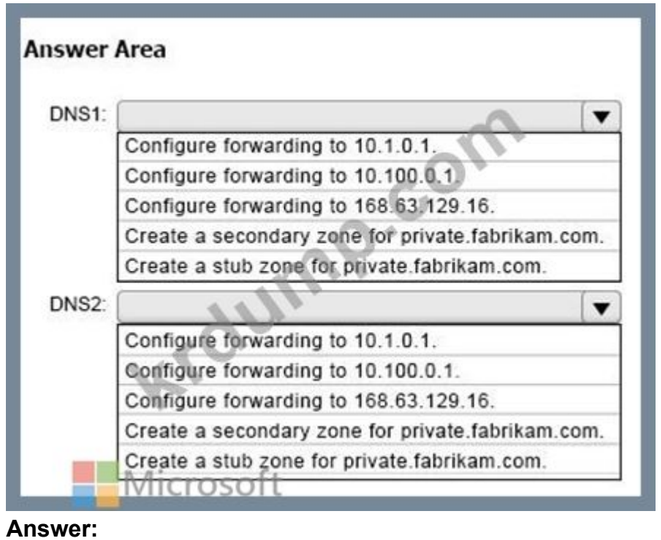
Name	Type	Description
private.fabrikam.com	Azure Private DNS zone	Linked to Vnet1
Vnet1	Virtual network	*None*
SQL1	Azure SQL Database	Has a private endpoint in Vnet1 that is registered in private.fabrikam.com
DNS2	Server that runs Windows Server 2022	Has the DNS server role and an IP address of 10.100.0.1

□□□□□ □□□□□ □□□ □ VPN□ □□□□ Vnet1□ □□□□□.

□□ □□□□□ □□□□ sql1.private.fabrikam.com□ IP □□□ □□□ □ □□□ □□□□ □□□.

DNS1□ DNS2□□ □□□ □□ □□□? □□ □□□□ □□ □□□ □□□ □□□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.

□□: □□ □□□ 1□□□□.



Answer:

nswer Area

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

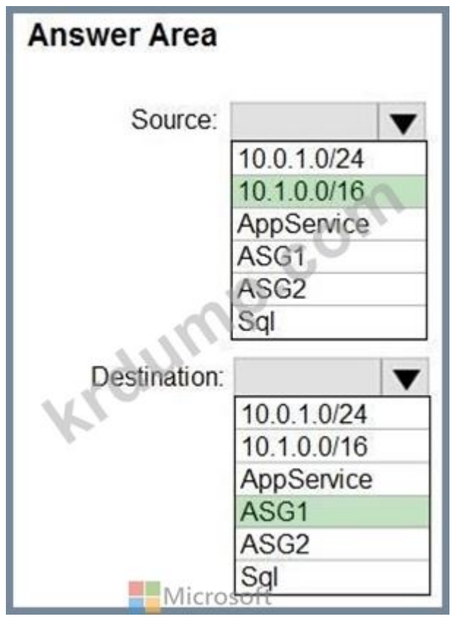
NEW QUESTION: 44
□□□ □□
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

□ □□□□ App1□ □□□□□ □□ 5□□ □□□ □□ □□□ □□□□□.
App1□ □□□□□ □□ □□□ SQL1 □ SQL2□ □□□ □ □□□ NSG1□ □□□ □□□□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□ □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Answer:



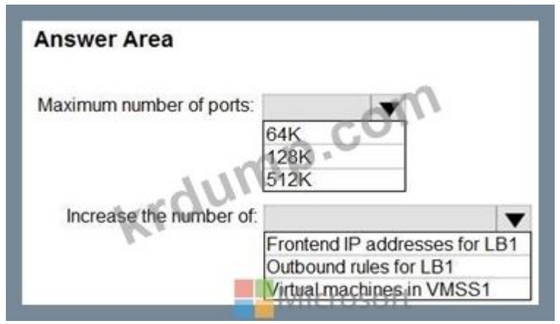
NEW QUESTION: 45

□□□ □□

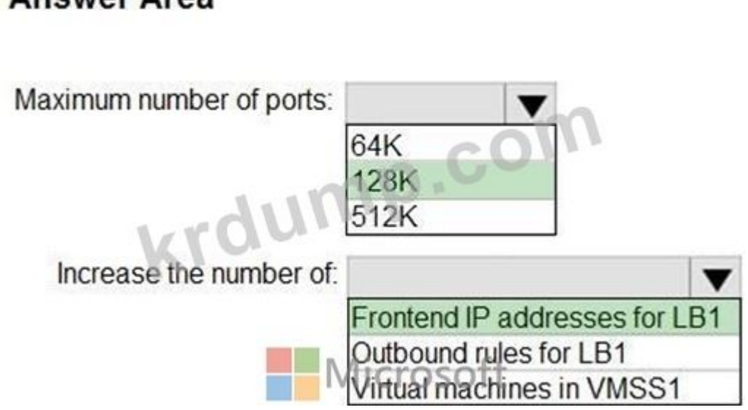
VMSS1□□□ □□ □□ □□ □□□ LB1□□□ □□ □□ Azure □□ □□□□ □□□ Azure □□□ □□□□. VMSS1□□ □□ IP □□□ □□ □□ □□ 8□□ □□□□. VMSS1□ LB1□ □□□ □□ □□□□ □□□□. LB1 □□ □□□□□ IP □□ 2□□ VMSS1□ □□□ □□□ □□□□ □□□□□ □□ 1□□ □□□□.

VMSS1□ □□ □□□□ □□□ □ □□ □□ □□ □□ □ □□□, VMSS1□□ □□□ □ □□ □□ SNAT □□ □□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections#scenarios

NEW QUESTION: 46

□□□ □□

Windows Server□ □□□□ DNS □□ □□□ □□□ Server1□□□ □□□ □□□□□ □□□ □□□□.

Azure □□□□ VNet1□ VNet2□□ □ □□ □□ □□□□□ □□□□ □□□□.

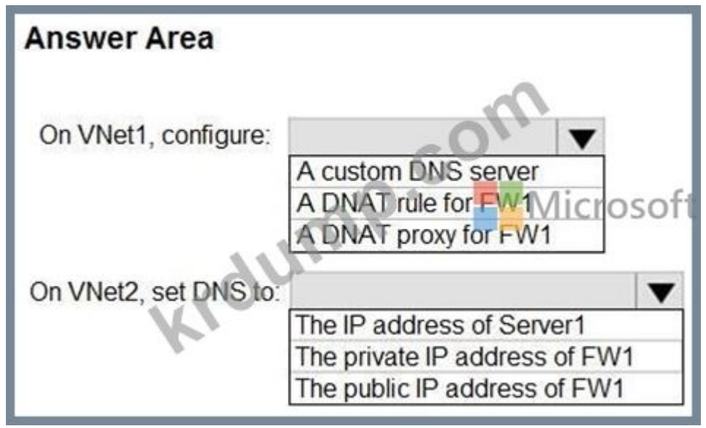
VNet1□□ FW1□□□ □□□ Azure □□□ □□□□□ □□□□ □□□□. VNet1□ VNet2□ □□□□□□.

□□□□□ □□□□□ ExpressRoute□ □□□□ VNet1□ □□□□ □□□□. □□□□□ □□□□□ VNet2□□ □□□ □ □□□□.

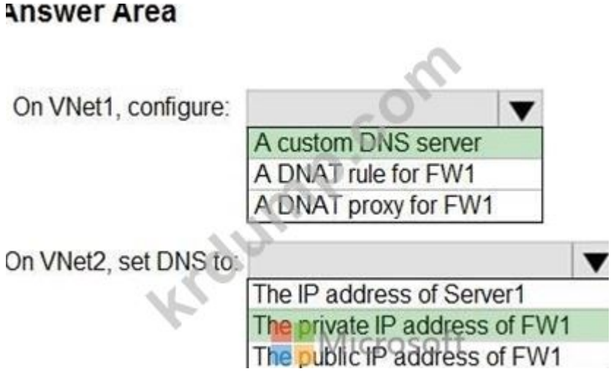
VNet2□ □□□ □□ □□□ □□ □□□ □□ Server1□ □□□□□ □□ □□□. □ □□□□ □□ □□□ □□□□□ □□□.

□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 47
Windows Server□ □□□□ □□ □□□ 5□ □□□□. □ □□ □□□ □□ □□ □ □□ □□□□□□.
www.contoso.corn□□□ □□□ □□□ □ □ □□ □□ □□ URL □□□ □□□□ □ □ □□ □□ □□□□ □□□□ □□ Azure □□□□□□ □□□□□□ □□□ □□□□□. □:
https://www.contoso.com/app1.
URL □□□ □□□□ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□
B. □□ □□
C. HTTP □□
D. □□□
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/application-gateway/configuration-request-routing-rules#rule-type

NEW QUESTION: 48
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□ □□ □□□□ □□□ □□□□□ □□□ □□□□□.
- □□□ □□□: Subnet1
- □□□: Microsoft.Storage
- □□ □□: □□ □□
- □□□: storage1

VM1□ □□ □□□□ □□□ □ □□□?
A. □□ □□ Azure □□□ storage1□ □□ □□□□ □□□ □□□ □□□□.
B. □□ □□ Azure □□□ storage1□ □□
C. storage1 □ storage2□ □□ □□ Azure □□□□ □□□□.
D. □□ □□ Azure □□□ storage1 □ storage2□ □□ □□ □□□ □□□ □□□
Answer: A (LEAVE A REPLY)
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: 49
□□□ □□
Sub1□ Sub2□□ □ □□ Azure □□□ □□□, □ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

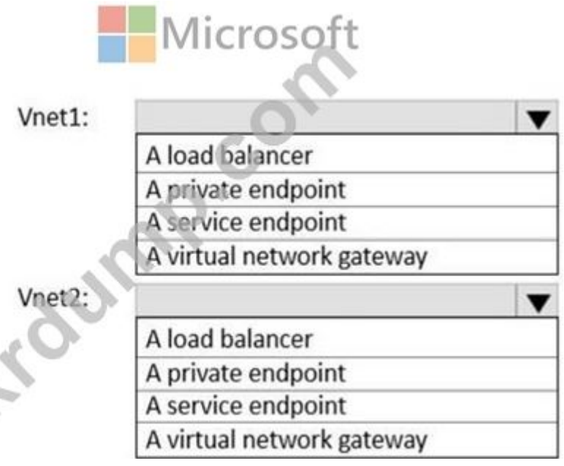
Name	Subscription	Type	Description
VNet1	Sub1	Virtual network	• Contains Subnet1
VM1	Sub1	Virtual machine	• Connected to Subnet1 • Hosts a resource named Resource1
VNet2	Sub2	Virtual network	• Contains Subnet2
VM2	Sub2	Virtual machine	• Connected to Subnet2 • Hosts an app named App1

Azure Private Link □□□□ □□□□ App1□ Resource1□ □□□□ □ □□□ □□ □□□.

Private Link □□□□ □□ □□□ □□□□□ □ □□ □□□□□ □□ □□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

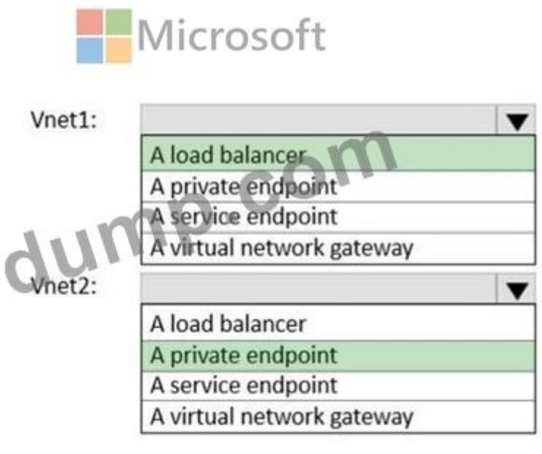
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



NEW QUESTION: 50

Azure □□ □□□□(Vnet1)□ □□□□□ □□□□□ □□□□. □□□□□ □□□□□□ □□ □□ VPN □□□ □□□□.

Vnet1□□ SKU□ VpnGw1□□ □□ □□□ GW1□□□ □□□ □□ □□□□ □□□□□□ □□□□□.

□□ □□□ □□ GW1□ □□ □□□ □ VPN □□□ □□□□ □□□□.

□□□□ □□□□□ □□ □□ GW1□ □□□ □ □□□ □□□□ □□□.

□□□ □□□□ □□ □□□ □□ □□□?

A. □□ □□□ □□□ □□□□ □□□□□.

B. BGP□ □□□□ □□□□□.

C. Azure □□ IP □□ □□□ □□□□ □□□□□.

D. IPsec/IKE □□□ □□□ □□□□ □□□□□.

Answer: (SHOW ANSWER)

Previously, when working with policy-based VPNs, you were limited to using the policy-based VPN gateway Basic SKU and could only connect to 1 on-premises VPN/firewall device. Now, using custom IPsec/IKE policy, you can use a route-based VPN gateway and connect to multiple policy-based VPN/firewall devices. To make a policy-based VPN connection using a route-based VPN gateway, configure the route-based VPN gateway to use prefix-based traffic selectors with the option "PolicyBasedTrafficSelectors".

https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps

NEW QUESTION: 51

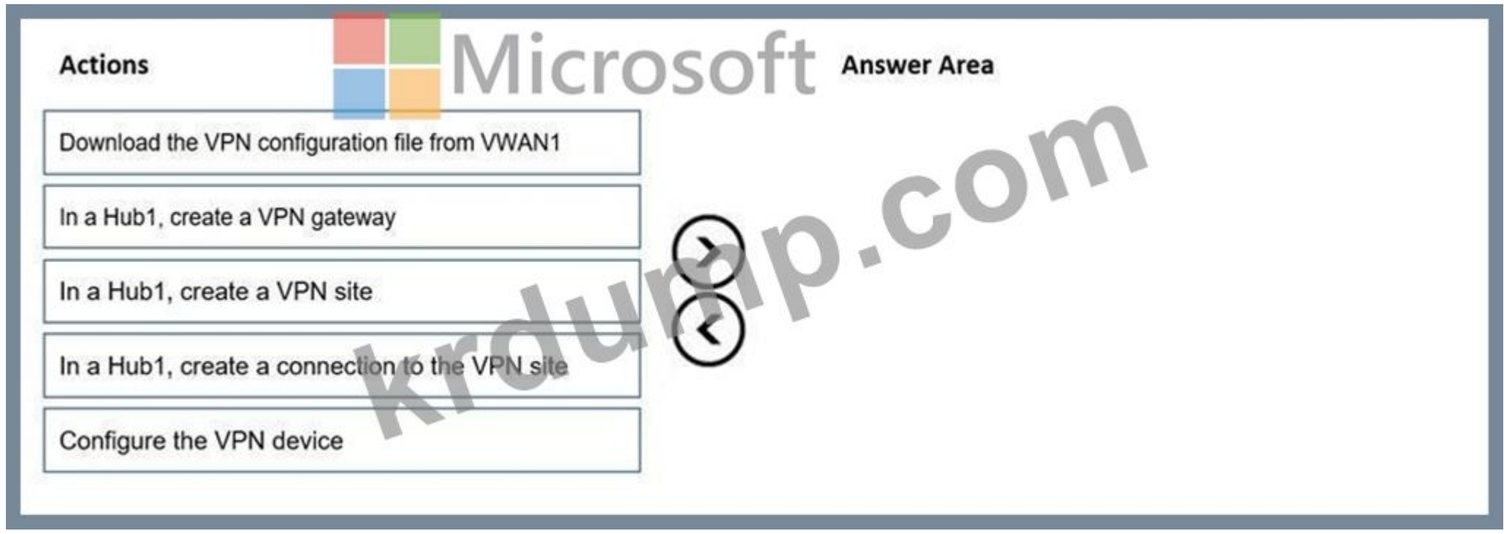
□□□ □ □□ □□

□□□ □ □□ □□□□□ □□□□ □□□□ □□□, □ □□□□□ □□ VPN □□□ □□□□ □□□□.

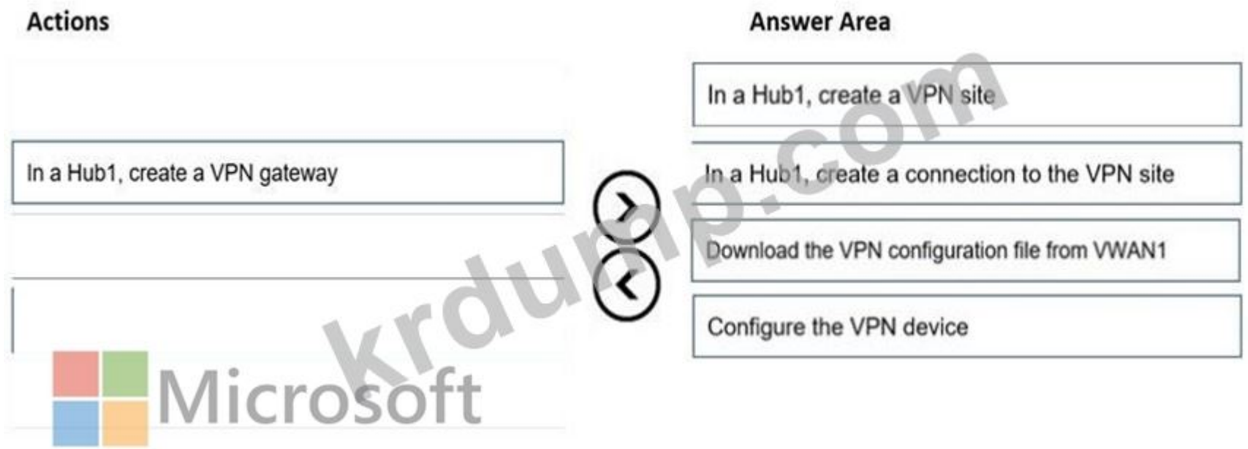
Azure □□ WAN(VWAN1)□ □□, □ □□ WAN□□ Hub1□□□ □□□ □□□□. Hub1□ □□□ □ VPN □□□ □□□□ □□□□□ □□□ □ □ □ □ □□ □□□□□.

Hub1□ □□□□ □ □□ □□□□ □□□ □ □□□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.



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: 52

□□□ □□

Subscription1□ Subscription2□□ □□□ Azure □□□ □ □ □□□□.

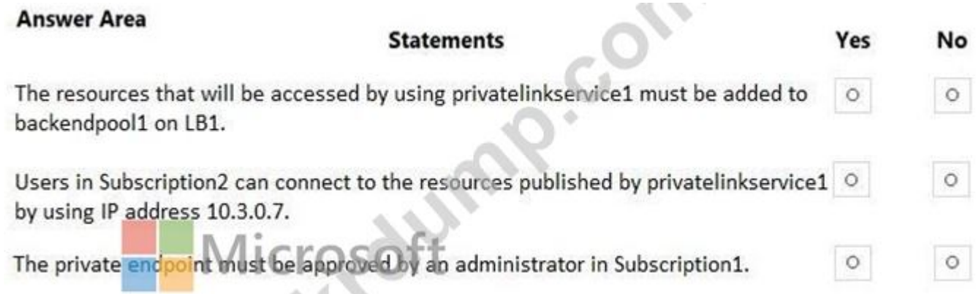
□ □□□ □□ □□□□ □□□ □□□ □□□□.

privatelinkservice1 □□□ □□ □□ □□ □□□□ □□□□□. (privatelinkservice1 □□ □□□□□□.)

Subscription1□□ □□ □□□ □□□ □□□□ lb1 □□□ □□□ □□□ □□ □□□□□. (lb1 □□ □□□□□□.)

privateendpoint4 □□□ □□□ □□ Subscription2□ □□□ □□□□□□ □□□□□. (privateendpoint4 □□ □□□□□□.)

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

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

NEW QUESTION: 53
VM1□□□ □□□ Azure □□ □□□ □□□□.
Azure Network Watcher□ □□□□ VM1□ □□ □□□□ □□□□ □□□□ □□□.
□□□ □□□ □□ □□□ □□□ □ □□□?

A. □□ □□□□ □□
B. □□ □□□□, VM1□ □□ □□ □ □□□□ □□□□ □□
C. VM1□□ □□ □□ □□
D. VM1□ □□ □□□□ □ □□ □□□ □□
E. □□ □□□□ □ □□□□ □□□□ □□□ □□
F. □□□□ □□□□ □□ □□
Answer: (SHOW ANSWER)
Once your packet capture session has completed, the capture file is uploaded to blob storage or to a local file on the virtual machine. The storage location of the packet capture is defined during creation of the packet capture.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal

NEW QUESTION: 54
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Azure Front Door □□□□ □□□(AFD1)□ Azure WAF(□ □□□□□□ □□□) □□(WAF1)□ □□□ Azure □□□ □□□□. AFD1□ WAF1□ □□□□ □□□□.
AFD1□ □□□□ □□□ □□ □□ □□□ □□□□ □□□.
□□ □□: WAF1□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □□□
B. □
Answer: A (LEAVE A REPLY)

NEW QUESTION: 55
□□□ □□
RT1□□□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□ □□□□□.

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

Vnet1□□□ Azure □□ □□□□□ □□□, □□ □□□□□□ □□ □□ □□□ □□□□ □□□□.

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**

□□□ □□ □□ □□ □□ □□□ □□□□ □□□□.

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□ ExpressRoute □□□ □□□□□. □□□□□ □□□□ □□□ □□ □□□ □□□□□.

- 0.0.0.0/0
- 10.0.0.0/16

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

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.	○	○

Answer:

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: 56

□□□ □ □□ □□

□□(Contoso, Ltd.)□ □□ □□ □□□ □□□□ □□□ Azure □□□ □□□□ □□□□.

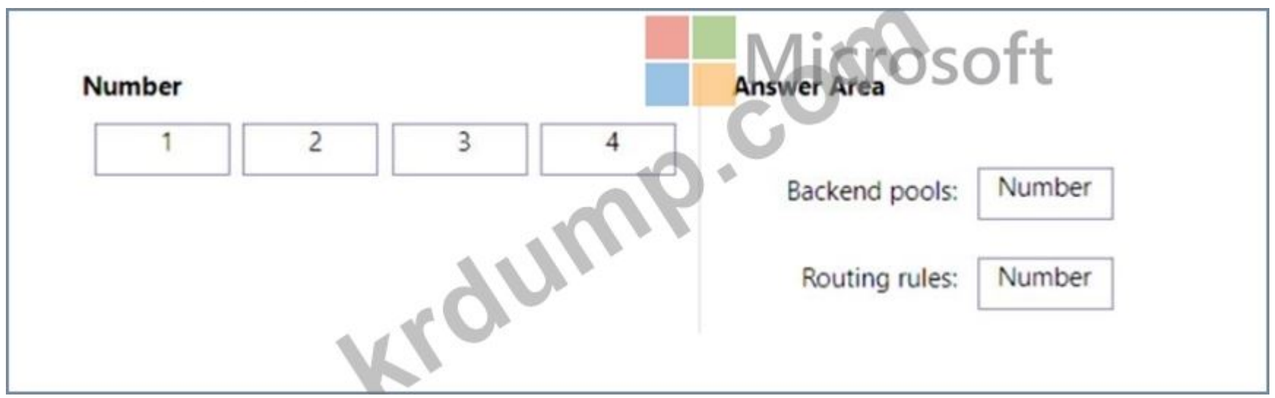
Name	Type	Location	Description
App1us	Azure App Service	East US	A website for the United States office of Contoso
App1uk	Azure App Service	UK West	A website for the United Kingdom office of Contoso
St1us	Storage account	East US	Contains images for the United States website
St1uk	Storage account	UK West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

Azure Front Door□ □□□ □□□□□. □□□□ □□ □□ □□□ □□□□ □□□.
- https://contoso.azurefd.net/uk URL□ □□ □□□ App1uk□□ □□□□□□ □□□.
- https://contoso.azurefd.net/us URL□ □□ □□□ App1us□ □□□□□□ □□□.
- https://contoso.azurefd.net/images URL□ □□ □□□ □□□ □□□ □□□.

□□□□□ □□ □□□ □□□□ □□□□ □□□□□□.

□□□ □ □□ □□□ □□ □□□ □□□ □□□□ □□□? □□□ □□□□□ □□ □□□ □□□□□ □□□ □□ □□□ □□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.

□□: □□ □□□ 1□□□□.



Answer:

Explanation:
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-routing-architecture?pivots=front-door-classic
https://learn.microsoft.com/en-us/azure/frontdoor/front-door-route-matching?pivots=front-door-classic#frontend-host-matching
https://learn.microsoft.com/en-us/azure/frontdoor/routing-methods

NEW QUESTION: 57
Azure Front Door □□□□□ □□□ □□ □□□ Azure WAF(□ □□□□□□ □□□) □□□ □□□□.
□□ □□ □□□ □□□□□ □□□ □□□□ □□□.
- □□□□□ □□ □□□ □□□□□.
- □□□□□□□□ □□ □□□ □□□□□.
- 131.107.100.0/24 □□□□□□ □□ □□□ □□ □□□□□.
1□ □□ 100□ □□□ □□□ □□□□□.
□□□ □ □□ □□□ □□□□ □□□?
A. □□ □□□ □□□ □□ □ □□ □□□ □□ □□
B. □ □□ □□□ □□ □□□ □□□ □□ □□
C. □□□ □□□ □□ □□□ □□□ □□ □□
D. □ □□ □□□ □□ □□ □□□ □□□ □□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
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

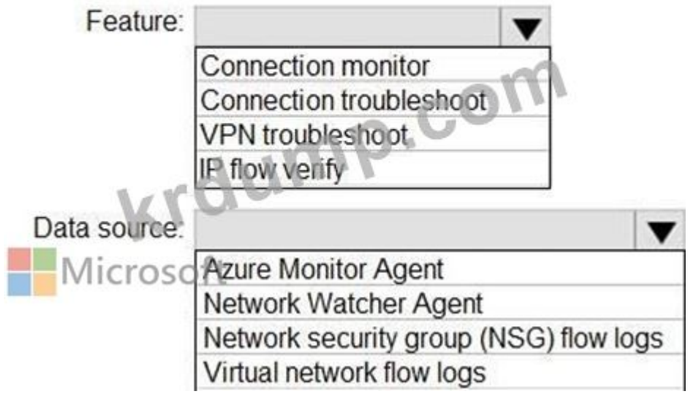
NEW QUESTION: 58
□□ □□□ □□ □ □□ □□□ JSON □□□ □□□□□□□ □□□□□ □□□ □□□ □□□ □□□□□ □□□□ □□□□ □□ □ □□□□. □□ □ □□ □□□ □□ □□□ □□□□□ □□□□ □□□□ □ □□□ □ □ □ □□ □□□□□?
A. □□
B. Azure PowerShell
C. Azure CLI
D. □ □□ □□
Answer: D (LEAVE A REPLY)

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: 59
OpenVPN□ □□□□ Azure Point-to-Site(P2S) VPN□ □□□ □□□□□.
□□□□ □□□□□ Active Directory □□□□ □□ □□□□□.
VPN □□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□?
A. Azure Key Vault
B. RADIUS □□
C. □□ □□
D. Azure Active Directory(Azure AD) □□□□□□ □□□
Answer: B (LEAVE A REPLY)
AD Domain authentication allows users to connect to Azure using their organization domain credentials. It requires a RADIUS server that integrates with the AD server. Organizations can also leverage their existing RADIUS deployment.
https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#authenticate-using-active-directory-ad-domain-server

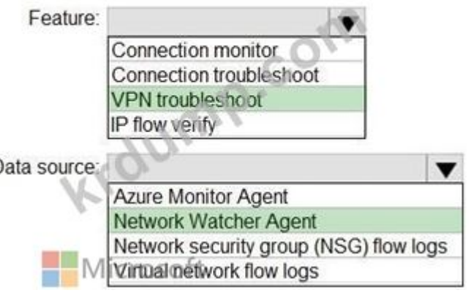
NEW QUESTION: 60
□□□ □□
VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□.
□□□□□ □□□□□ □□□ □(S2S) VPN □□□ □□□□ VNet1□ □□□□□.
VPN □□□ □□□ □□ Azure Network Watcher□□ □□□ □□□□□ □□ □□□.
□□□ □□□□□ □□ Network Watcher □□□ □□□□ □□, □□ □□□ □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



NEW QUESTION: 61

□□ □□ Azure □□□ □□ □□□□.

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

□ □□ □□□□□□ □□ IP □□□ □□□ □□□ □□ □□ □□□ 20□□ □□□□ □□□□.

□□□□ □□□□□ Azure DDoS □□□□ □□□ □□□□ □□□. □□□□ □□□ □□□□□ □□□.

□□□ □ □□ DDoS □□□□ □□ □□□ □□□□ □□□?

A. 1

B. 2

C. 3

D. 6
Answer: B (LEAVE A REPLY)
https://azure.microsoft.com/en-us/pricing/details/ddos-protection/

NEW QUESTION: 62
VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□. VNet1□□ Pool1□□□ Azure Virtual Desktop □□□ □□ □□□□ □□□□.
Pool1□□ □□□ □□ □□□□ □□ Azure Firewall□ TLS □□□ □□□□ □□□.
□□ □ □□□□ □□□□ □□□? □□□ □□ □□□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. Azure □□ DNS □□
B. □□ □□□□□
C. Azure □ □□□
D. Azure NAT □□□□□
E. Microsoft Enter □□□□□□ □
F. □□□□ ID
Answer: C,F (LEAVE A REPLY)
https://www.keytos.io/docs/azure-pki/azure-certificate-management/how-to-issue-tls-certificates-for-azure-firewall/

NEW QUESTION: 63
□□□ □ □□ □□
□□□ □□ Azure □□□□ Azure □□ □□(VM)□ □□□□ □□□ □□□□□□□ □□□□□□. □□□ VM□□ □□□□□ □□□ □□□□ □□□□. □□ □□□□ □□ □□(NSG)□ □□□□ □□ VM□ □□ □□□□ □□□□ □□□□.
□□□□□ □□□□ □□□□ □□□□ □□ □ □□ □□□ □□□□□ NSG □□ □□□ □□□□□□ □□□□□□.
□□ □ □□ □□□ □□ □□□? □□□ □□□□, □□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□□□.

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.

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: 64

□□□ □□

□□□ Azure □□□□ □□ □□ □□□ □□□ □□□□ □□□ □□□□ □□□□.

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

□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

□□□□ □□ □□ □□□ □□ □□□□ □□□□□□ □□□□ □□□□.

Name	Prefix	Default site
New York	10.9.0.0/16	Yes
Seattle	10.8.0.0/16	No

□ □□ □□□□ □□□□□ □□ □□□ □ VPN □□□ □□□□ □□□□.

□□ □ □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

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	◯	○

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: 65
□□ □□ 2 - □□□ □□□□
□□
□□□ □□□□□ □□□□□□□ □□□ □□ □□□□ □□□ □ □□□ □□□□□.
Contoso□ □□ Azure □□□ □□□□□ Azure□□ □ □□ □□ □□□□□ □□□□ □□□□.

□□ □□:

Azure □□□□ □□□

Contoso□ contoso.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. □□ Azure □□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

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□□ GW1□□□ □□□ □□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□ □□

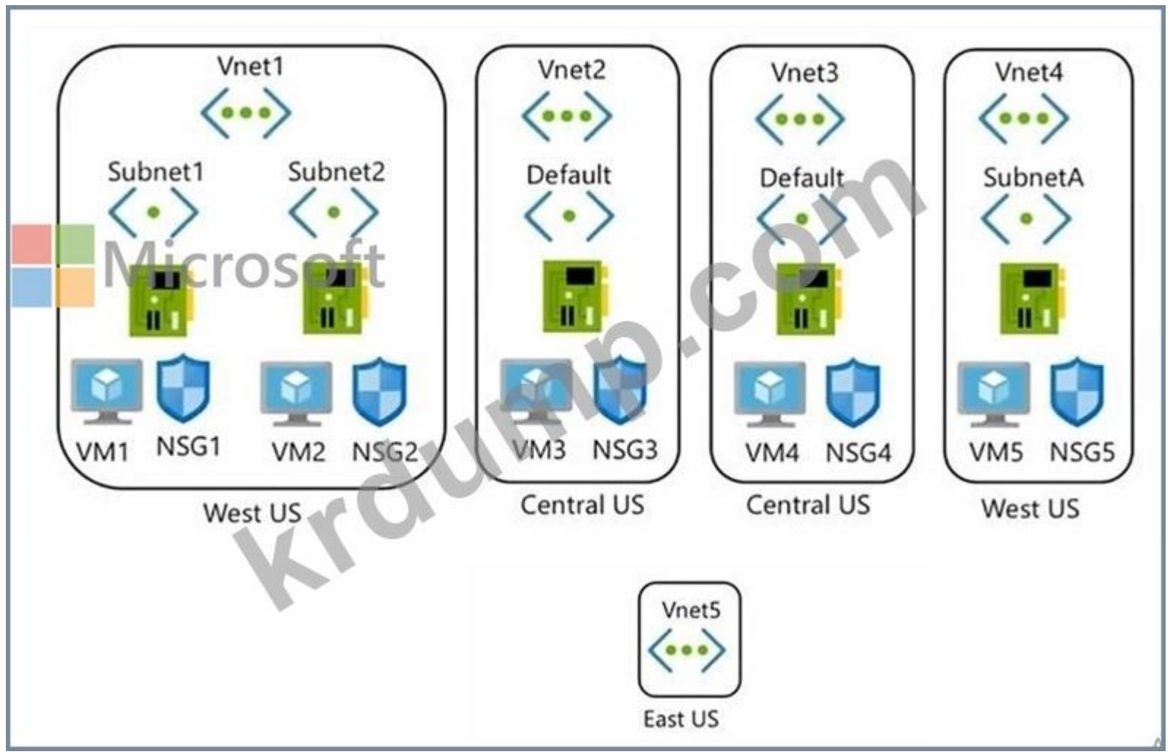
Azure □□□□ □□ □□ □□□ □□□ Windows Server 2019□ □□□□ □□ □□□ □□□□ □□□□.

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

NSG(□□□□ □□ □□)□ □□ □□□ □□□□ □□□□□□ □□□□ □□□□. □ NSG□□ □□□□□ RDP □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□□. □ □□ □□□ □□□□ ICMP □□□□ □□□□ □.

ASG1□□□ □□□□□□ □□ □□□ VM1□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□□□ □□□ □□□□□



Azure □□□□ DNS □□

Azure □□□□ □□ □□ □□□ Azure □□□□ DNS □□□ □□□□ □□□□.

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

Zone1.contoso.com□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

□□ Azure □□□

Azure □□□□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.

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

□□ □□:

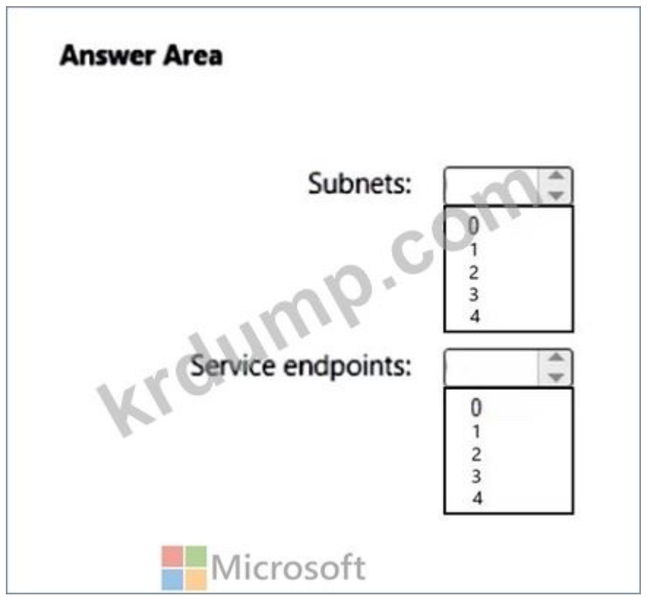
□□ □□□□ □□ □□
Contoso□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□.
- □□ □□ □□□ Vnet6□□□ □□□ □□ □□□□□ □□□□, □□ □□□□□ □□ □□□□ □□□ □□□□□□□.
Vnet6□ □□□□ □ □□ □□□□ □□
Vnet6□ □□□ □ □□ □□ □□
Vnet6□ □□ VPN □□ □□□ □□□□□.
Vnet6□ □□□□ KeyVault1, DB1 □ Vnet1□ □□□□ □ □□□ □□□□□.
□□□□□□□ □□ □□□□
- Vnet4□ Vnet5□ □□ □□□□ □□ □□□ □ □□□ □□□.
□□□□□□□ □□ □□□□□ □□.
- VM-Analyze□□ □□□ □□ □□□ Subnet1□ □□□□□. VM-
Analyze□ Subnet2□□ □□□ □□□□ □□□□ □□□□ □□□.
□□□.
□□□□ □□ □□ □□
Contoso□ □□□ □□ □□□□ □□ □□ □□□ □□□ □□□□.
- P2S(Point-to-Site) VPN □□□□ □□ Azure Active Directory(Azure AD) □□□ □□□□□.
- NSG3 □ NSG4□ □□ NSG □□ □□□ □□□□□□.
- Vnet1/Subnet1□ □□□ NSG10□□□ □□□ NSG□ □□□□□.
□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.
□□□.

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

- Vnet1/Subnet2□ □□□ NSG11□□□ □□□ NSG□ □□□□□.
□□□ □□ □□ □□□ □□□ □□ □□□□□ □□ □□□ □□□□□.

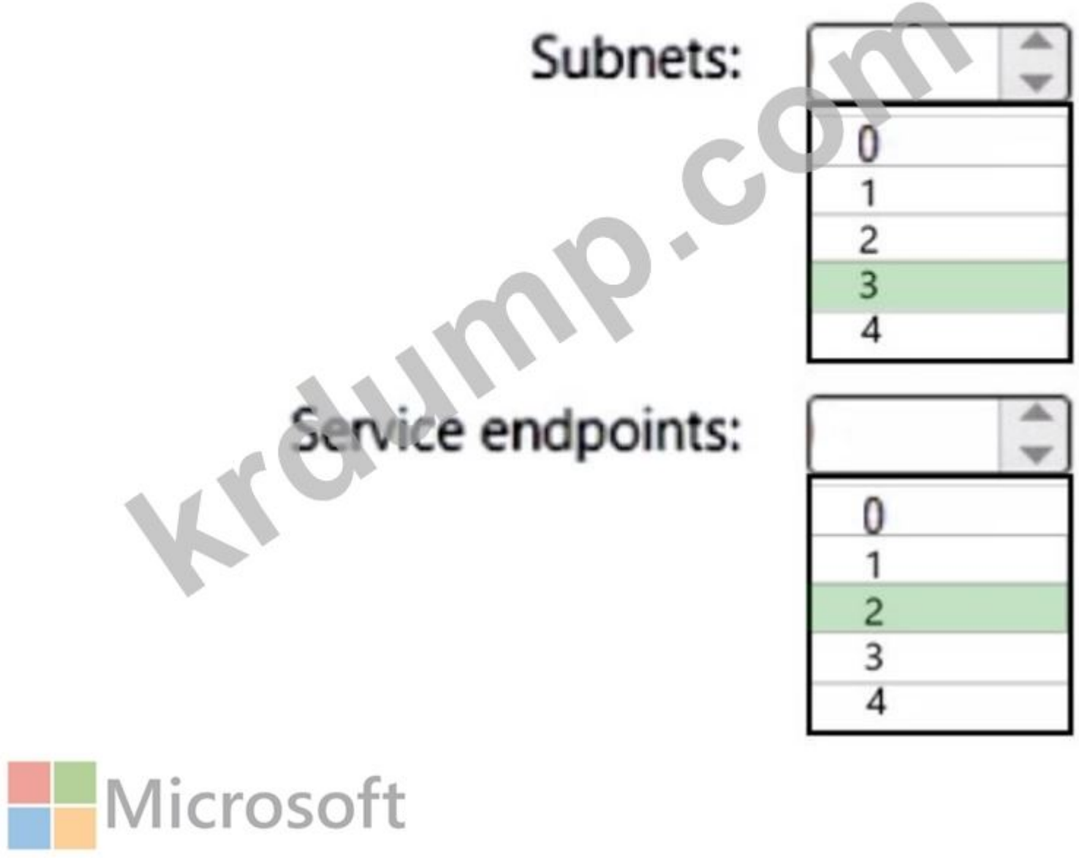
Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

□□□ □□
Vnet6□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□.
□□□□ □□ □□ □□□ □ □□□ □□□□□ □□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.


Answer Area
Subnets:
0
1
2
3
4
Service endpoints:
0
1
2
3
4
Microsoft

Answer:

Answer Area



Microsoft

NEW QUESTION: 66

Azure □□□ □□□□□□. □□ □□ □□□ □□□□ □□ □□□ □□□ □□□□□.

Name	Description
Vnet1	A virtual network
Subnet1	A subnet on Vnet1
App1	A multitier application that consists of frontend web servers, backend application servers, database servers, and search servers that all connect to Subnet1
NSG1	A network security group (NSG) associated to Subnet1

□□ □□ □□□ □□□□□ Rule1□□□ □□□ NSG1 □□□ □□□□ □□□.
- App1□ □□ □□□ □□ HTTP □□□ □□□ □ □□□ □□□□□.
□□□ □□□ □□.
- □□□ □□ □□□ □□□ □ □□ □□□ □□□□□□.
- □□ □□ □□□ □□□□□□.
Rule1□ □□□ □□□ □□□□ □□□?
A. □□□□□□ □□ □□
B. IP □□
C. □□□□
D. □□ □□□□
Answer: A (LEAVE A REPLY)
Adding the ip address of the search servers will have administrative overhead when deploying new search servers.

NEW QUESTION: 67
□□□ □□□□□ □□□□□ □□□□ □□□□.
□□ □□□□□ □□□ Azure □□□ □□□□.
ExpressRoute □□□ □□□□□ □□□□ □□□□.
ExpressRoute □□□ □□□□ Azure □□ □□□□□ □□□□□ □□□□□ □□□ □□□□□.
□□□ ExpressRoute □□□ □□□□□.
□ □□□ □□□□ □□□.
□□□ □□□□□ □□ □□□ □□□□ □□□?
A. IKEv2 □□ □
B. □□□
C. □□ IP □□
D. □□□ □
Answer: D (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings#circuits

NEW QUESTION: 68
500□□ □□ □□□□ □□ Azure Virtual Desktop □□□ □□□□. □□□□□ □□□ □□ □□□□□ □□□□ NAT □□□□□□ □□□□□.
□□□□ □□ □□□□ □□ □□□□ □□□ □□□□ □□□□ □ □□□ □□□□□. Azure Monitor□□ □□ □□ SNAT □□ □□□ □□□□□□.
□□ □□□ SNAT □□□ □□□ □□□.
□□□ □□ □□□?
A. □□ IP □□□ □□□□□.
B. NAT □□□□□□ □□ □□□□ □□□□□□.
C. □□□□□ □□□ □□ Azure Standard Load Balancer□ □□□□□.
Answer: A (LEAVE A REPLY)
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: 69

□□□ □□

□ □□ □□ □□□□ □□□□ Azure Front Door □□□□□ □□□□. □□ □ □□ www.contoso.com□□□ □□□ □□□ □□□□□.

□□ □□ □□□ □□□ □□ □□□□.

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

□□□□ □ □□□ □□ □□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

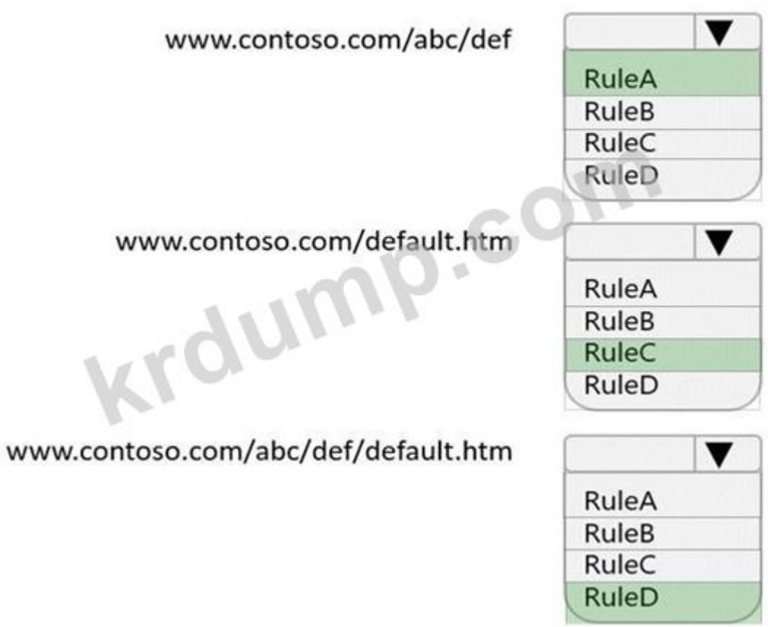
www.contoso.com/abc/def [RuleA / RuleB / RuleC / RuleD]

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

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

Answer:

Answer Area



Explanation:

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

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

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

https://docs.microsoft.com/en-us/azure/frontdoor/standard-premium/concept-route#path-matching

NEW QUESTION: 70

□□□ □□

□□□ Vnet1□□□ □□□ Azure □□ □□□□□ □□□□ □□□, □ □□□□□ □□ IP □□ □□□ □□□□□.

192.168.0.0/20. Vnet1□□ IP □□ □□□ □□□□ Subnet1□□□ □□□□ □□□□ □□□□.

192.168.0.0/24.

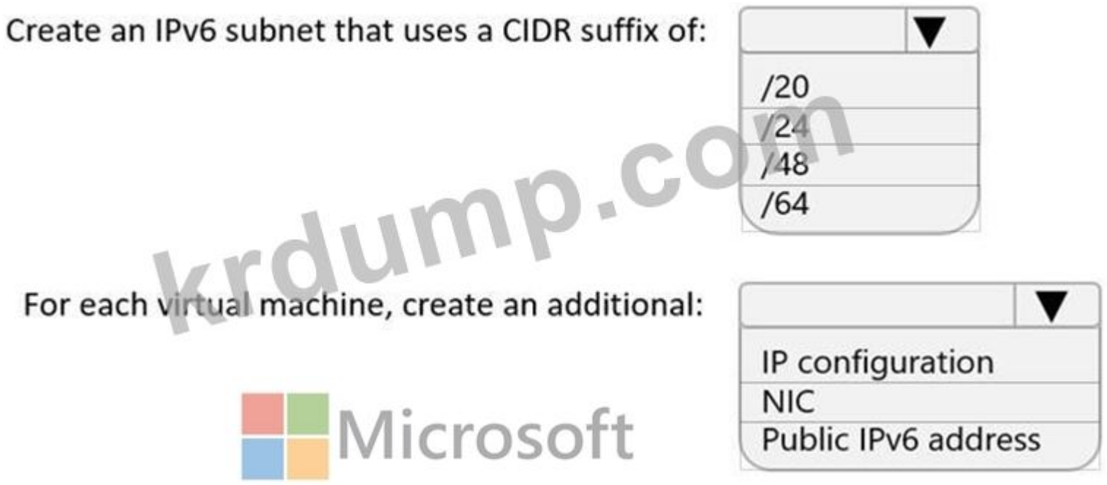
/48 CIDR □□□□ □□□□ Vnet1□ □□ IPv6 □□ □□□ □□□□□.

□□□1□ □□ □□ □□□□ □□□□ □□□ IPv6 □□□ □□□□ □□ □□□ □ □□□ □□□□ □□□. □ □□□□ □□ IPv4 □□□ □□ □□□□□ □□□.

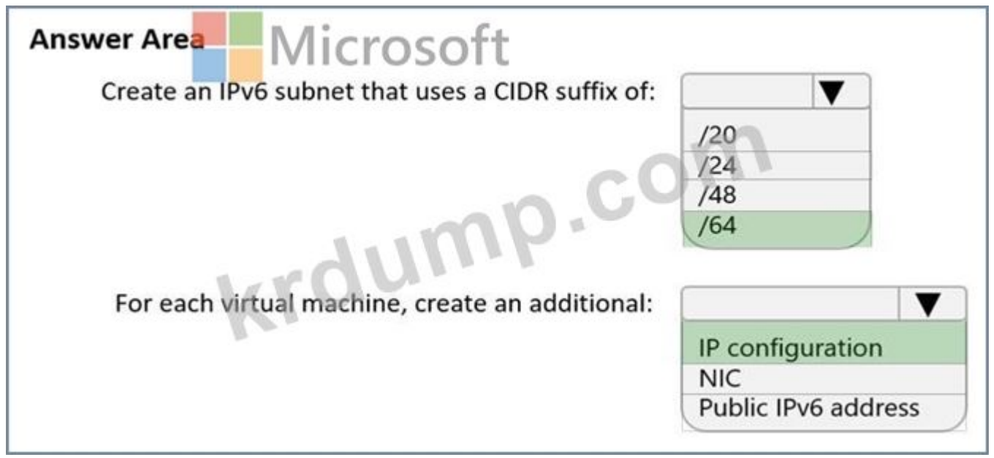
□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area



Answer:



Explanation:

You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. You can add a private IPv6 address to one secondary IP configuration (as long as there are no existing secondary IP configurations) for an existing network interface. Each network interface may have at most one IPv6 private address.

https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-network-interface-addresses

NEW QUESTION: 71

□□□ □□

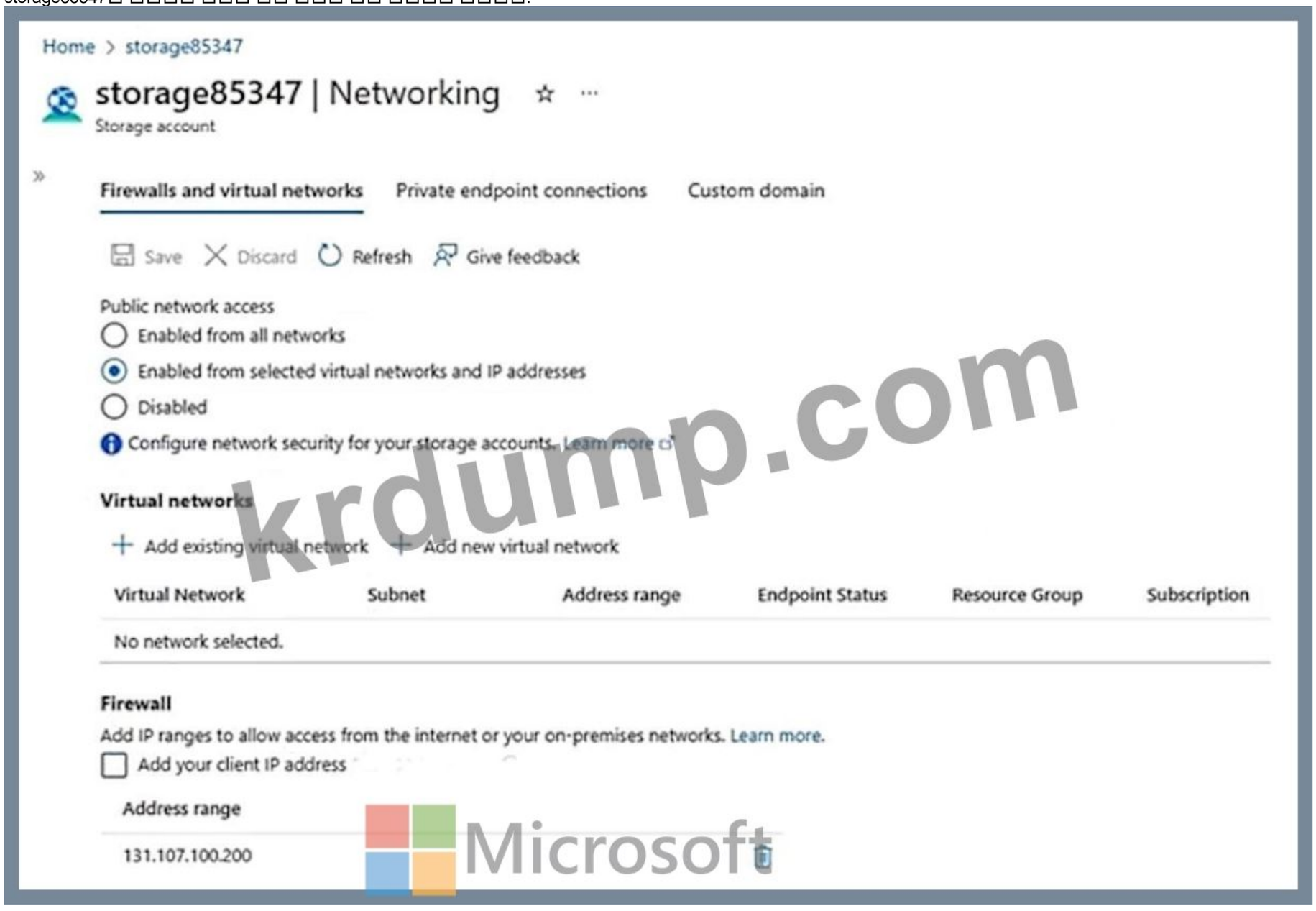
□□□ Server□□ □□□ □□□ □□□, □ □□□□ □□ IP □□□ □□□□ □□□□.

131.107.100.200.

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

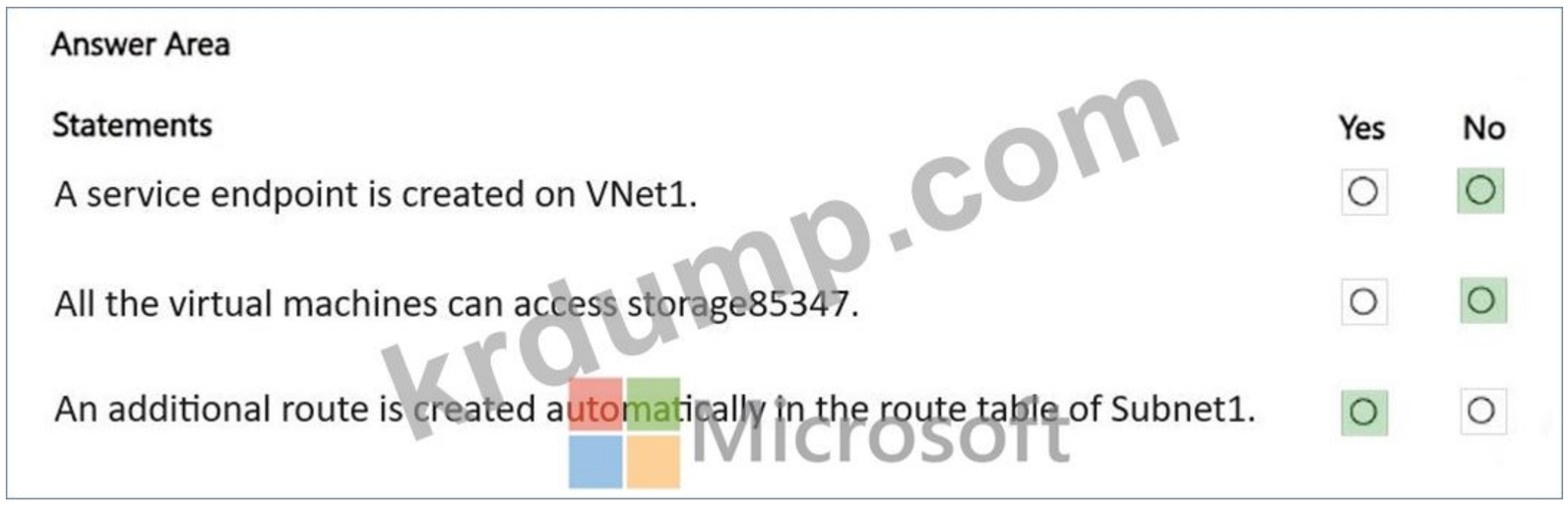
Name	Type	Description
storage85347	Storage account	Accessible from anywhere
VNet1	Virtual network	Contains two subnets named Subnet1 and Subnet2
Subnet1	Subnet	Contains 50 Azure virtual machines
Subnet2	Subnet	Contains 50 Azure virtual machines

storage85347□ □□□□ □□□ □□ □□□ □□ □□□□ □□□□.



□□□ □ □□ □□□□ □□□ Subnet1□ storage85347□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

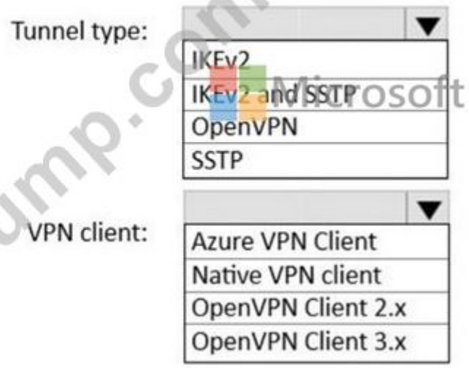


NEW QUESTION: 72
Azure Front Door□ Azure □ □□□□□□ □□□(WAF) □□□□□ □□□□.
□□ IP □□□□ □□□□ □□ □□ □□□ □□□□ WAF □□□ □□ □□□□□.
□□□ □□ □□□ □□□□ □□□□□ □□ □□ □□□ □□□□ □□□.
Log Analytics□□ □□ □□□□ □□□□ □□□?
A. AGWFirewallLogs
B. AZFWThreatIntel
C. AzureDiagnostics
D. □□ □□

Answer: C (LEAVE A REPLY)

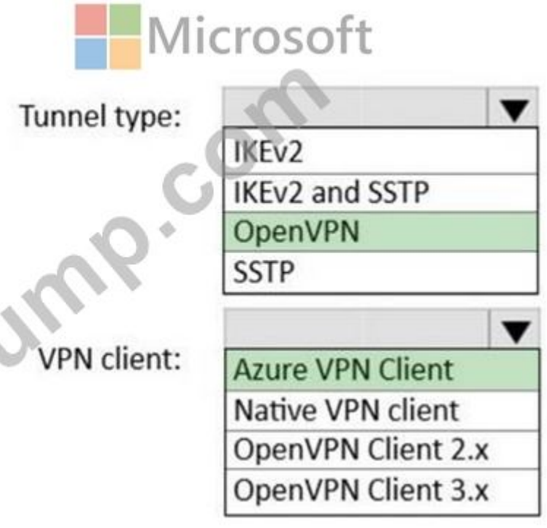
NEW QUESTION: 73
□□□ □□
□□□ VNet1□□□ □□ □□□□□ vGW1□□□ Azure VPN □□□□□□ □□□ Azure □□□ □□□□ □□□□.
□ □□□□ □□□ 11 □□□ □□□□ □□□□ 50□ □□□□.
□□□□ VNet1□ □□□□ □□□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□□□ P2S(Point-to-Site) VPN□ □□□ □ □□□ □□□□□□.
vGW1□ □□ □□.
- □□□□ Microsoft □□□□□ □□□ □ □□□ □□□□□□.
□□ □□□ □□□□□.
□□ □□□ □□□ □□□□ □□, □□□ □□□□ □□ VPN □□□□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



NEW QUESTION: 74

□□□ □□

Site1□ Site2□□ □ □□ □□□□□ □□□□ □□□□. □ □□□□ □□ □□□ □□□ □□□□ □□□□ □□□□□.

Azure □□□□ VNet1□ VNet2□□ □ □□ □□ □□□□□ □□□□ □□□□.

VNet1□ VNet2□ □□ □□ Azure □□□ □□□ □□ □□□□ □□□□ □□□□ □□□□ □□□□.

□□ □□ □□□ □□□□ □□□ □(S2S) VPN □□□□ □□□□ □□□.

- □□□1□ □□□2□ Azure □□□ □□ □□□□ □□□.

□□ □□□ □□□ □□□□□.

- □□□1□ □□□2□ □□□□ □□ □□□□□ □□□ □ □□□ □□□.

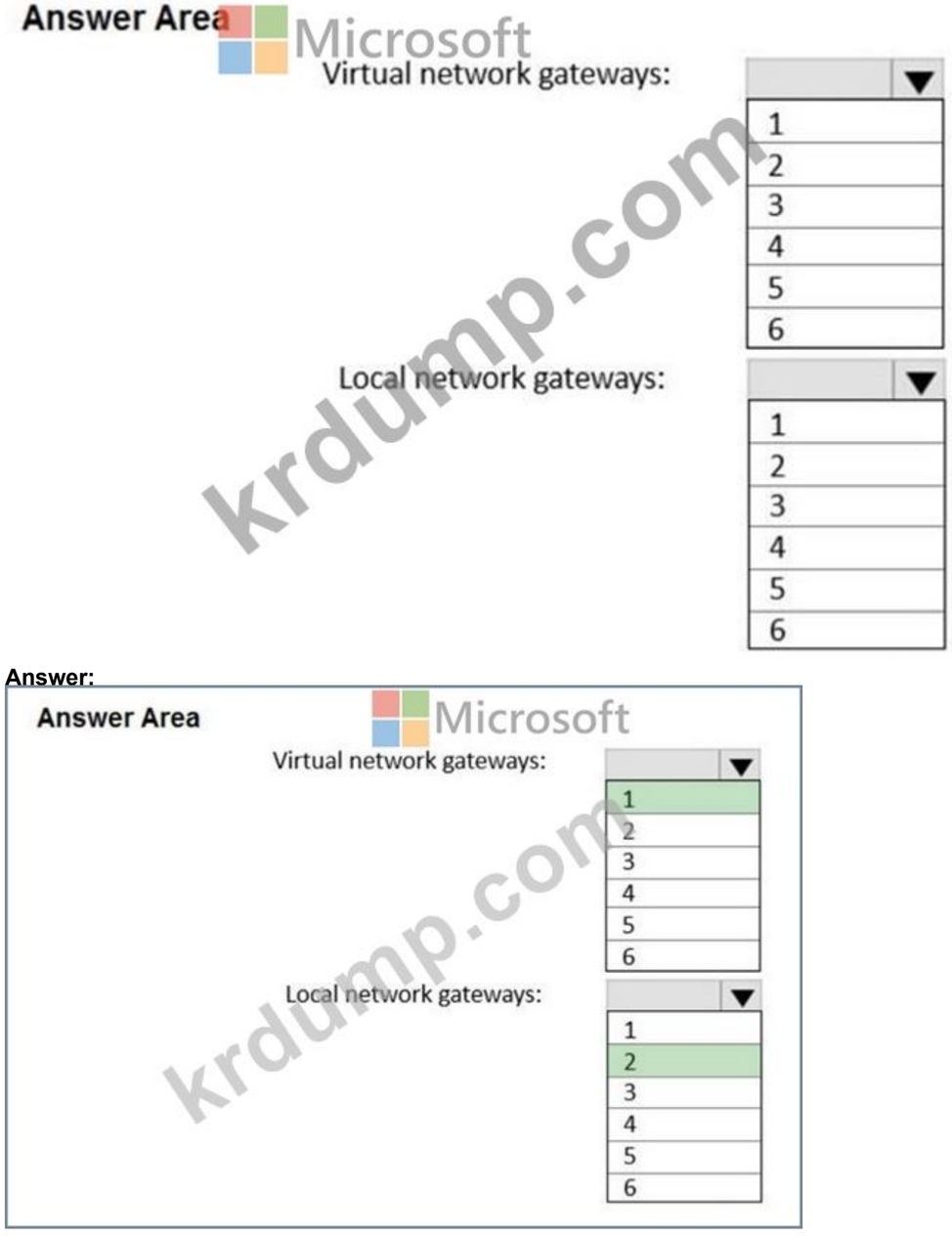
VNet1 □ VNet2□ □□□.

- □□□□□ 3□□ □□□□ □□□□ □□ □□□□ □□□□□□ □□□□□ □□□.

□□ □□.

Azure□ □□□□ □□ □□ □□ □□□□ □□□□□ □ □□ □□□□ □□□□□ □□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer:

NEW QUESTION: 75

ExpressRoute □□□ □□ □□□□ □□ MS □□□□ □□□□ □□□□□ □□□ □□ □□□ □□□ □□□□□. □□ □ ExpressRoute □□□ □□ □□□□ □□ □□ □□□□□?

A. ExpressRoute □□□ □□□ □□□ □□□□ □□□□.

B. ExpressRoute □□□ □□□ □(s-key)□ □□ □□□□ □□□ □ □□□□.

C. ExpressRoute □□□ □□□ □□ □□ □□ □ □□ □□□□ □□□□ □ □□□□.
D. ExpressRoute □□□ □□□ □□□ □□□ 1:1 □□□ □□□□□.
E. ExpressRoute □□□ S □ □□□□ 1:1 □□□ □□□□□.
Answer: A,B,E (LEAVE A REPLY)
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: 76
□□□ □□
□□ □□ □□□ □□□□ □□□□ Azure Front Door □□□ □□□□ □□□□.

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

□□□□ Front Door□ □□ URL□ □□□□ □ □□□□ □□□□□.
https://www.fabrikam.com.
www.fabrikam.com □□□ □□□ □□ □□□□ □□□□□□□□.
www.fabrikam.com□ □□ DNS □□□□ □□□□ □□□□ Azure□ □□□□□ □□□.
□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Answer Area

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

NEW QUESTION: 77
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type	Description
VNet1	Virtual network	*Not applicable*
FW1	Azure Firewall	Deployed to VNet1
SQLDB1	Azure SQL Database	Configured to only accept connections in Proxy mode Deployed to VNet1

VNet1□□ □□□□ SQLDB1□ FQDN□ □□□□ □□ □□□□ □□□□□□ FW1□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□?
A. DNAT
B. □□□□
C. □□ □□□□
D. □□□

Answer: C (LEAVE A REPLY)
Azure Firewall supports Application Rules to filter outbound traffic based on FQDNs.

NEW QUESTION: 78
□□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
- Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678

VNET1□□ □□ □□□□ □□□□ □□□□□ □□□□ □□□. □□□□ KQL□ □□□□ Azure □□□□ □□□□ □□□□ □□ □□□ □ □□□ □□□□ □□□.

□ □□□ □□□□□ Azure □□□ □□□□□□.

Answer:

Plan
Stage 1: Determine the resource group of VNET1
Stage 2: In Azure Monitor set up monitoring with the VNET's Resource Group as source, and Log Analytics workspace as destination

Stage 1: Determine the resource group of VNET1
Step 1: In Azure portal locate VNET1 and detect which resource group it is in (here we use XGroup).

Stage 2: In Azure Monitor set up monitoring with the VNET's Resource Group as source, and Log Analytics workspace as destination

Create diagnostic settings

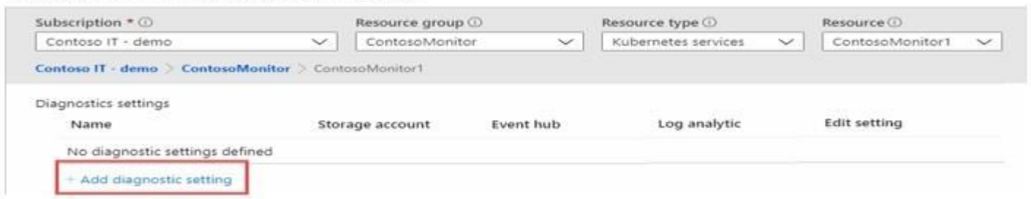
Step 2: You can configure diagnostic settings in the Azure portal either from the Azure Monitor menu or from the menu for the resource (XGroup in our case).

Where you configure diagnostic settings in the Azure portal depends on the resource:

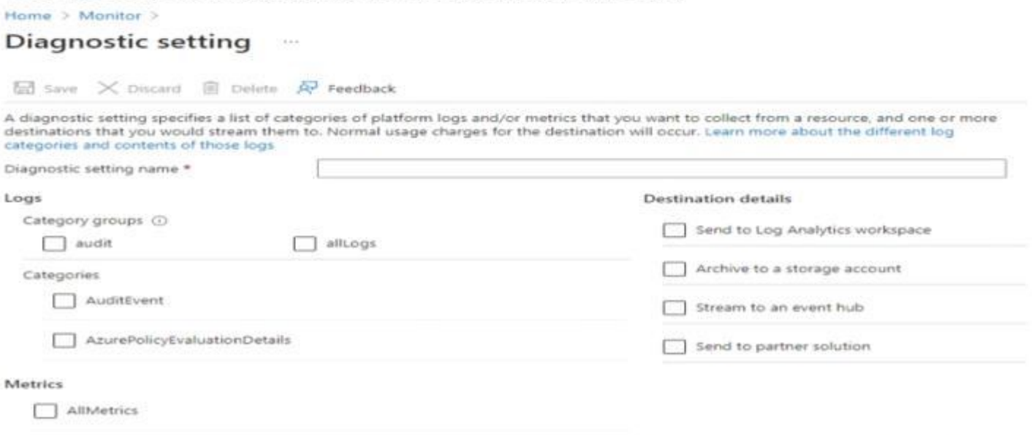
For a single resource, select Diagnostic settings under Monitoring on the resource's menu.

Step 3: If no settings exist on the resource you've selected, you're prompted to create a

setting. Select Add diagnostic setting.



Step 4: Give your setting a name if it doesn't already have one.



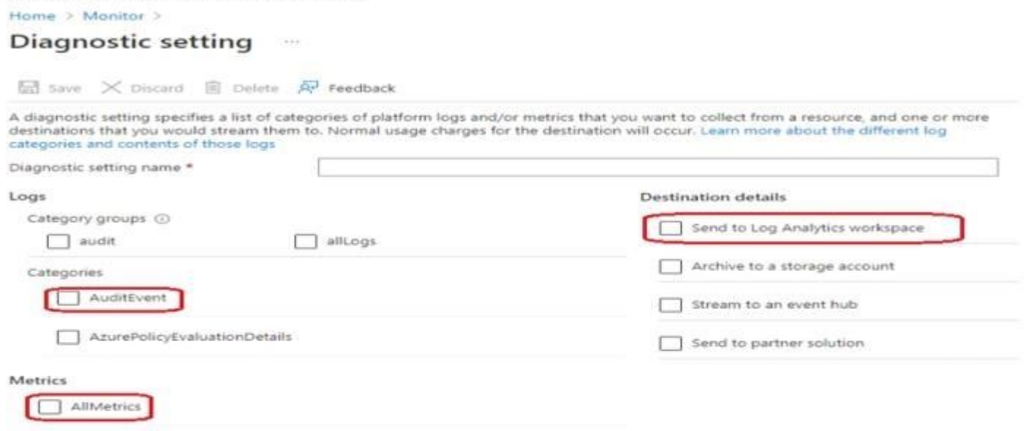
Step 5: Logs and metrics to route: For logs, either choose a category group or select the individual checkboxes for each category of data you want to send to the destinations specified later. The list of categories varies for each Azure service. Select AllMetrics if you want to store metrics in Azure Monitor Logs too.

We do the following:

Categories: Select AuditEvent

Metrics: Select AllMetrics
(to log all events and metrics)

Destination details: Select Send to Log Analytics workspace
(To be able to query using KQL)



Step 6: Destination details -skip

Step 7: Select Save.

Note: Azure virtual network collects the same kinds of monitoring data as other Azure resources.
Azure virtual network uses Azure Monitor.

Collection and routing
Platform metrics and the Activity log are collected and stored automatically, but can be routed to other locations by using a diagnostic setting.

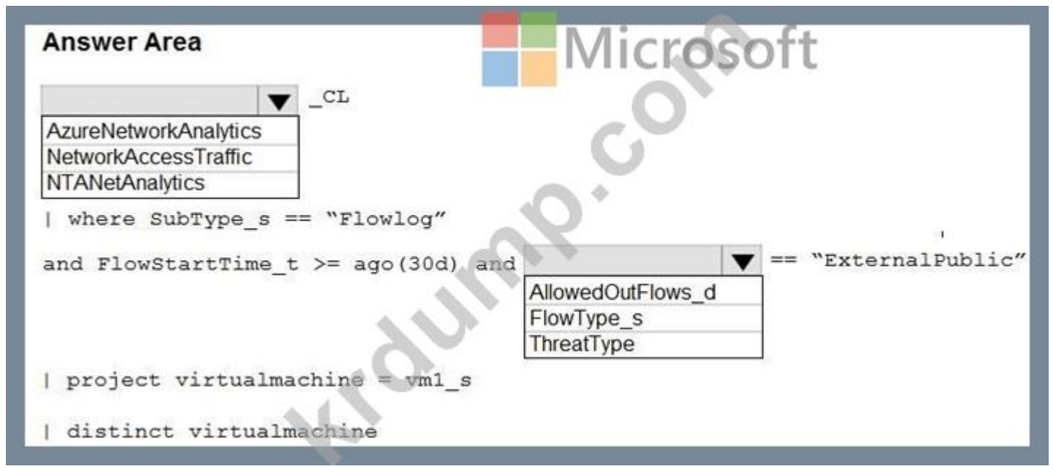
Each Azure resource requires its own diagnostic setting, which defines the following criteria:

Sources: The type of metric and log data to send to the destinations defined in the setting.
The available types vary by resource type.
Destinations: One or more destinations to send to.

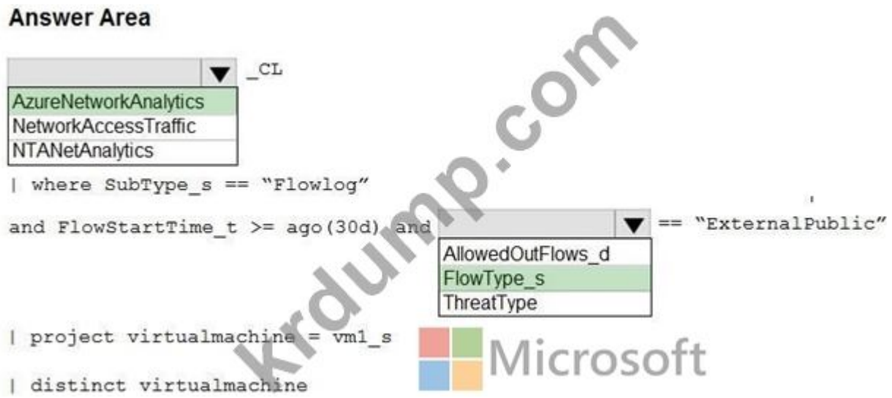
Destinations
Platform logs and metrics can be sent to the destinations listed in the following table.
* Log Analytics workspace
Metrics are converted to log form. This option might not be available for all resource types.
Sending them to the Azure Monitor Logs store (which is searchable via Log Analytics) helps you to integrate them into queries, alerts, and visualizations with existing log data.
* Etc.

Reference:
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings
https://learn.microsoft.com/en-us/azure/virtual-network/monitor-virtual-network

NEW QUESTION: 79
□□□ □□
□□□ 1,000□□ □□ □□□ □□□ Azure □□□ □□□□ □□□□.
□□□□ □□ □□(NSG) □□ □□□ □□□□□.
□□ 30□ □□ Azure □□ IP □□□ □□ □□ IP □□□ □□ □□□ □□ □□ □□□ □□□□ □□□.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics-schema?tabs=nsg#data-aggregation

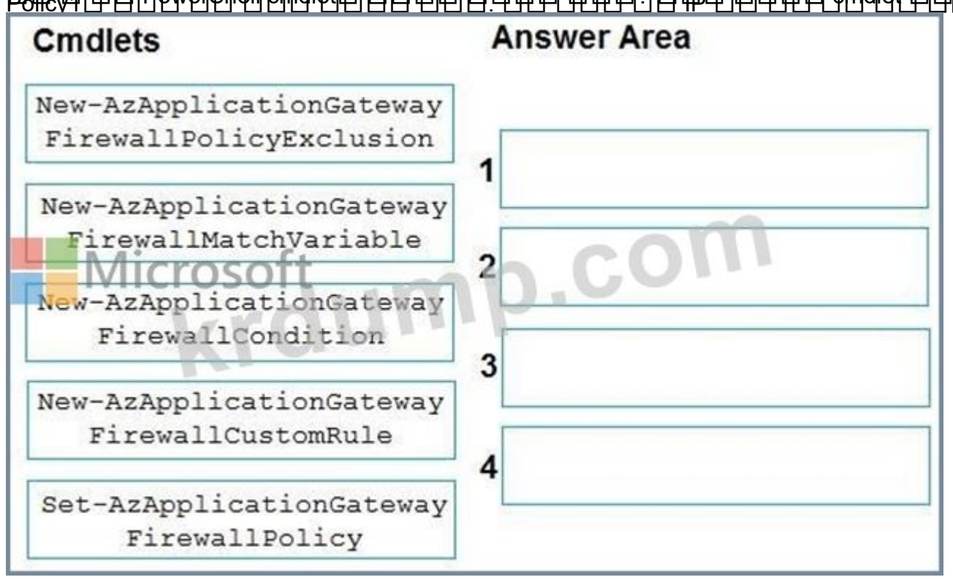
NEW QUESTION: 80

□□□ □ □□ □□

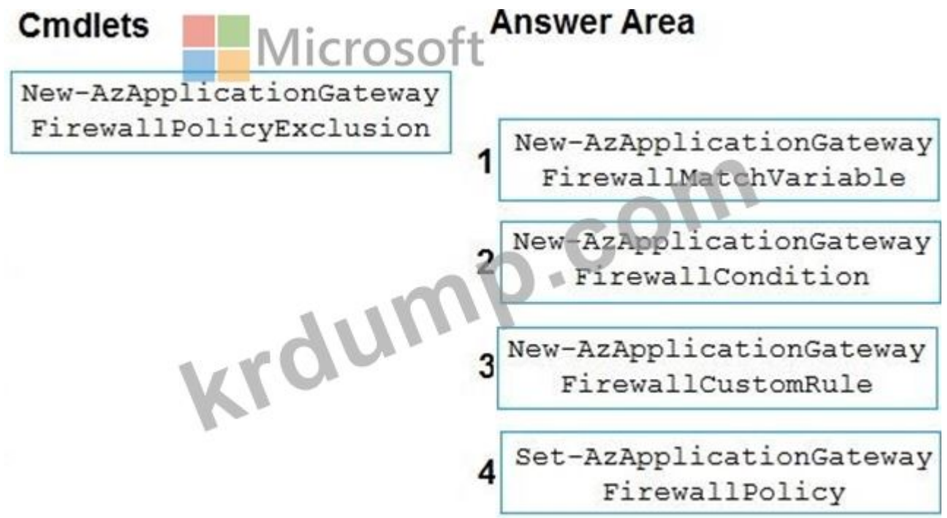
Azure □□□□□□ □□□□□□ AG1□□□ □□□ Azure □ □□□□□□ □□□(WAF) v2 □□□ □□□□. AG1□□ Policy1□□□ □□□ □□□ □□□□.

□□ □ □□ PowerShell cmdlet□ □□ □□□ □□□□ □□□□? □□ □□ □□□□ cmdlet □□□□ □□□ cmdlet□ □ □□□□ □□□ □□□ □□□□ □□□□□□.

Policy1□ □□□□ □□□ □□□ □□□□ □□□□. □□□ □□□□ □ IP □□ □□□ □□□□ □□□□ □□□□.



Answer:



NEW QUESTION: 81

□□: □ □□□ □□□ □□□□□□ □□□□ □□□ □□ □ □□□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.

Azure WAF(□ □□□□□□ □□□)□ □□□□ Azure □□□□□□ □□□□□□ □□□□.

□□□□□□ □□□□□□ □□□□ □□□□ □□□□□□ □□□□□□ URL□ □□□□□.

□□ URL□ □□□□□ □□ HTTP 403 □□□ □□□□□.□□ □□□ □□□□ □□□ □□ □□□ □□□□□□□.

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


□□□□□□ □□□□□□ □□ URL□ □□□ □ □□□ □□□□ □□□.
□□ □□: □□□ □□□ □□ □□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

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: 82

contoso.onmicrosoft.com□□□ Azure Active Directory(Azure AD) □□□□ □□□ Azure □□□ □□□□. □□ □□□□ □□ □□□□ □□□□ □□□□.

- App1□□□ Azure App Service □
- contoso.com□□□ Azure DNS □□
- private.contoso.com□□□ Azure □□ DNS □□
- Vnet1□□□ □□ □□□□

App1□ □□ □□ □□□□□□ □□□□. □□□□□□ □□ □□□□ Azure DNS□ □□□□ □□□□□.

Azure DNS□ □□□ □□ □□□□□ □□□ □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. app1.privatelink.azurewebsites.net
B. app1.contoso.com
C. app1.contoso.onmicrosoft.com
D. app1.private.contoso.com
Answer: A (LEAVE A REPLY)
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: 83
□□□ Azure □□□□ □□□ □□ □□□□ □□□□ □□□□.
- Vnet1□□□ □□□ □□ □□□□
- subnet1□ AzureFirewallSubnet□□□ □□□ □□□ □ □
- FW1□□□ □□□ □□ Azure □□□
- Subnet1□ □□□ RT1□□□ □□□ □□□ □□□
- RT1□□ 0.0.0.0/0□ FW1□□ □□□□□ □□
Windows Server□ □□□□ □□ 10□□ Subnet1□ □□□ □, □□ □□□ □□□ □□□□□ □□ □□ □□□□□□.
□□ □□□ □□□□ □ □□□ □□ □□□.
□□□ □□ □□□?
A. Subnet1□ □□ 1688□ □□ □□□□□ □□□□ □□□□ □□□□ □□ □□(NSG)□ □□□□□.
B. □□□□□ NAT □□□ □□ Azure □□ □□ □□□□ □□□□□.
C. FW1□□ Azure Key Management Service(KMS)□□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□□.
D. FW1□□ AzureCloud□ □□ □□□□□ □□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 84
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
□□ □□□□ □□□ Azure □□□ □□□□.

- Vnet1□□□ □□ □□□□
- Vnet1□ Subnet1□□□ □□□ □□□
- Subnet1□ □□□□ VM1□□□ □□ □□
- storage1, storage2, storage3□□□ □□□ □ □□ □□□□ □□

VM1□ storage1□ □□□□ □ □□□ □□□□ □□□. VM1□ □□ □□□□ □□□ □□□□□ □□□□ □□ □□□.
□□ □□: □□□□ □□ □□(NSG)□ □□□ NSG□ Subnet1□ □□□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

This just creates a network security group and associates it to Subnet1. Further configuration is required.

NEW QUESTION: 85

VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□. VNet1□ □□□ □□□□ /24□□□.
□□ □□□ □□ Azure □□□□□□ □□□□□□ □□□ □□□□□.

- □□ □□□□□: 1
- □□ □□□□□: 1
- □□ □□□□: 1
- □□ □□□□ □: 10

□□□□□□ □□□□□ □□□□ □□ □□□ □□□□ □□□. □□□□ □□□□□□ □□□□□ □□□□ □□□□ IP □□ □□ □□□□□ □□□.
□□ □□□ IP □□□ □□ □□ □□□□□?

A. 1

B. 2

C. 11

D. 12

E. 20

Answer: C (LEAVE A REPLY)

Application Gateway uses one private IP address per instance, plus another private IP address if a private frontend IP is configured.
https://learn.microsoft.com/en-us/azure/application-gateway/configuration-infrastructure#size-of- the-subnet

NEW QUESTION: 86

PL1□□□ Azure Private Link □□□□ □□□, □ □□□□ LB1□□□ Azure □□ □□□□ □□□□□.
PL1□ □ □□ □□ □□□□□ □□□□ □□□ □ □□□ □□ □□□.
□□□ □□ □□□?

A. LB1□ □□□□□ IP □□ □□ □□□□.

B. PL1□ □□□ NAT IP □□ □□ □□□□.

C. □□ NAT □□□□ Azure Application Gateway v2 □□□□□ □□□□□.

D. □□ SKU□ LB1□ □□□□□□.

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 87

□□□□□

□□□ □□□ □□□□

□□□ □□ □□ □□□ □□ □□□ □□□□□□.

- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx

Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

- □ □□□□: 12345678

VNET2□ VPN □□□□□□ ExpressRoute □□□□□□ □□□ □□□□□.

□□□□□□ □□□ □ □□□ VNET2□ □□□□ □□□.

□ □□□ □□□□□ Azure □□□ □□□□□□.

Configure ExpressRoute and Site-to-Site coexisting connections using the Azure portal
Step 1: In the Azure portal, search for and select virtual networks.

Step 2: On the Virtual networks page, select the virtual network you want to add a subnet to. Select the VNET2 virtual network

Step 3: On the virtual network page, select Subnets from the left navigation.

Step 4: On the Subnets page, select + Subnet.

Step 5: On the Add subnet screen, enter or select values for the subnet settings.

You can configure the following settings for a subnet:
* Name - The name must be unique within the virtual network.
* Subnet address range - The range must be unique within the address space and can't overlap with other subnet address ranges in the virtual network. You must specify the address space by using Classless Inter-Domain Routing (CIDR) notation.

The Gateway Subnet must be /27 or a shorter prefix (such as /26 or /25).

Specify: 10.0.0.0/27

Step 6: Select Save.

Reference:
https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet

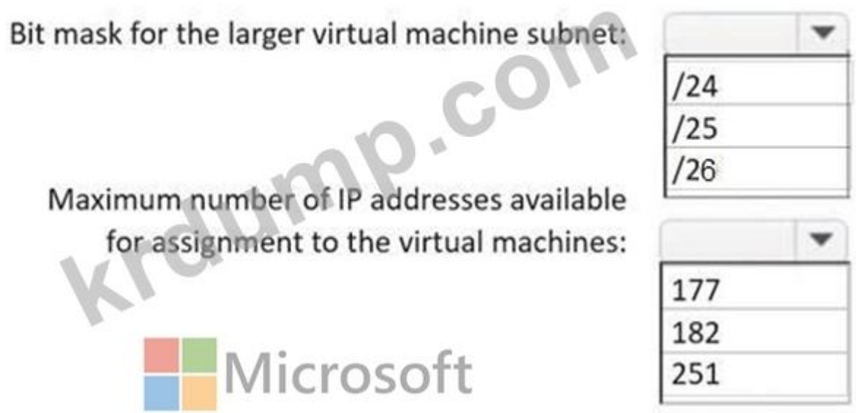
NEW QUESTION: 88
□□□ Azure □□□□ □□□ □□ □□□□ □□□□ □□□□.
- Vnet1□□□ □□□ □□ □□□□
- subnet1□ AzureFirewallSubnet□□□ □□□ □□□ □ □
- FW1□□□ □□□ □□ Azure □□□
- Subnet1□ □□□ RT1□□□ □□□ □□□ □□□
- RT1□□ 0.0.0.0/0□ FW1□□ □□□□□ □□

Windows Server□ □□□□ □□ 10□□ Subnet1□ □□□ □, □□ □□□ □□□ □□□□□ □□ □□ □□□□□□.
□□ □□□ □□□□ □ □□□ □□ □□□.
□□□ □□ □□□?
A. □□□□□ NAT □□□ □□ Azure □□ □□ □□□□ □□□□□.

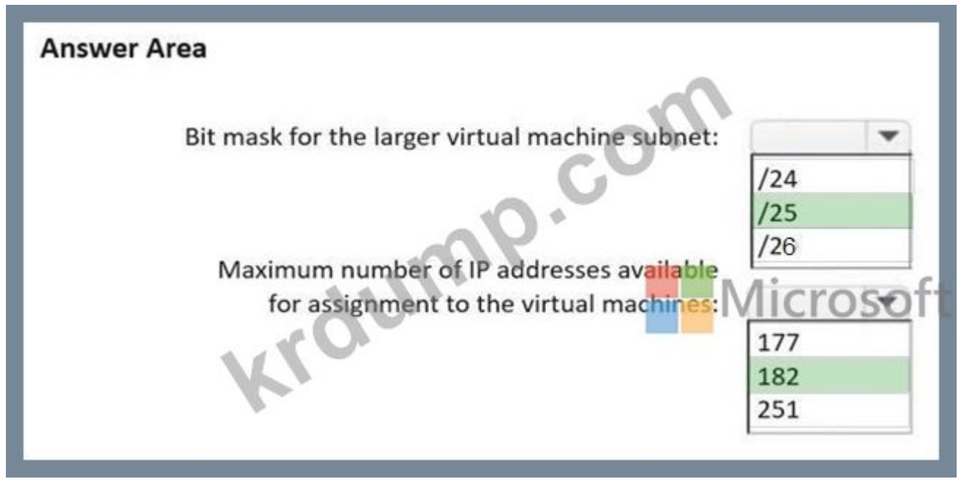
B. FW1□□ Azure Key Management Service(KMS)□□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□□.
C. NAT □□□□□□ □□□□□.
D. Subnet1□ □□ 1688□ □□ □□□□□ □□□□ □□□□ □□□□ □□ □□(NSG)□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
VM1□□□ Azure □□ □□□ □□□□.
Azure Network Watcher□ □□□□ VM1□ □□ □□□□ □□□□ □□□□ □□□.
□□ □□□ □□□ □ □ □□□?
A. VM1□□ □□ □□ □□
B. □□ □□ v2 □□ □□
C. Block blob □□□□ □□ □□
D. □□ □□ v2 □□ □ VM1□□ □□ □□ □□
E. □□ □□ v2 □□ □ Block blob □□□□ □□□ □□
F. Blob □□□, VM1□ □□ □□ □ Block Blob □□□□ □□
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: 90
□□□ □□
Azure □□□ VNet1□□□ □□ □□□□□ □□□□. VNet1□ 192.168.0.0/24 IP □□ □□□ □□□□□.
Azure □□ □□□ Azure Bastion□ VNet1□ □□□ □□□□□.
VNet1□ □□ IP □□□□ □□□ □□□□ □□□. □ □□□□ □□ □□□ □□□ □ □□ IP □□ □□ □□□□□ □□□.
□□ □□ □□□□□□□□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
Answer Area



Answer:



NEW QUESTION: 91

□□□ □ □□ □□

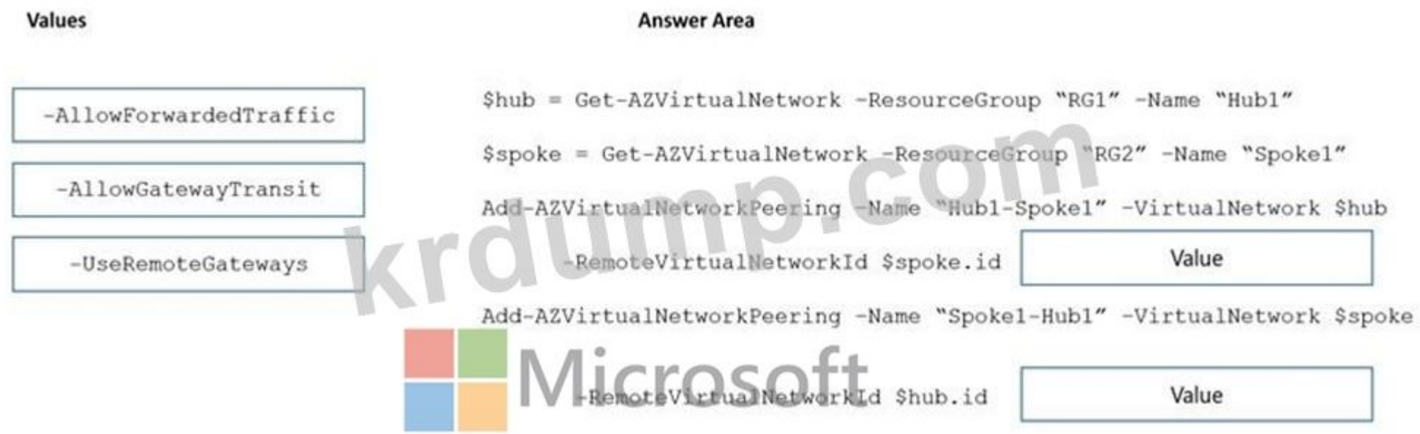
Hub1□ Spoke1□□□ □ □□ Azure □□ □□□□□ □□□□. Hub1□ □□□ □ VPN □□□ □□□□ □□□□□ □□□□□ □□□□□.

Hub1□ Spoke1 □□ □□□□ □□□□ □□□□.

Spoke1□ □□□ □□ □□□ Hub1□ □□ □□□□□ □□□□□ □□□ □ □□□ □□□□ □□□.

PowerShell □□□□□ □□□ □□□□ □□□? □□□ □□□ □□□ □□ □□□□□ □□ □□□ □□□□. □ □□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□ □□□ □ □□□ □□ □□□ □□□□□□ □ □□□□ □ □□ □□□□.

□□: □□ □□□ 1□□□□.



Answer:

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: 92

□□□ □□

Vnet1□□□ Azure □□ □□□□□ □□□, □ □□□□□□ Subnet1□ Subnet2□□ □ □□ □□□□ □□□□. □ □□□ □□ □□ □□□ □□□□ □□□□.

□□ □□□ □□ NATgateway1□□□ □□□ NAT □□□□□□ □□□□□.

Create network address translation (NAT) gateway ...

Validation passed

Basics | Outbound IP | Subnet | Tags | Review + create

Basics

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

Outbound IP

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

Subnets

Virtual network	Vnet1
Subnets	None

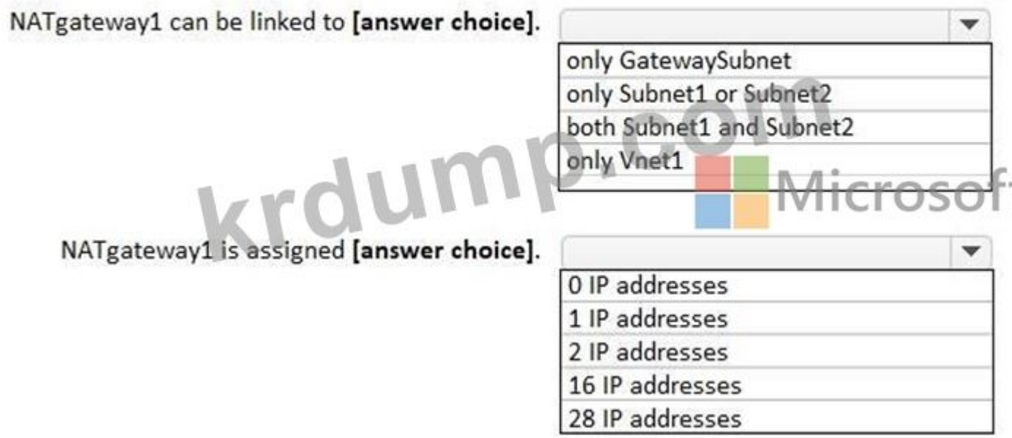
Tags

None

Create | < Previous | Next > | Download a template for automation

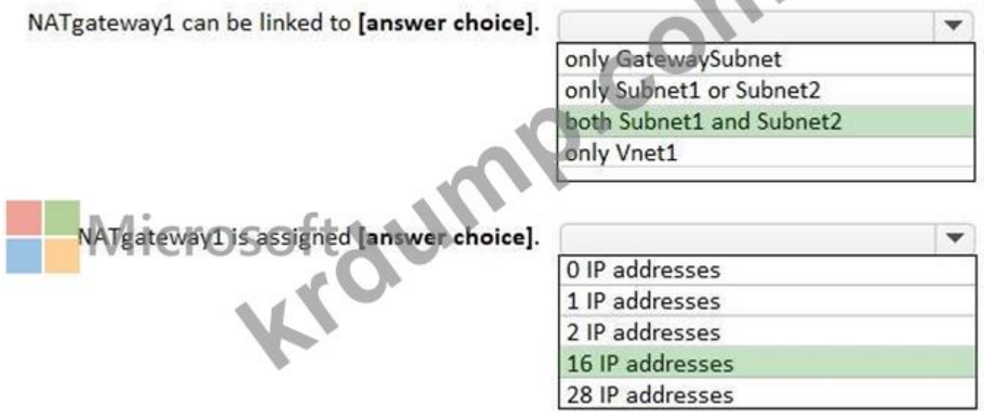
□□ □□□ □□□ □□□ □□□□ □ □□□ □□□□ □□ □□□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



Explanation:
NAT Gateway can be associated to multiple subnets as long as they are in the same VNET.
The (28) indicates that the public IP prefix is a /28, which allows 16 IP addresses.
https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/faq#can-nat-gateway-be-attached-to-multiple-subnets

NEW QUESTION: 93
□□ □ □□□ □□□□□ □□□□ □□□□. □ □□□□□ ExpressRoute □□□ □□ Azure□ □□ □□ □□□□□ □□□□ □□ □□□□□ □□□ □□□□□.

GW1□□□ □□□ Azure Application Gateway□ □□□, □ □□□□□□ □□□□□ □□ □□□□ □□□□□.
□□ □ □□□ □□□□□ Azure Virtual WAN□□ □□□□□□□ □□□□□.
□□ □□□□□ □□□□ □ □□ □□□ □□□□ □□□. □□□□ □□□□□ □□ □□□□ □□□□□ □□□□ □□□.
□□□□ □□□□ □ □ □□ □□ □□□ □□□□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. □□□ □□ □□□ □□□□□.
B. □□ □□□□ □□□□ □□□□□.
C. □□ □□□□□□ □□□□ □□□ □□ □□□ □□□□.
D. □□ □□□□ □□□ □□□□□.
E. □□ □□ □□□□ □□□□ □□□□□.
F. GW1□ □□□□□□.
Answer: C,D,E (LEAVE A REPLY)
Transition connectivity to virtual WAN hub:
Step 1. (E) Delete the existing peering connections from Spoke virtual networks to the old customer-managed hub. Access to applications in spoke virtual networks is unavailable until steps 1-3 are complete.
Step 2. (D) Connect the spoke virtual networks to the Virtual WAN hub via VNet connections.
Step 3. (C) Remove any user-defined routes (UDR) previously used within spoke virtual networks for spoke-to-spoke communications. This path is now enabled by dynamic routing available within the Virtual WAN hub.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology

NEW QUESTION: 94
□□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
- Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.

- □ □□□□: 12345678
Azure □□ □□□□□□ www.relecloud.com□ □□ □□□ frontdoor1.azurefd.net□□ □□□□□ □□ □□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.

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

NEW QUESTION: 95
□□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678
subnet1-□ □□ □□□□□ storage35433841 □□□□ □□□ □□ □□□ □□□□ □□□.
2□□ □□□ □□□ □ □□□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.

Answer:

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

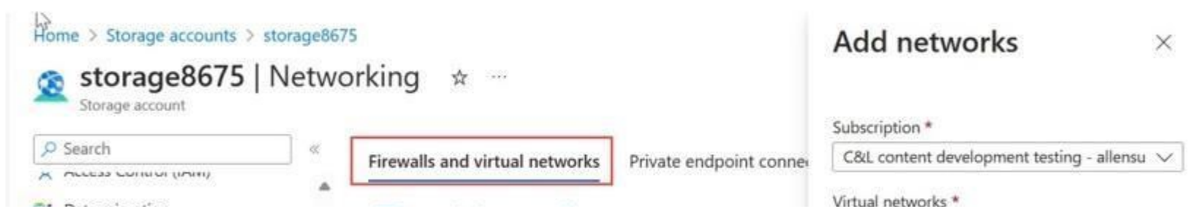
Step 3: In Security + networking, select Networking.

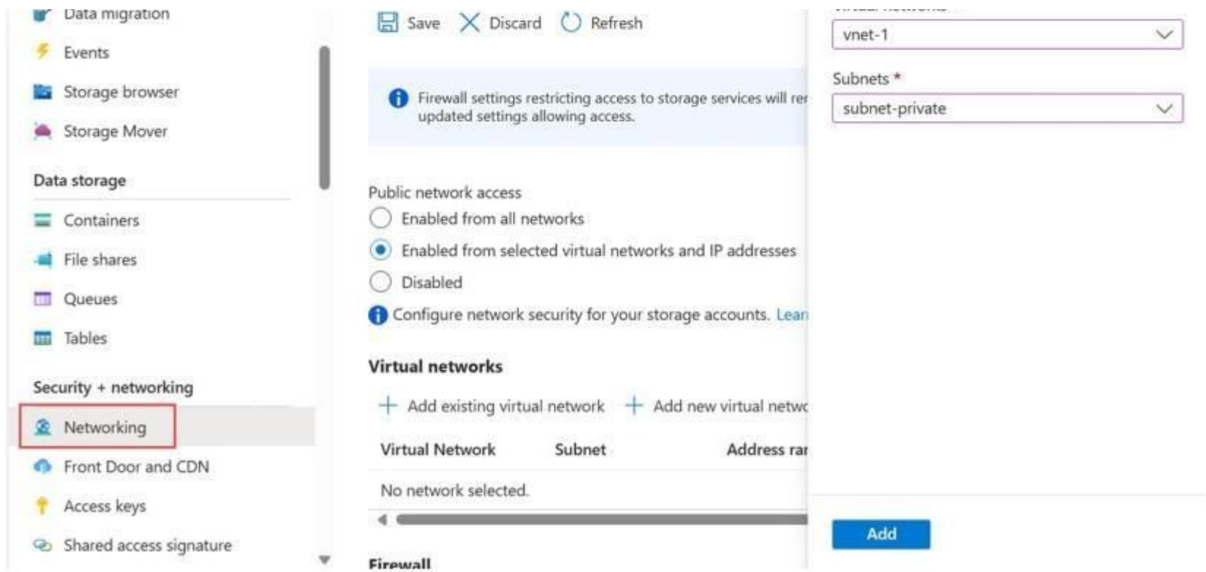
Step 4: In the Firewalls and virtual networks tab, select Enabled from selected virtual networks and IP addresses in Public network access.

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

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

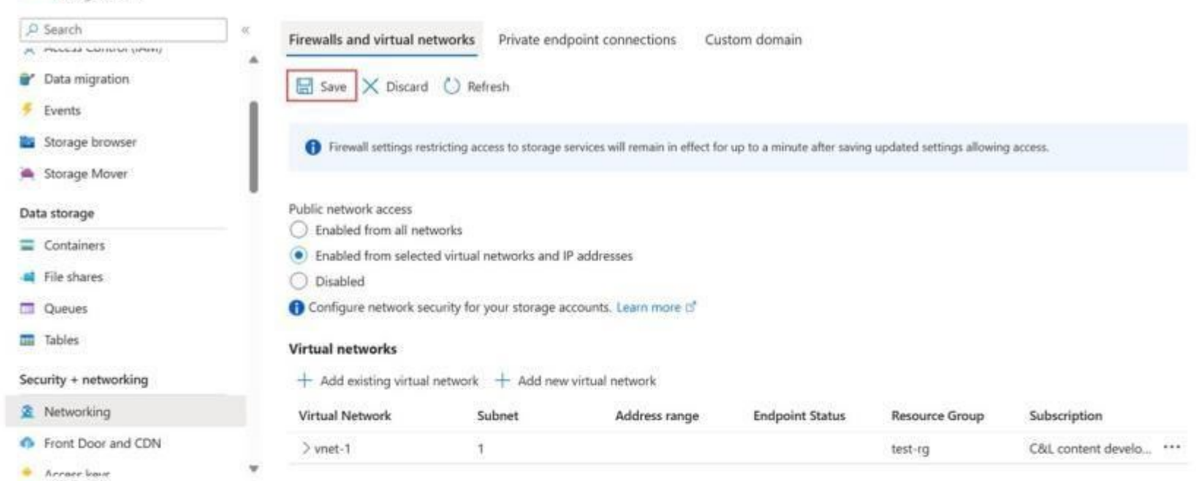
Setting - Value
Subscription: Select your subscription.
Virtual networks: Select the available virtual network
Subnets: Select subnet1-2.





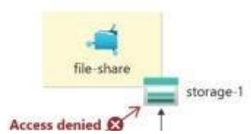
Step 7: Select Add.

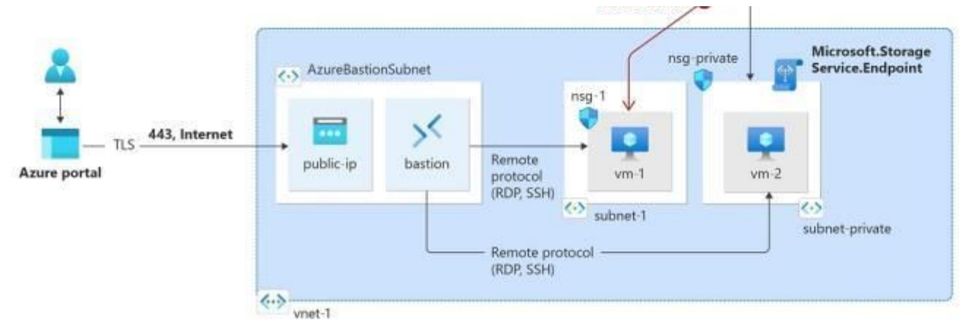
Step 8: Select Save to save the virtual network configurations.



Note: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal

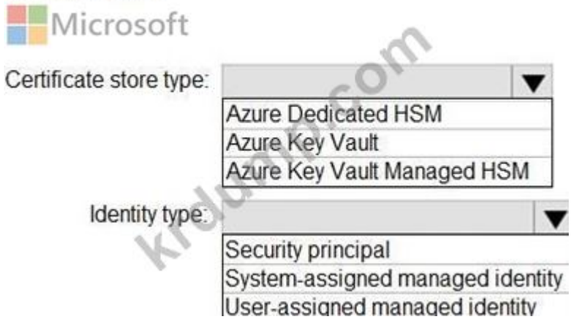
Note: Virtual network service endpoints enable you to limit network access to some Azure service resources to a virtual network subnet. You can also remove internet access to the resources. Service endpoints provide direct connection from your virtual network to supported Azure services, allowing you 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.



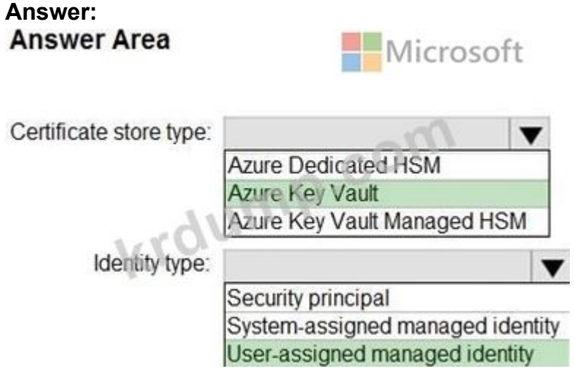


Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources

NEW QUESTION: 96
□□□ □□
Azure □□□ □□□□ □□□□.
AGW1□□□ □□□ Azure □□□□□□ □□□□□□ □□□ □□□□□.
AGW1□ □□ TLS □□□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□ □□□ □□ □□□ □□□ □□□□ □□□□ □□□.
- □□□ □□□ □□□□□□ □□□.
□□ □□□ □□□ □□□□ □□□□ □□, □□□□ □□□□ □□ □□ □□□ IDD □□□□ □□□? □□□ □□□□□ □□ □□□□ □□□ □□□ □□□□□□. □□: □ □□□ 1□□□□.
Answer Area



Answer:
Answer Area



NEW QUESTION: 97

□□ □□ 2 - □□□ □□□□

□□

□□□ □□□□□ □□□□□□□ □□□ □□ □□□□ □□□ □ □□□ □□□□□.

Contoso□ □□ Azure □□□ □□□□□ Azure□□ □ □□ □□ □□□□□ □□□□ □□□□.

□□ □□:

Azure □□□□ □□□

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**

□ □□□□. □□ Azure □□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

Vnet1□□ GW1□□□ □□□ □□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□ □□

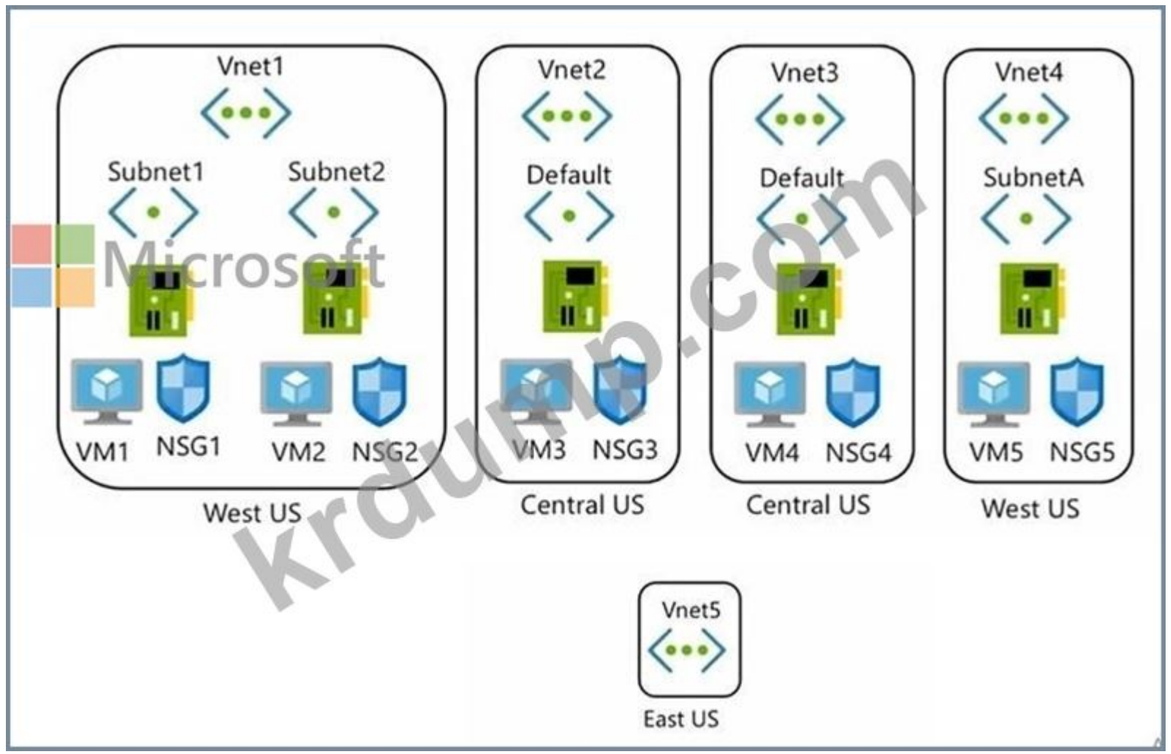
Azure □□□□ □□ □□ □□□ □□□ Windows Server 2019□ □□□□ □□ □□□ □□□□ □□□□.

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

NSG(□□□□ □□ □□)□ □□ □□□ □□□□ □□□□□□ □□□□ □□□□. □ NSG□□ □□□□□ RDP □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□□. □ □□ □□□ □□□□ ICMP □□□□ □□□□ □.

ASG1□□□ □□□□□□ □□ □□□ VM1□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□□□ □□□ □□□□□



Azure □□□□ DNS □□

Azure □□□□ □□ □□ □□□ Azure □□□□ DNS □□□ □□□□ □□□□.

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

Zone1.contoso.com□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

□□ Azure □□□

Azure □□□□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.

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

□□ □□:

□□ □□□□ □□ □□
Contoso□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□.
- □□ □□ □□□ Vnet6□□□ □□□ □□ □□□□□ □□□□, □□ □□□□□ □□ □□□□ □□□ □□□□□□□.
Vnet6□ □□□□ □ □□ □□□□ □□
Vnet6□ □□□ □ □□ □□ □□
Vnet6□ □□ VPN □□ □□□ □□□□□.
Vnet6□ □□□□ KeyVault1, DB1 □ Vnet1□ □□□□ □ □□□ □□□□□.
□□□□□□□ □□ □□□□
- Vnet4□ Vnet5□ □□ □□□□ □□ □□□ □ □□□ □□□.
□□□□□□□ □□ □□□□□ □□.
- VM-Analyze□□ □□□ □□ □□□ Subnet1□ □□□□□. VM-
Analyze□ Subnet2□□ □□□ □□□□ □□□□ □□□□ □□□.
□□□.
□□□□ □□ □□ □□
Contoso□ □□□ □□ □□□□ □□ □□ □□□ □□□ □□□□.
- P2S(Point-to-Site) VPN □□□□ □□ Azure Active Directory(Azure AD) □□□ □□□□□.
- NSG3 □ NSG4□ □□ NSG □□ □□□ □□□□□□.
- Vnet1/Subnet1□ □□□ NSG10□□□ □□□ NSG□ □□□□□.
□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.
□□□.

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

- Vnet1/Subnet2□ □□□ NSG11□□□ □□□ NSG□ □□□□□.
□□□ □□ □□ □□□ □□□ □□ □□□□□ □□ □□□ □□□□□.

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

□□□ □□
ASG1□ □□ NSG□□ □□□ □ □□□, □□ □□ □□ □□□□ □□□□□□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

NSGs:

- NSG1 only
- NSG1 and NSG2 only
- NSG1, NSG2, and NSG5 only
- NSG1, NSG2, NSG4, and NSG5 only
- NSG1, NSG2, NSG3, NSG4, and NSG5

Virtual machines:

- VM2 only
- VM2 and VM5 only
- VM2, VM4, and VM5 only
- VM2, VM3, VM4, and VM5

Answer:

Answer Area

NSGs:

- NSG1 only
- NSG1 and NSG2 only
- NSG1, NSG2, and NSG5 only
- NSG1, NSG2, NSG4, and NSG5 only
- NSG1, NSG2, NSG3, NSG4, and NSG5

Virtual machines:

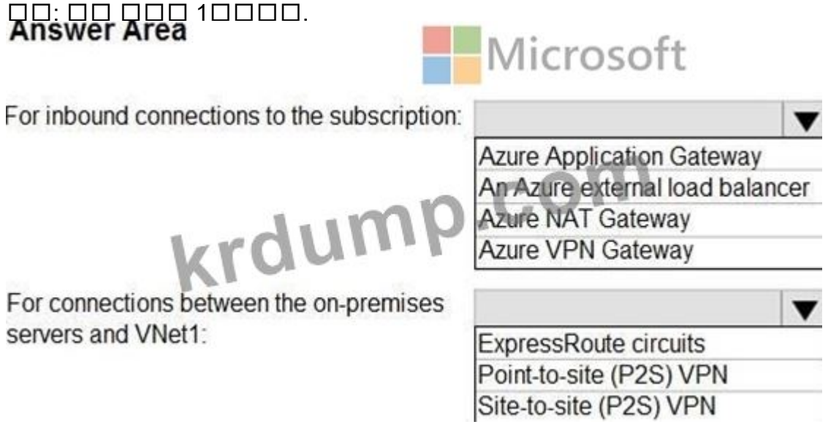
- VM2 only
- VM2 and VM5 only
- VM2, VM4, and VM5 only
- VM2, VM3, VM4, and VM5

Explanation:
Box 1: NSG1 and NSG2 only
NSG5 also is out of the question:

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.
Box 2: VM2 Only
Network interfaces attached to an ASG must be in the same vNet.
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

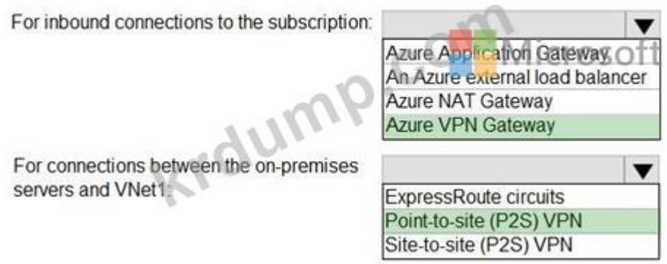
NEW QUESTION: 98
□□□ □□□ □□ □□□□□ □□□ □□□ □□□□ □□□□. □□ □□ Azure □□□ □□□ □□□ □□□□□.
□ □□□ □□ □□ □□□□ Azure □□□□ □□□□ □□□□.
□□ 1Gbps□ □□□□□ ExpressRoute□ □□□□ □□□. ExpressRoute Unlimited □□□ □□□□ □□□□ □□□. □□□□ □□□ □□□□□ □□□.
□□ □□□ ExpressRoute □□□ □□□□ □□□?
A. ExpressRoute □□
B. □□□□□□□ □□□□
C. ExpressRoute □□□□
D. ExpressRoute □□
Answer: (SHOW ANSWER)
ExpressRoute local, standard, global offer unlimited data plans.
ExpressRoute local: access azure region locally
ExpressRoute Standard: access azure multiple regions within a geopolotical location.
ExpressRoute Global: access azure regions globally/all over the world
https://docs.microsoft.com/pl-pl/azure/expressroute/expressroute-faqs#what-is-expressroute-local

NEW QUESTION: 99
□□□ □□
□□□□ 50□□ □□ □□□□□ □□□□. □ □□□□□□ Windows Server□ □□□□ □□□ □□□ □□□□.
Azure □□□ VNet1□□□ □□ □□□□□ □□□□. VNet1□□ DB1□□□ □□□□□□ □□□ □□□□.
□□□□□ □□□□ □□□□□ Azure □□□□ □□□□ □□□□ DB1□ □□□□ App1□□□ □□ □□□ □□□□□.
VNet1□ □□ Azure □□□□ □□□ □□□ □□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.
Answer Area



Answer:

Answer Area



Explanation:

https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/azure/use-azure-network-adapter

NEW QUESTION: 100

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

VM1□□ □□□□□ □□ azsql1.database.windows.net□ □□ □□□□□ IP □□□ □□□ □ □□□ □□□□ □□□.

□□□ □□ □□□□ □□□?

A. database.windows.net□□□ □□□ □□ DNS □□

B. database.windows.net□□□ □□□ □□ DNS □□

C. privatelink.database.windows.net□□□ □□□ □□ DNS □□

D. privatelink.database.windows.net□□□ □□□ □□ DNS □□

Answer: D (LEAVE A REPLY)

The private link resource type is a SQL database, therefor the recommended private DNS zone name is privatelink.database.windows.net.

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#azure-services-dns-zone-configuration

NEW QUESTION: 101

□□□ □ □□ □□

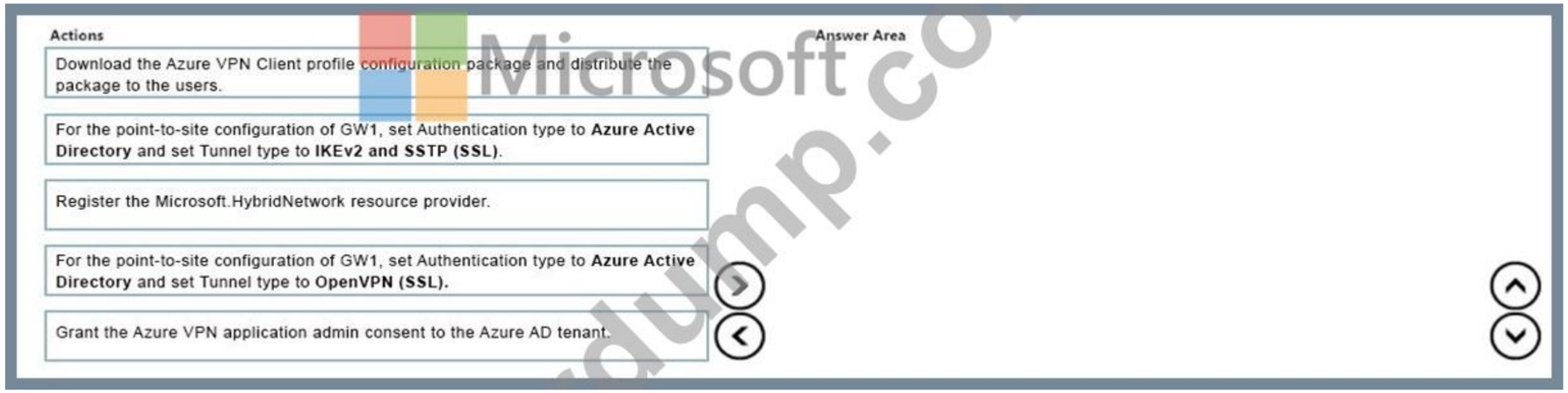
GW1□□□ Azure VPN □□□□□□ □□□ Azure □□□ □□□□. GW1□ P2S(Point-to-Site) VPN □□□ □□□□□.

□□□□ SSTP □□□ □□□□ Windows 11 □□□□ GW1□ □□□□□.

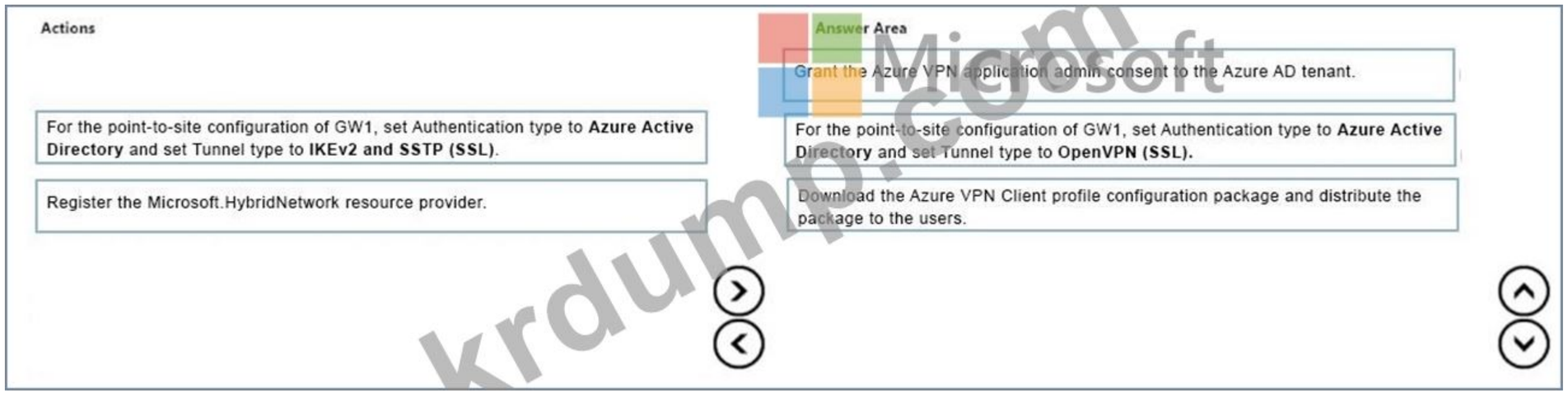
P2S VPN □□□ Azure AD □□□ □□□□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.

□□: □□□ □□ □□□ □□ □ □□□□. □□ □□□ □□□□ □□□□ □□□□□.



Answer:



NEW QUESTION: 102

□□□□□ □□□□□ Azure□ □□□□ □□ ExpressRoute□ □□□□ □□□□□ □□□ □□□□.

Azure □□ □□□ □-□□□□ □□ □□□ □□□□ □□□ □□ □□□ □□ □□□ □□□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. Azure □□□

B. IP □□ □□

C. □□ □□□

D. Azure □□□ □□□

Answer: C (LEAVE A REPLY)

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: 103

□□□ □□
□□□ Azure □□□□ AGW1□□□ □□□ Azure □□□□□□ □□□□□□ □□□□ □□□□.
AGW1□ □ □□□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□□.
- □□: https://www.contoso.com/fashion/shirts
- □□:
https://www.contoso.com/buy.aspx?category=fashion&product=shirts
□□□ □□□ □□□ □□ □□□ □□ □□□.
- □□□ □□ □□: □□ □□
- □□□□ □□: □□□
- □□□: □□(=)
□□ □□□ □□□ □□□ □□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.
□□: □□ □□□ 1□□□□.

Answer Area

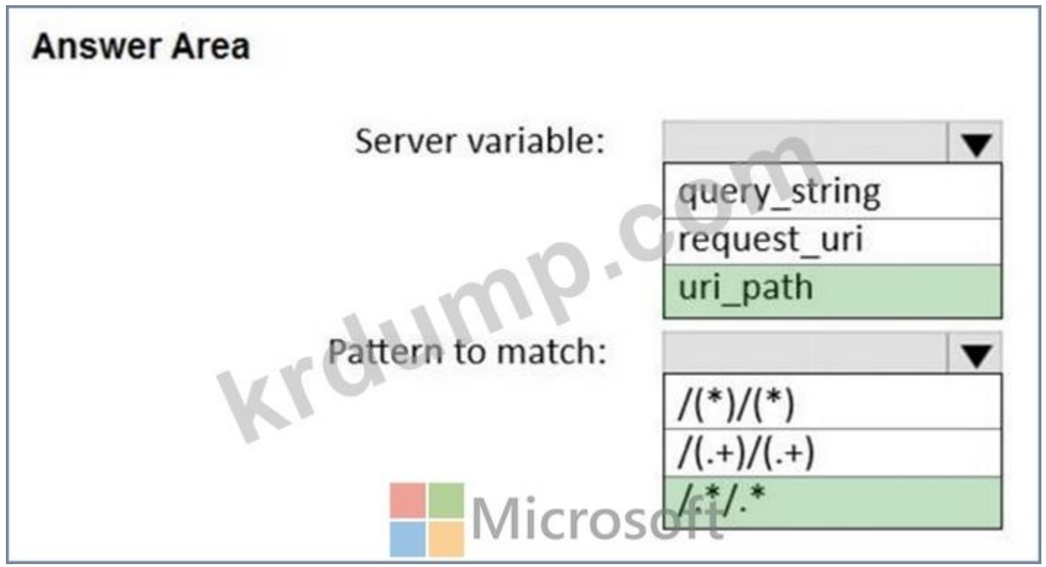
Server variable:

query_string
request_uri
uri_path

Pattern to match:

/(*)/(*)
/(.+)/(.+)
/.*/.*

Answer:



NEW QUESTION: 104
□□□ □□□ □□□□ □□ □□□□.
□□ □□□ □□ □□ □□□ □□ □□□□□ □□□ Azure □□□ □□□□ □□□□.

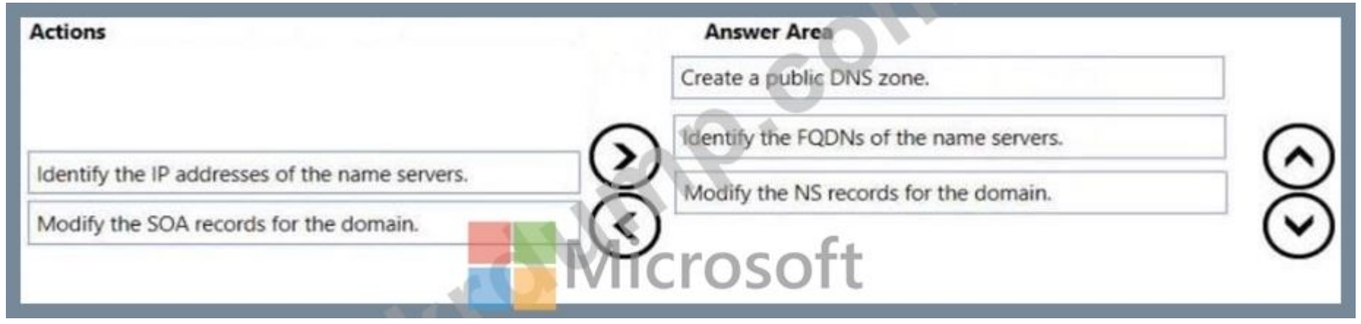
Name	Location
Vnet1	East US
Vnet2	North Europe
Vnet3	West US
Vnet4	West Europe

ExpressRoute□ □□□□ □□ □□□□□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□ □□□□ □□ 1Gbps□□ □□□.
- □□□□ □□ □□ □□□□□ □□□ □ □□□ □□□.
- □□□ □□□□□ □□□.
ExpressRoute □□□ □ □ □□□□□□□ □□, □□ ExpressRoute SKU□ □□□□□ □□□?
A. □□□□□□□ □□□□ □□ 1□
B. □□□□□□□ □□□□ □□ 2□
C. ExpressRoute Standard □□ 4□
D. □□□□□□□ □□ □□ 1□
Answer: A (LEAVE A REPLY)
Express Route Premium SKU provides ability to connect from on-premises to any of the Azure regions across the globe.

NEW QUESTION: 105
□□□ □ □□ □□
DNS □□□□ □3□ □□□□□ □□ □□□□□.
Azure□ DNS □□□ □□□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.

Answer:

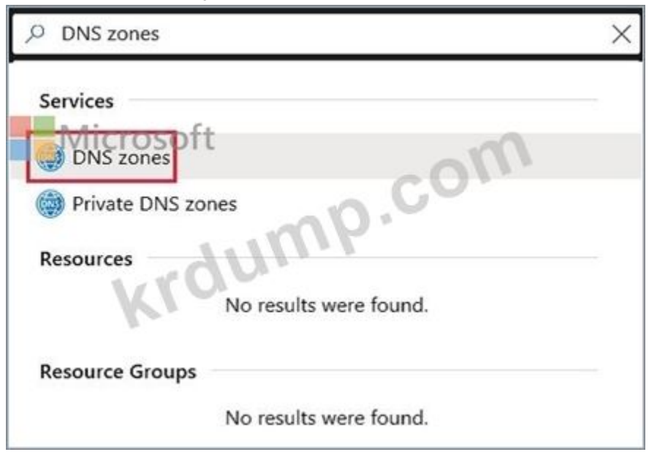


Explanation:

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.

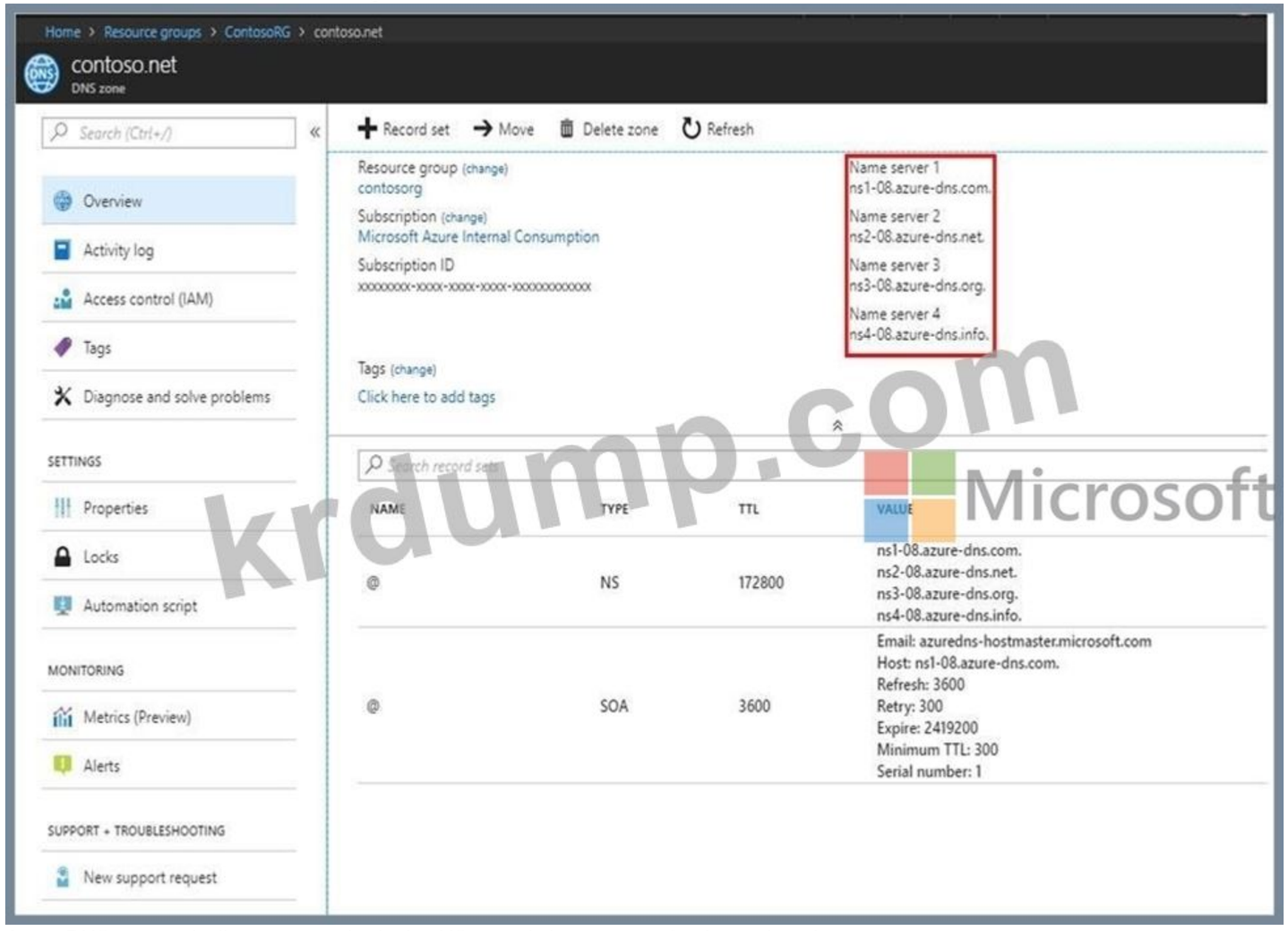
3. On the Create DNS zone page, enter the following values, and then select Create.

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: 106

□□ □□ 2 - □□□ □□□□

□□

□□□ □□□□□ □□□□□□□ □□□ □□ □□□□ □□□ □ □□□ □□□□□.

Contoso□ □□ Azure □□□ □□□□□ Azure□□ □ □□ □□ □□□□□ □□□□ □□□□.

□□ □□:

Azure □□□□ □□□

Contoso□ contoso.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. □□ Azure □□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

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□□ GW1□□□ □□□ □□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□ □□

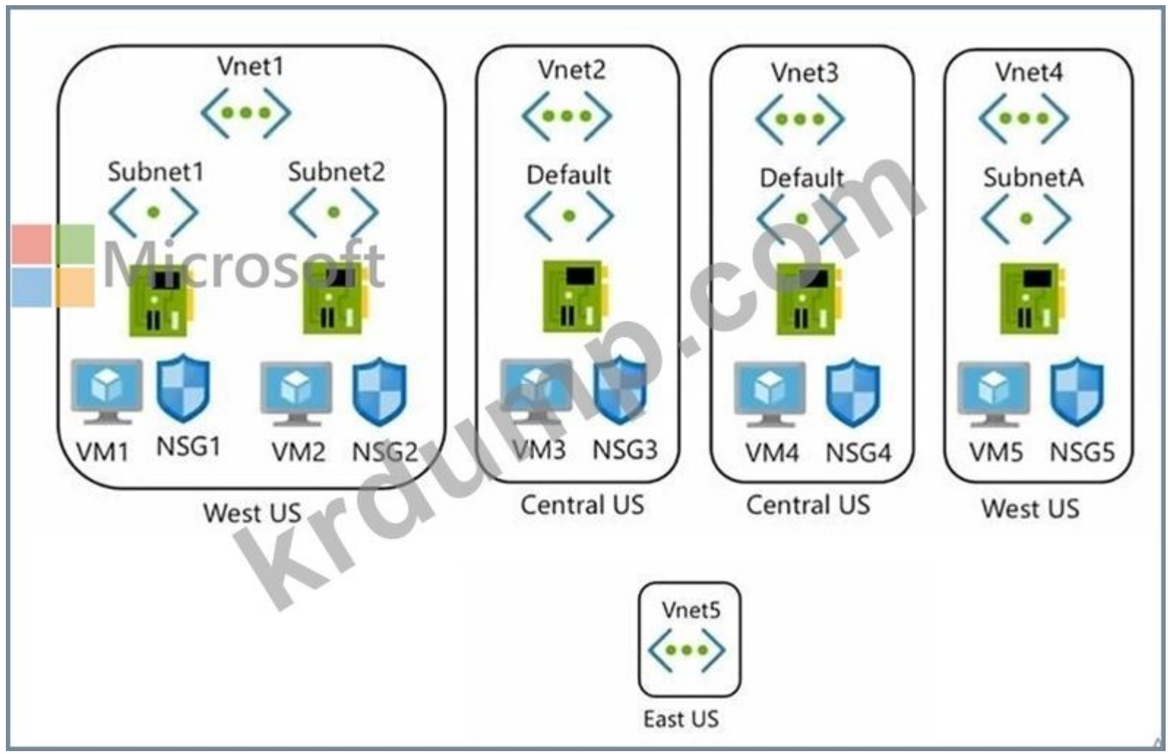
Azure □□□□ □□ □□ □□□ □□□ Windows Server 2019□ □□□□ □□ □□□ □□□□ □□□□.

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

NSG(□□□□ □□ □□)□ □□ □□□ □□□□ □□□□□□ □□□□ □□□□. □ NSG□□ □□□□□ RDP □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□□. □ □□ □□□ □□□□ ICMP □□□□ □□□□ □.

ASG1□□□ □□□□□□ □□ □□□ VM1□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□□□ □□□ □□□□□



Azure □□□□ DNS □□

Azure □□□□ □□ □□ □□□ Azure □□□□ DNS □□□ □□□□ □□□□.

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

Zone1.contoso.com□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

□□ Azure □□□

Azure □□□□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.

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

□□ □□:

□□ □□□□ □□ □□
Contoso□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□.
- □□ □□ □□□ Vnet6□□□ □□□ □□ □□□□□ □□□□, □□ □□□□□ □□ □□□□ □□□ □□□□□□□.
Vnet6□ □□□□ □ □□ □□□□ □□
Vnet6□ □□□ □ □□ □□ □□
Vnet6□ □□ VPN □□ □□□ □□□□□.
Vnet6□ □□□□ KeyVault1, DB1 □ Vnet1□ □□□□ □ □□□ □□□□□.
□□□□□□□ □□ □□□□
- Vnet4□ Vnet5□ □□ □□□□ □□ □□□ □ □□□ □□□.
□□□□□□□ □□ □□□□□ □□.
- VM-Analyze□□ □□□ □□ □□□ Subnet1□ □□□□□. VM-
Analyze□ Subnet2□□ □□□ □□□□ □□□□ □□□□ □□□.
□□□.
□□□□ □□ □□ □□
Contoso□ □□□ □□ □□□□ □□ □□ □□□ □□□ □□□□.
- P2S(Point-to-Site) VPN □□□□ □□ Azure Active Directory(Azure AD) □□□ □□□□□.
- NSG3 □ NSG4□ □□ NSG □□ □□□ □□□□□□.
- Vnet1/Subnet1□ □□□ NSG10□□□ □□□ NSG□ □□□□□.
□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.
□□□.

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

- Vnet1/Subnet2□ □□□ NSG11□□□ □□□ NSG□ □□□□□.
□□□ □□ □□ □□□ □□□ □□ □□□□□ □□ □□□ □□□□□.

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

□□□ □□
VM-Analyze□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□.
Subnet2□ □□□ □□□ □□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Address prefix:

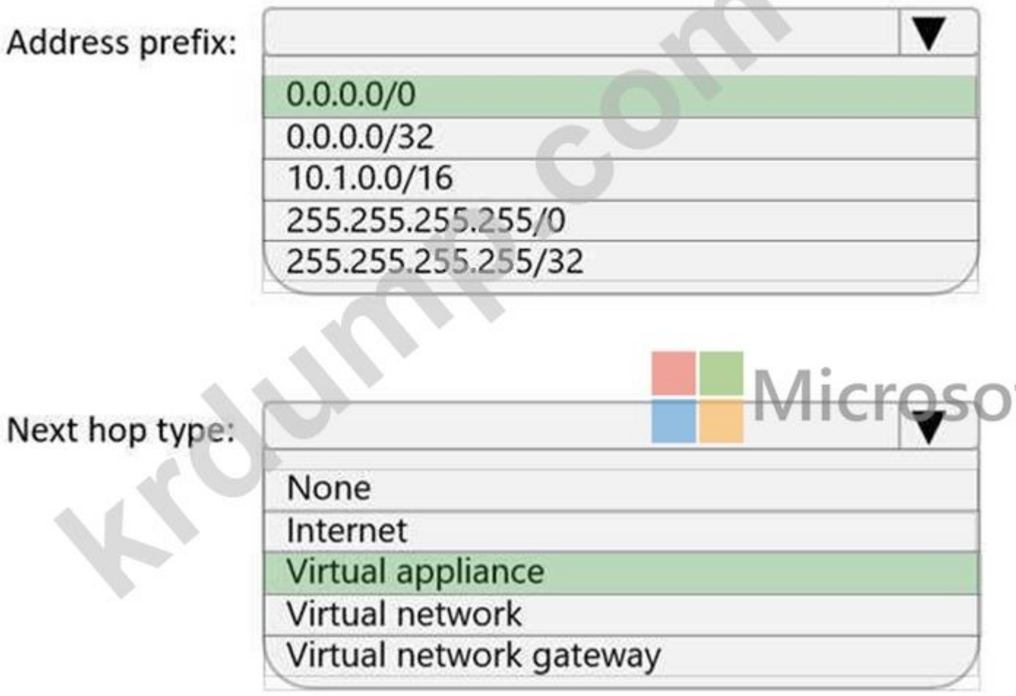
- 0.0.0.0/0
- 0.0.0.0/32
- 10.1.0.0/16
- 255.255.255.255/0
- 255.255.255.255/32

Next hop type:

- None
- Internet
- Virtual appliance
- Virtual network
- Virtual network gateway

Answer:

Answer Area



Explanation:

We create a Route Table with a UDR that points 0.0.0.0/0 to a Virtual Appliance and assign it to Subnet2.

The IP of the virtual appliance (not asked for here) would then be VM-Analyze which then inspects the traffic.

NEW QUESTION: 107

□□□ □□

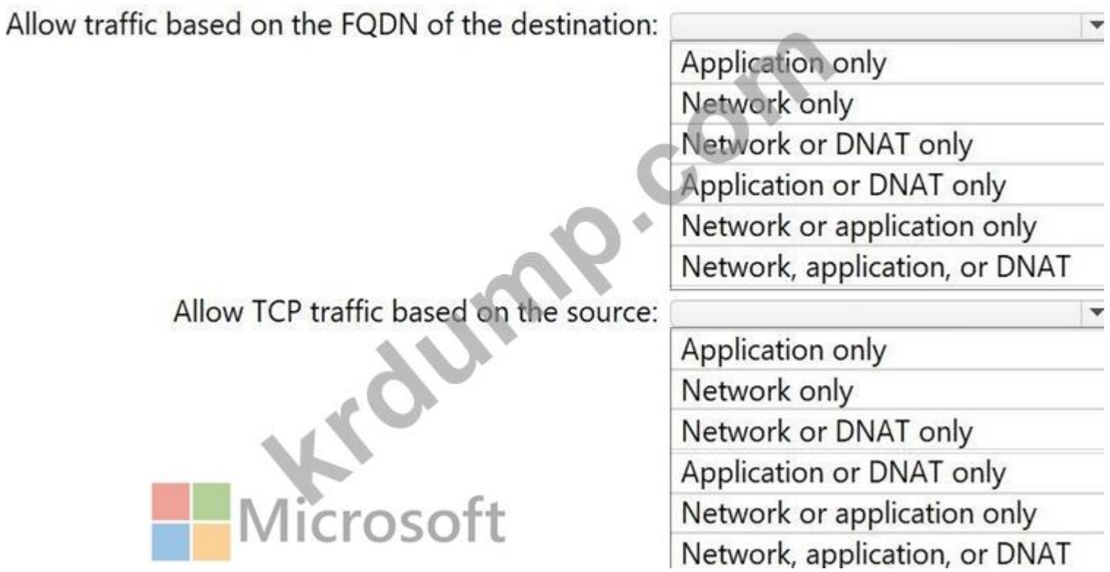
□□□ Azure □□□□ FWPolicy1□□□ □□□ Azure □□□ □□□ □□□□ □□□□.

FWPolicy1□ □□ □□ □□□ □□ □□□□ □□□.

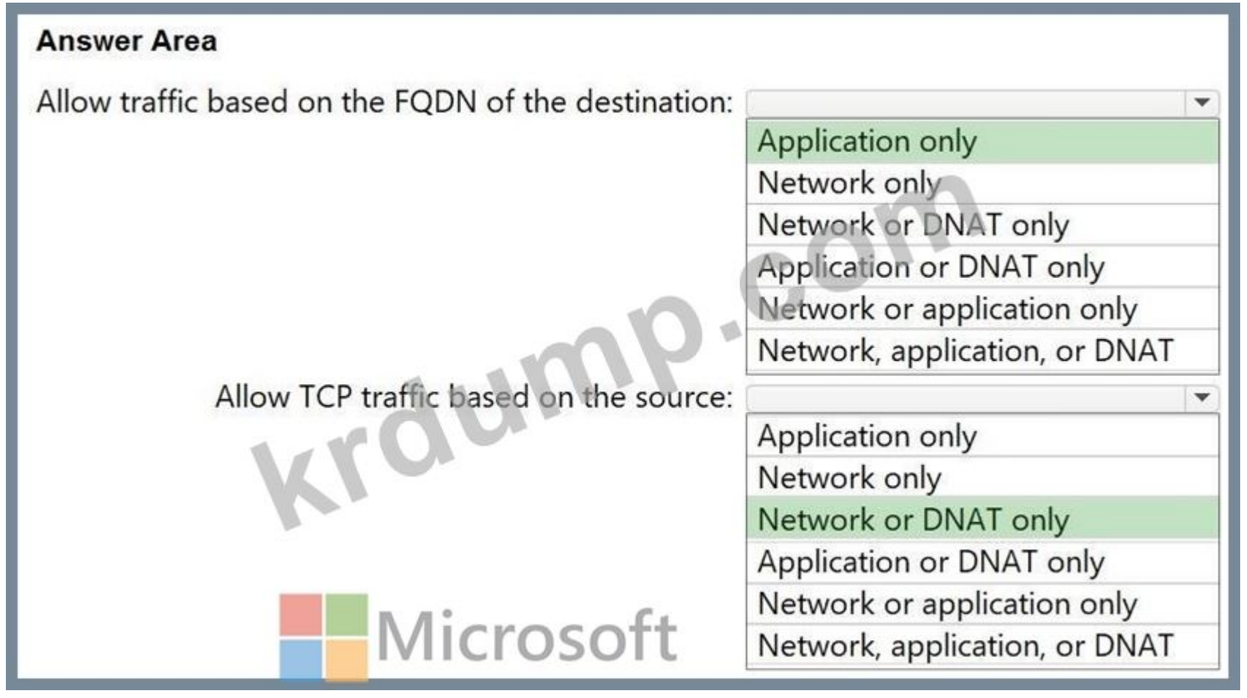
- □□□□ FQDN□ □□□□ □□□□ □□□□□.
- □□□ □□ TCP □□□□ □□□□□.

□ □□□□□ □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:



NEW QUESTION: 108

□□□ □□

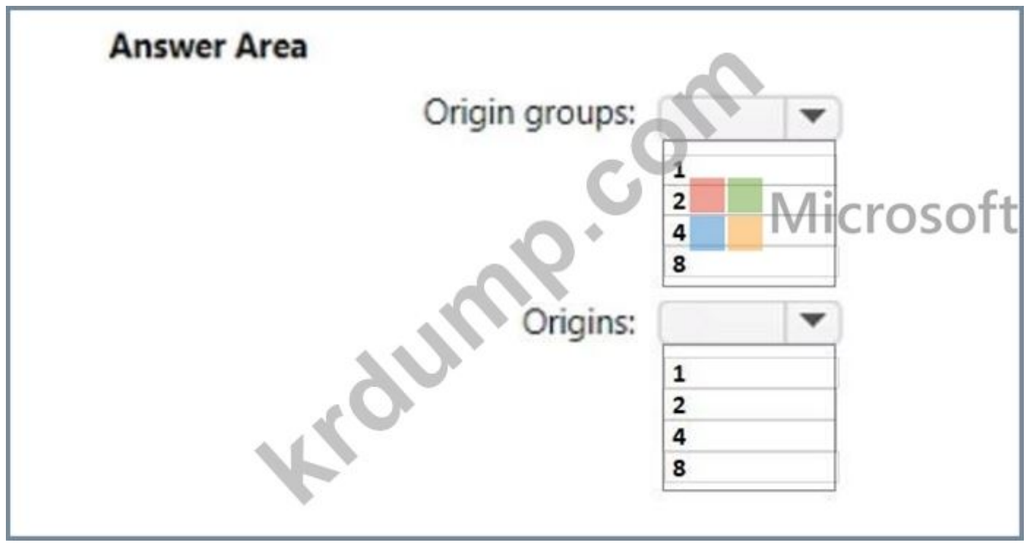
App1□□□ □□ □□□ Azure □□□ □□□□. App1□ □□ □□ □□□ Azure App Service □□ □□□□□.

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

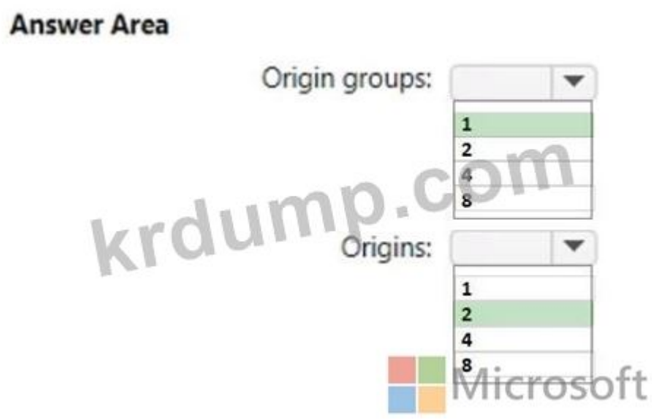
Azure Front Door□ □□□□ App1□ □□□□ □□□. □□□□ App1□ □□ □□ □□□ □□ □□□ □□ □□□ □□□□ □□ □□ □□□□□□ □□□□ □□□.

□□□□ □□ □□ □□□ □□ □ □□□ □□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

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.

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.

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

NEW QUESTION: 109
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

VNet1□□ Subnet□□□ □□□ □□□□ □□□□.
□□□1□ □□□ □□□□ □□□□1□ □□□□3□□ □□□ □ □□□ □□ □□□. □□, □□ □□□ □□□□□ □□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□□□□ □□ □□
B. Azure Private Link
C. □□□ □□□□□ □□
D. □□□ □□
Answer: C (LEAVE A REPLY)
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

NEW QUESTION: 110
Sub1□ Sub2□□ □ □□ Azure □□□ □□□□. Sub1□□ VM1□□□ □□ □□□ □□□□.
Azure Private Link□ □□□□ VM1□ Sub2□ □□□□□ □□□ □ □□□ □□ □□□□□.
VM1□ □□ □□□□ □□□□□ □□ □□ □□□□ □□□□□□ □□□□ □□□.
Sub1□□ □□ □□□ □□□□ □□□?
A. Azure □□□□ DNS □□
B. Azure □□ □□□
C. □□□ □□□□□
D. □□□ □□□□□
Answer: B (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview

NEW QUESTION: 111
Azure □□ □□□□□ □□□□ □□ IP □□ □□□ □□□□ □□□□.
□□□□□ IP □□□ □□□ □□□ □□□ □□□□□?
A. □□ □□ □□□
B. □□□ □□□□□
C. □□ □□□□ □□□
D. □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
□□□ □□ □□□(DNS)□ □□□ □□□ IP □□□ □□□□□.

□□ □□□ □□ □ Azure Private DNS□□ □□□ □ □□ □□ □□□□□?

A. CNAME

B. □□

C. AA

D. AAA

E. AAAA

F. PTR

Answer: C,D (LEAVE A REPLY)

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: 113

□□□ □□

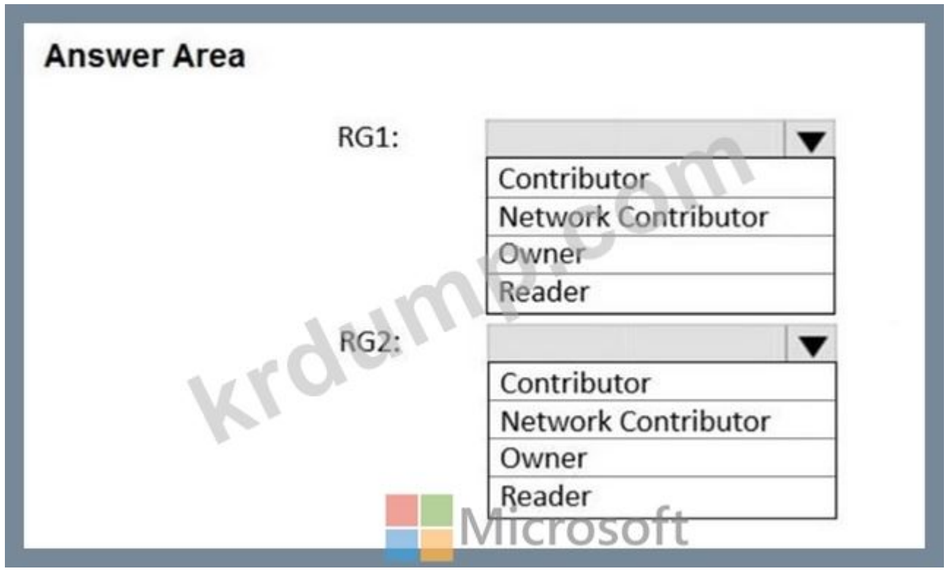
□□□ User1□ □□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Description
Policy1	Azure Firewall policy
RG1	Resource group that contains multiple resources
RG2	Resource group that contains multiple resources
FW1	Azure Firewall instance in RG1 that protects the resources in RG2 and RG3

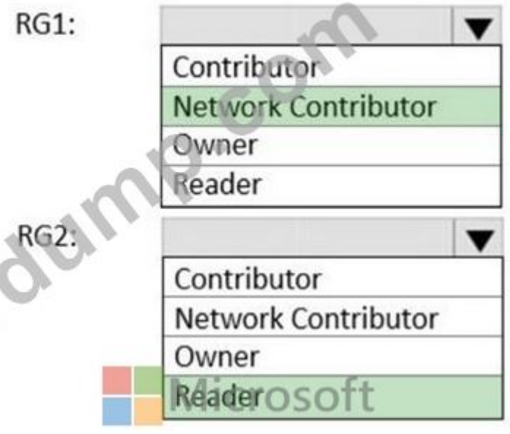
Azure Firewall Manager□ □□□□ User1□ Policy1□ FW1□ □□□ □ □□□ □□ □□□.

□□□□ □□ □□ □□□ □□□ □□□.

User1□□ □ □□□ □□□ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.



Answer:



NEW QUESTION: 114

VM1□□□ □□ □□, NIC1□□□ □□ □□□□ □□□□□ □□, □□□ IP1□□□ □□ SKU □□ IP □□□ □□□ Azure □□□ □□□□. NIC1□ VM1□ □□□□ □□, IP1□ NIC1□ □□□□ □□□□.
IP1□ □□ SKU□ □□□□□□□ □□□.
□□□ □□ □□ □□□?

A. VMI□ □ NIC□ □□□□□.
B. IP1□ NIC1□□ □□ □□□□□.
C. VM1□□ NIC1□ □□□□□.
D. vM1□ □□□□□.

Answer: B (LEAVE A REPLY)
To upgrade a Basic SKU public IP address associated with a virtual machine's network interface in Azure, you need to first dissociate the Basic IP, then upgrade it to Standard SKU, and finally reassociate it with the network interface.
Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-upgrade-vm

NEW QUESTION: 115
□□□ □□
□□ □□□□□□ VPN □□□ □□□□.
□□ □□□□□ □□ □□□□ □□□□□□ □□□ Azure □□□ □□□□.
□□□ □□ □□□ □□□ □□□ □□□ □ VPN □□□ □□□□ □□□.
PowerShell □□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

```
...
$policy = [                    ] -IkeEncryption AES256 -IkeIntegrity SHA384 -DhGroup DHGroup24 -IpsecEncryption AES256
          New-AzIpsecPolicy
          New-AzIpsecTrafficSelectorPolicy
          New-AzServiceEndpointPolicy
          New-AzVpnClientIpsecPolicy
    -IpsecIntegrity SHA256 -PfsGroup None -SALifeTimeSeconds 14400 -SADataSizeKilobytes 102400000
...
[                              ] -Name $Connection16 -ResourceGroupName $RG1 -VirtualNetworkGateway1 $vnet1gw
  New-AzVirtualHub
  New-AzVirtualNetworkGateway
  New-AzVirtualNetworkGatewayConnection
  New-AzVirtualNetworkGatewayNatRule
    -LocalNetworkGateway2 $lng6 -Location $Location1 -ConnectionType IPsec -IpsecPolicies $policy -SharedKey 'AzureA1b2C3'
```

Answer:

Answer Area

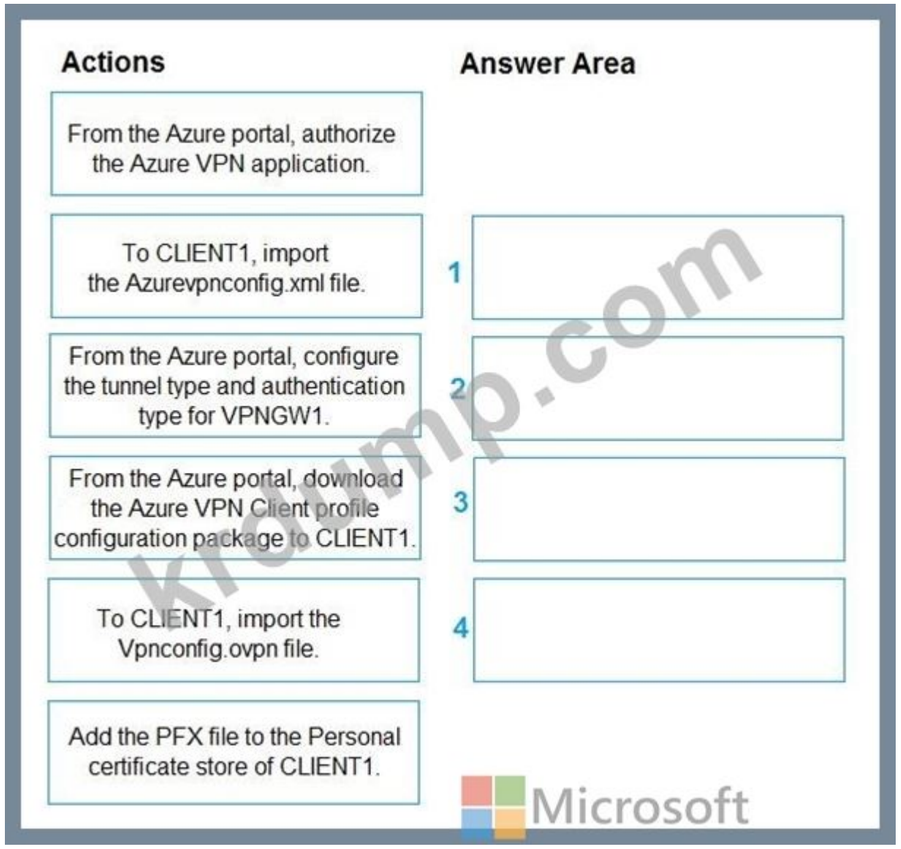
```
...
$policy =  [ New-AzIpsecPolicy | New-AzIpsecTrafficSelectorPolicy | New-AzServiceEndpointPolicy | New-AzVpnClientIpsecPolicy ]  -IkeEncryption AES256 -IkeIntegrity SHA384 -DhGroup DHGroup24 -IpsecEncryption AES256
    -IpsecIntegrity SHA256 -PfsGroup None -SALifeTimeSeconds 14400 -SADataSizeKilobytes 102400000
...
[ New-AzVirtualHub | New-AzVirtualNetworkGateway | New-AzVirtualNetworkGatewayConnection | New-AzVirtualNetworkGatewayNatRule ]  -Name $Connection16 -ResourceGroupName $RG1 -VirtualNetworkGateway1 $vnet1gw
-LocalNetworkGateway2 $lng6 -Location $Location1 -ConnectionType IPsec -IpsecPolicies $policy -SharedKey 'AzureA1b2C3'
```

Explanation:
Box 1: New-AzIpsecPolicy
https://learn.microsoft.com/en-us/powershell/module/az.network/new-azipsecpolicy?view=azps-9.2.0 Box 2: New-AzVirtualNetworkGatewayConnection
https://learn.microsoft.com/en-us/powershell/module/az.network/new-azvirtualnetworkgatewayconnection?view=azps-9.2.0#example-1

NEW QUESTION: 116
10□□ □□ □□□□ □□□□ Azure □□ □□□□□ □□□□□ □□□. □ □□□□ IPv6 □□□ □□□□□. □ □□□□ □□ 200□□ □□ □□□ □□ □□□ □□□□□□.
□□ □□□□ □□□ □□□ □□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. /64
B. /120
C. /48
D. /24
Answer: (SHOW ANSWER)
The subnets for IPv6 must be exactly /64 in size. This ensures future compatibility should you decide to enable routing of the subnet to an on-premises network since some routers can only accept /64 IPv6 routes.
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview#capabilities

NEW QUESTION: 117
□□□ □ □□ □□

CLIENT1□□□ □□□ □□□□ □□□, □ □□□□ Windows 11□ □□□□ Azure VPN □□□□□□ □□□□ □□□□.
VPNGW1□□□ □□□ Azure □□ □□□□ □□□□□□ □□□□.
□□□□□1□ VPNGW1□ □□□ □ □□□ □□□□ □□□. □□□□ Microsoft Entra □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□, □□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□□□.



Answer:

Actions

To CLIENT1, import the Vpnconfig.ovpn file.

Add the PFX file to the Personal certificate store of CLIENT1.

Answer Area

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

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

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

4 To CLIENT1, import the Azurevpnconfig.xml file.

NEW QUESTION: 118

□□□ □□

□□□ Azure □□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

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

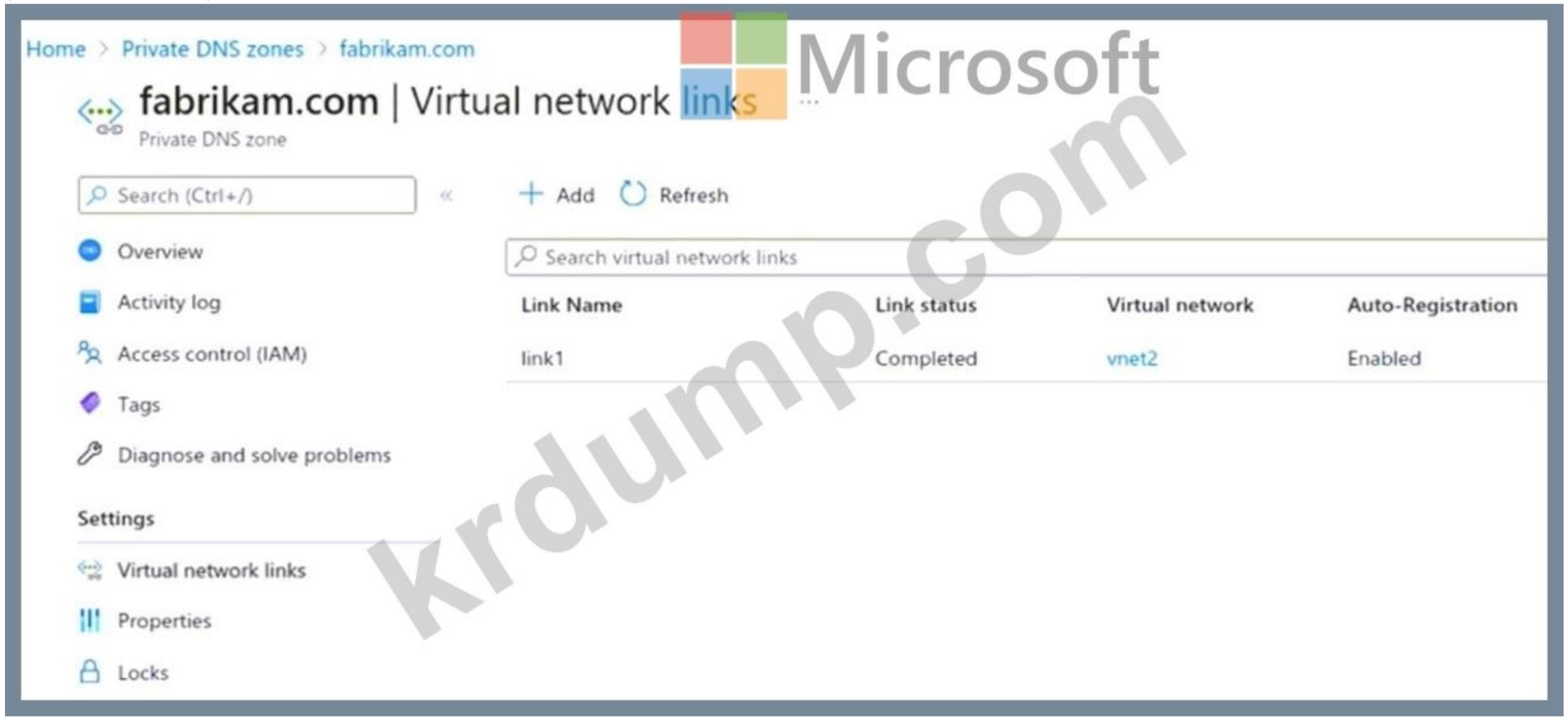
VM5□□ □□□ □□ □□□ □□□, □□ □□ □□□ IP □□ □□□ □□□ □□□□.

- IP □□: 10.4.0.5
- □□□ □□□: 255.255.255.0
- □□ □□□□□: 10.4.0.1
- DNS □□: 168.63.129.16

fabrikam.com□□□ Azure □□□□ DNS □□□ □□□, □□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

fabrikam.com DNS □□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□□.
(□□ □□ □□□□□.)



VM5□ app1.fabrikam.com□ IP □□□ □□□□ □ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

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:

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.	○	○

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: 119

□□□ □□

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□ □□ □□(CA)□□ app1.contoso.com□ □□□□ □□□□ □□ □□□□ appservice1□ □□□□□.

App1□ https://app1.contoso.com URL□ □□□□ □□□ □ □□□ □□ □□□. □□, App1□□ □□□ □□ □□□□ FD1□ □□ □□□□□□ □□□□ □□□□ □□□.

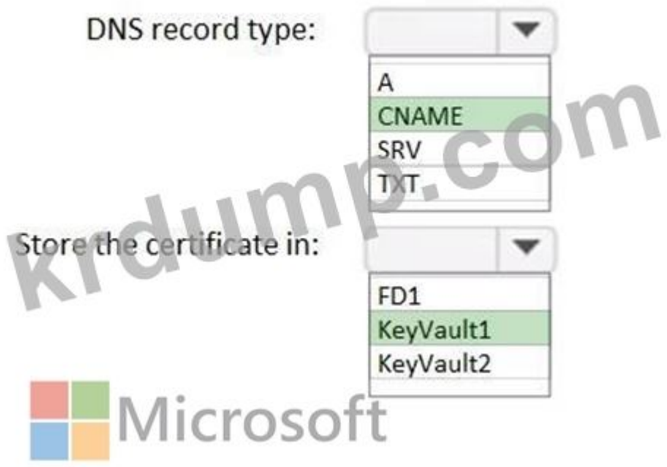
□□ □□□ DNS □□□□ □□□□ □□, □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area



Explanation:

DNS: CNAME (When you added a custom domain to your Front Door's frontend hosts, you created a CNAME record in the DNS table of your domain registrar to map it to your Front Door's default .azurefd.net hostname) Store certificate in: KeyVault1 (Your key vault must be configured to use the Key Vault access policy permission model.) There you have a link with all explained https://learn.microsoft.com/en-us/azure/frontdoor/front- door-custom-domain-https.

NEW QUESTION: 120

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Description
VNet1	Virtual network that contains a subnet named Subnet1
Endpoint1	Private endpoint that is connected to Subnet1 and linked to an Azure App Service web app named App1
storage1	Storage account that can only be accessed via Endpoint1
NSG1	Network security group (NSG) that is linked to Subnet1

NSG1□ □□□□ storage1□ □□ □□□ □□□□ □□□. □□□ □□ □□□□ □□□?

A. Azure Private Link □□□

B. □□□□□□ □□ □□

C. □□ □□□□□ □□□□ □□

D. □□□ □□□□□

Answer: (SHOW ANSWER)

To control access to a storage account via a private endpoint using a Network Security Group (NSG), you must first enable a specific property on the subnet where the private endpoint is located.

*-> 1. Enable Network Policies for Private Endpoints: On the subnet containing the private endpoint, you must enable the PrivateEndpointNetworkPolicies property. By default, network policies for private endpoints are disabled, which causes traffic to the private endpoint to bypass NSG rules.

2. Configure NSG Rules: Once network policies are enabled, you can then define and apply inbound or outbound security rules in your NSG to manage traffic to the storage account's private IP address.

3. Disable Public Access: To ensure the storage account is only accessible via the private endpoint, navigate to the storage account's Networking settings and set Public network access to Disabled.

Reference:

https://learn.microsoft.com/en-us/azure/private-link/disable-private-endpoint-network-policy

NEW QUESTION: 121

□□□ □□

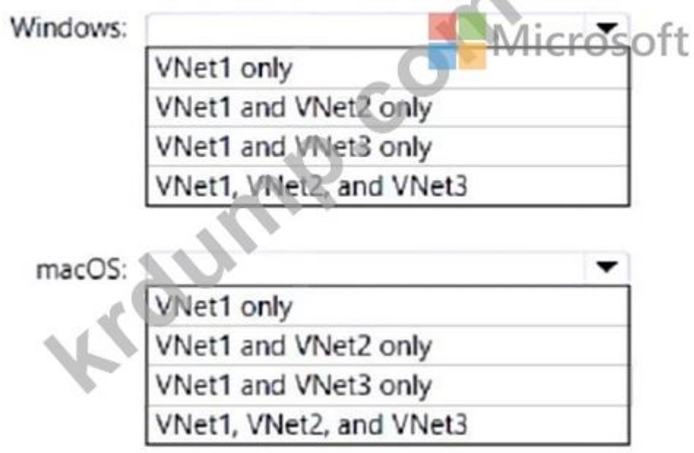
□□□ Azure □□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

Name	Configuration
VNet1	Peers with VNet2 Has the Allow gateway transit setting enabled Contains an Azure VPN gateway named VGW1 that has BGP disabled
VNet2	Peers with VNet1 Has the Use remote gateway setting enabled
VNet3	Connected to VNet1 via a Site-to-Site (S2S) VPN connection

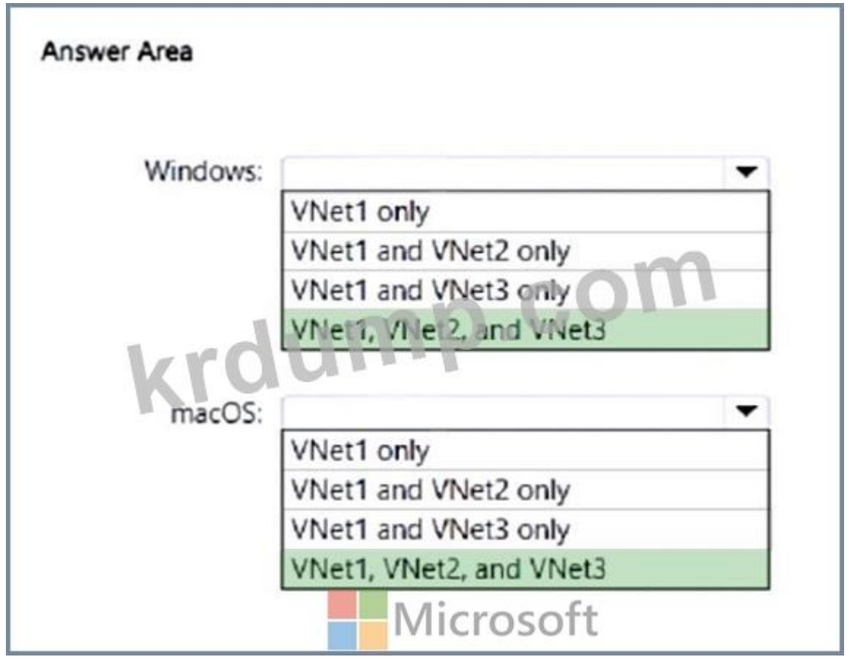
Windows □□ macOS □□ □□□ □□□□ □□□ □□□□. □□□ □□□ OpenVPN □□□□□ □□□□ VGW1□ □□□□□.

□ □□□ □□□□ □ □□ □□ □□□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

Answer Area



Answer:



NEW QUESTION: 122

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.

Azure WAF(□ □□□□□□ □□□)□ □□□□ Azure □□□□□□ □□□□□□ □□□□.

□□□□□□ □□□□□□ □□□□□□ □□□□□□ URL□ □□□□ □□□□□ □□□□□□. □□ URL□ □□□□□ □□□□□ HTTP 403 □□□ □□□□□□. □□ □□□ □□□□□ □□□ □□ □□□ □□□□□ □□.


```
{
 "timeStamp": "2021-06-02T18:13:45+00:00",
 "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
 "operationName": "ApplicationGatewayFirewall",
 "category": "ApplicationGatewayFirewallLog",
 "properties": {
   "instanceId": "appgw_0",
   "clientIp": "137.135.10.24",
   "clientPort": "",
   "requestUri": "/login",
   "ruleSetType": "OWASP_CRS",
   "ruleSetVersion": "3.0.0",
   "ruleId": "920300",
   "message": "Request Missing an Accept Header",
   "action": "Matched",
   "site": "Global",
   "details": {
     "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
     "data": "",
     "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
     "line": "1247"
   },
   "hostname": "app1.contoso.com",
   "transactionId": "f7546159y1hjk7wal14568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


□□□□□□ □□□□□□ □□ URL□ □□□ □ □□□ □□□□ □□□.

□□ □□: 137.135.10.24□ □□□□ WAF □□ □□ □□ □□□ □□□□.

□□ □□□ □□□□?

A. □□□

B. □

Answer: A (LEAVE A REPLY)

NEW QUESTION: 123

□□□ □ □□ □□

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

Gateway1□ Subnet1□ □□□□ □□□. □ □□□□ VM1□ □□□□□ □□□□□ □□□.

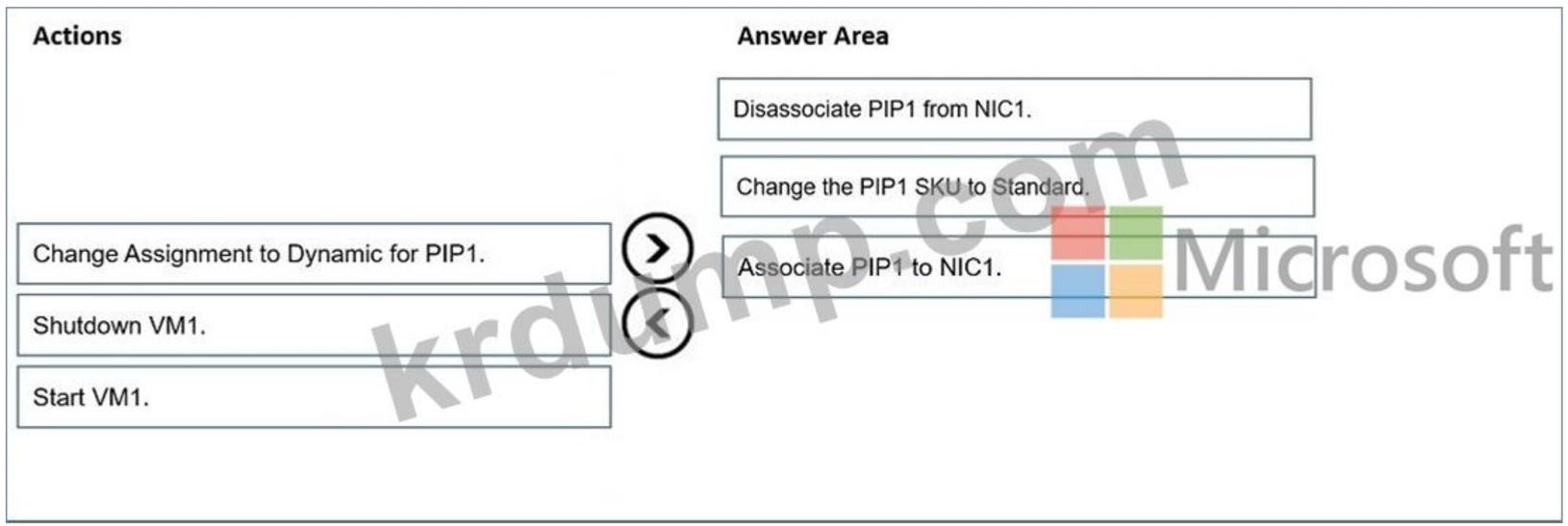
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.

Actions

- Disassociate PIP1 from NIC1.
- Change the PIP1 SKU to Standard.
- Change Assignment to Dynamic for PIP1.
- Shutdown VM1.
- Start VM1.
- Associate PIP1 to NIC1.

Answer Area

Answer:



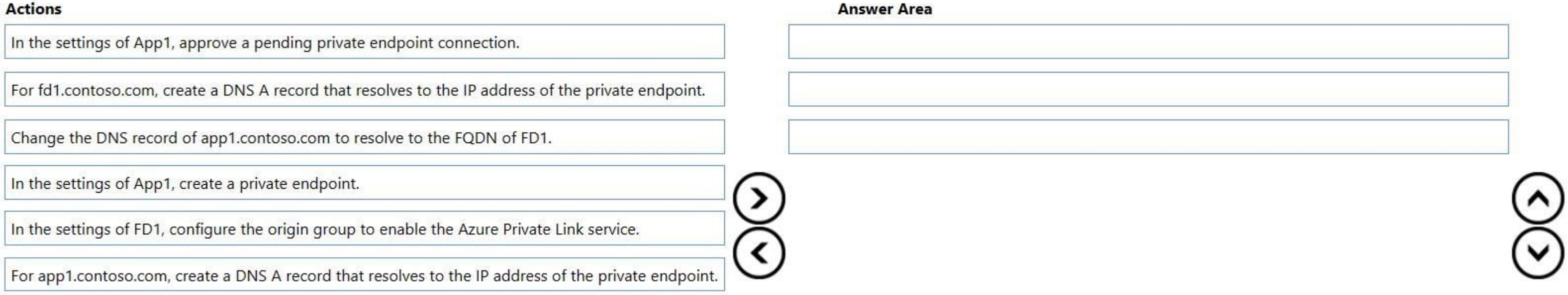
Explanation:
https://learn.microsoft.com/en-us/azure/nat-gateway/tutorial-migrate-ilip-nat

NEW QUESTION: 124
□□□ □ □□ □□

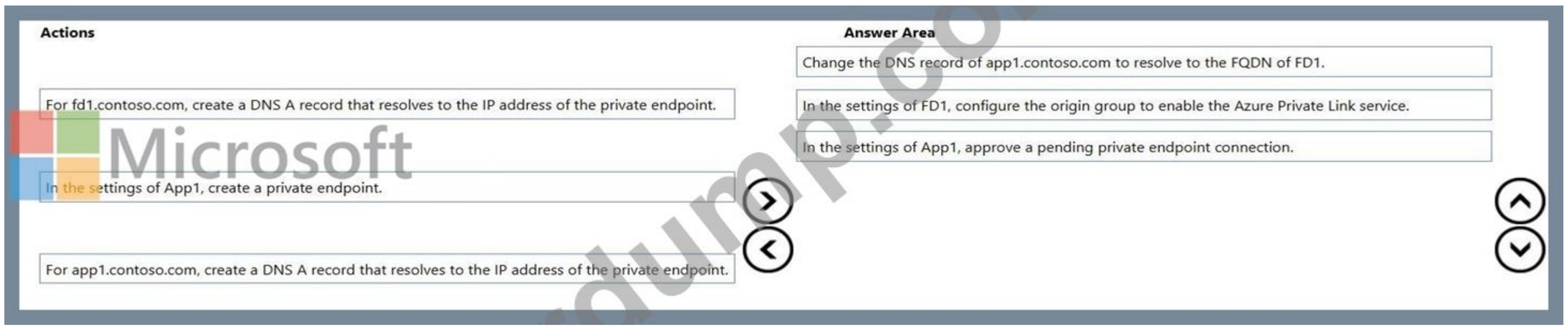
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□□□ App1□ □□ □□□□ □□ □□□□□□.
□□ □□□ □□□□ □□□.
- □□□□ □□□ □□□□□□ □□□□ App1□ □□□□ □□□.
- App1□ □□ □□ □□□ □□□ FD1□ □□ □□□□□ □□□.
- App1□□ □□ □□ □□□ □□□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.



Answer:



NEW QUESTION: 125

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□ □ □□□□.

□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.

Azure □ □□□□□□ □□□(WAF)□ □□□□ Azure □□□□□□ □□□□□□ □□□□.

□□□□□□ □□□□□□ □□□□ □□□□ □□□□□□ □□□□□□ URL□ □□□□□ □□□.

□□ URL□ □□□□□ □□□□□ HTTP 403 □□□ □□□□□□.□□ □□□ □□□ □□ □□□ □□ □□□ □□□□□□□.

```
{
 "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": "f7546159ylhjk7wall4568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
  }
 }
```


□□ URL□ □□□□□□ □□□□□□ □□ □□ □□□□ □□□□ □□□.
□□ □□: ruleId□ 920300□ WAF □□□ □□□□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
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: 126
□□□ □□ □□□□□ □□□□ □□ □□ □ VPN □□□ □□□□□ □□□□□□. □ □□ □□ □ VPN□ □□ □□□□ □ □□□ □□□□ □□ □□□ □ □□□□.
A. SSTP
B. □□VPN
C. IPSeright
D. IKEv2 VPN
Answer: C (LEAVE A REPLY)

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: 127
□□ □□ 3 - □□□ □□□□
□□
□□□□□(Proseware, Inc.)□ □□□□ □□□ □□ □□□□□□□ □□□ □ □□ □□□ □□□□□.
□□ □□. □□□□□ □□
Proseware□ corp.proseware.com□□□ □□□ □□□□□ Active Directory Domain Services(AD DS) □□□□□ □□□□ □□□, □ □□□□□ proseware.com□□□ □□□ Microsoft Entra □□□□ □□□□□□.
Proseware□ proseware.com□ □□□ Azure □□□ □□□□ □□□□.
Proseware□ □□ □□ □□(CA)□ □□□□ □□□□.
□□ □□. □□□□ □□□
□□ □□□□□ □□ □□ □□ □□ □□□ □□□□.

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□ ExpressRoute □□□ □□□□ Azure□ □□□□□.
SFONet□ □□□ □(S2S) VPN□ □□□□ Azure□ □□□□□.
□□ □□. Azure □□□
Azure □□□□ □□ □□ □□□ □□ □□□□ □ □□□□ □□□□ □□□□.

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

□□□□ VM1, VM2, VM3, VM4□□ □□□ □□ □□ 4□□ □□□□ □□□□. VM1□ VM2□ App1□□□ □□ □□□□□□.

VM3 □ VM4□ app2.proseware.com□□□ FQDN□ □□□□ □□□□ □ □□ App2□□ □ □□□□□□□ □□□□□□. □□□□ HTTP □□ HTTPS□ □□□□ app2.proseware.com□ □□□□□□.

VM1, VM2, VM4□ SpokeVNet□ □□□□ □□□□.

□□□□ □□ □□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □□□□.

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

□□□□ FD1□□□ Azure Front Door Standard □□□□ □□□□ □□□□. FD1□□ □□ □□□□□ □□□ □□□□ APPGW1□ □□□□ □□ □□ □□ □□□ □□□□ □□□□.

HubVNet□ ERGW1□□□ ExpressRoute □□□□□□ □□□□ NYCNet□ □□□□□.

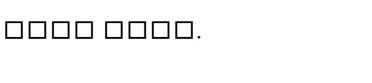
□□□ □□ □□ □ □□ □□. □□□ □□ □□

Proseware□ □□□ □□ □□ □□□ □□□ □□□□□.

- PRDNS1□□□ □□□ Azure □□□□ DNS □□□□ HubVNet□ □□□□ PRDNS1□ SpokeVNet□ □□□□□.
- DNSRS1□□□ □□□ DNS □□□ □□ □□□ □□□□, DNSRS1□ PRDNS1□ □□□□□.
- Azure □□ □□□□ □□□□ □□□□ □□ □□□ □□□□□.
- □□□□□ □□□□□□ SUBNET-JUMPHOSTS□ TCP □□ 3389□ □□ □□□□ □□□ □□□□□.
- □□□□□ SpokeVNet□□ □□□□ TCP □□ 80 □□□ □□□□□.
- Azure Virtual Network Manager □□□ □□□□ NSG □□□□ □□ □□□□□ □□□.
- HubVNet□ NVA1 □ NVA2□□ □□□ □□□□ □□ □□□□□□(NVA) □ □□ □□□□□.
- HubVNet□ LBGW1□□□ □□□ □□□□□ □□ □□□□ □□□□□.
- NVA1 □ NVA2□ □□□□ LBGW1□ LBS1□□ TCP □□ 443, 1433 □ 1434□ □□□□ □□□□□ □□□□□.

- App2□ □□□ □□ □□□□ FD1□ □□□□ □□□□□ □□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□ □□ □□□ □□□□□.
- Azure Virtual Network Manager □□□ □□□□ □□□□□□.
- NYCNet□ SFONet □□ □□□□ ExpressRoute □□ □ S2S VPN□ □□ □□□□□□.
- Windows 11 □□□ □□ □□□□ P2S(Point-to-Site) VPN□ proseware.com □□ □□□ □□□□ HubVNet□ □□□ □ □□□ □□□□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□ □□ □□□ □□□□□.
- □□□ □ □□ CA□ □□□□□□.
- APPGW1□ □□ □□□□□ □□ □□□ □□ □ □□□□ □□□□□ □□□□.
- Azure□□ □□□□□ □□ □□ □□□ □□□ □□ □ □□□□ □□□□□ □□□□□□.
- app2.proseware.com□□ □□□□ □□ □□□ □□□□ FD1□ □□ □□□□□□ □□□□.
- NYCNet□ □□□□ □□□ □□ □□□□□□ □□□□ Azure □□□□ □□□□□ □□□□ □□□.
- HubVNet □ SpokeVNet□ □□□□ □□ □□□ □□□□ □□□□□□ □□□□ Azure □□□□ □□□□ □ □□□ □□□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□□□ □□ □□□ □□□□□.
- □□□□□ □□□□ □□□□ □□ □□□□□ □□□□ □ □□□ IP □□ □□□ □□□□□□.
- SpokeVNet□□ azure.proseware.com □□□□□□□ corp.proseware.com □□□□□□□ □□ □□ □□ □□□ PRDNS1□ □□□□ □□□□□.
- □□□ □ □□□ □□□ □□□□□□□.
□□□ □□
NYCNet□ SFONet □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

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.

Answer:

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.

NEW QUESTION: 128

□□□□□

□□□ □□□ □□□□

□□□ □□ □□ □□□ □□ □□□ □□□□□□.

- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx

Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

- □ □□□□: 12345678

VNET2□ VPN □□□ □□□ □□□□□.

□□□2-1□□ □□□□ □□ □□□ □□□□ □□□□ □□□□ □□ □□□□□ □□□□ □□□□□ □□ □□□. □ □□□□ □□ □□□ □□□□□ □□□□ □□ □□□□ □□□.

□ □□□ □□□□□ Azure □□□ □□□□□□.

Answer:

Route network traffic with a route table using the Azure portal

Azure routes traffic between all subnets within a virtual network, by default. You can create your own routes to override Azure's default routing. Custom routes are helpful when, for example, you want to route traffic between subnets through a network virtual appliance (NVA) (or a Firewall).

Send Traffic from Azure Firewall to Internet

Even if the Azure Firewall is created with support for Forced Tunneling, you do not have to add a Route Table here at all.
The default behavior will provide outbound connectivity to Internet just like a regular firewall.

Phase 1: Create a route table
In this section, create a route table to define the route of the traffic through the NVA virtual machine. The route table is associated to the subnet-1 subnet where the vm-public virtual machine is deployed.

Step 1: In the search box at the top of the portal, enter Route table. Select Route tables in the search results.

Step 2: Select + Create.

Step 3: In Create Route table enter or select the following information:
* Details omitted. *

Step 4: Select Review + create.

Step 5: Select Create.

Phase 2: Create a route
In this section, create a route in the route table that you created in the previous steps.

Step 1: In the search box at the top of the portal, enter Route table. Select Route tables in the search results.

Step 2: Select route-table-public.

Step 3: In Settings select Routes.

Step 4: Select + Add in Routes.

Step 5: Enter or select the following information in Add route:
Route name: to-firewall.
Destination type: Select IP Addresses.
Destination IP addresses/CIDR ranges Enter 0.0.0.0/0

Use 0.0.0.0/0 for any unmatched routes.

Next hop type: Select Virtual appliance.
Next hop address: Enter the IP address of the Firewall.
This is the IP address you of the Firewall.

Step 6: Select Add.

Step 7: Select Subnets in Settings.

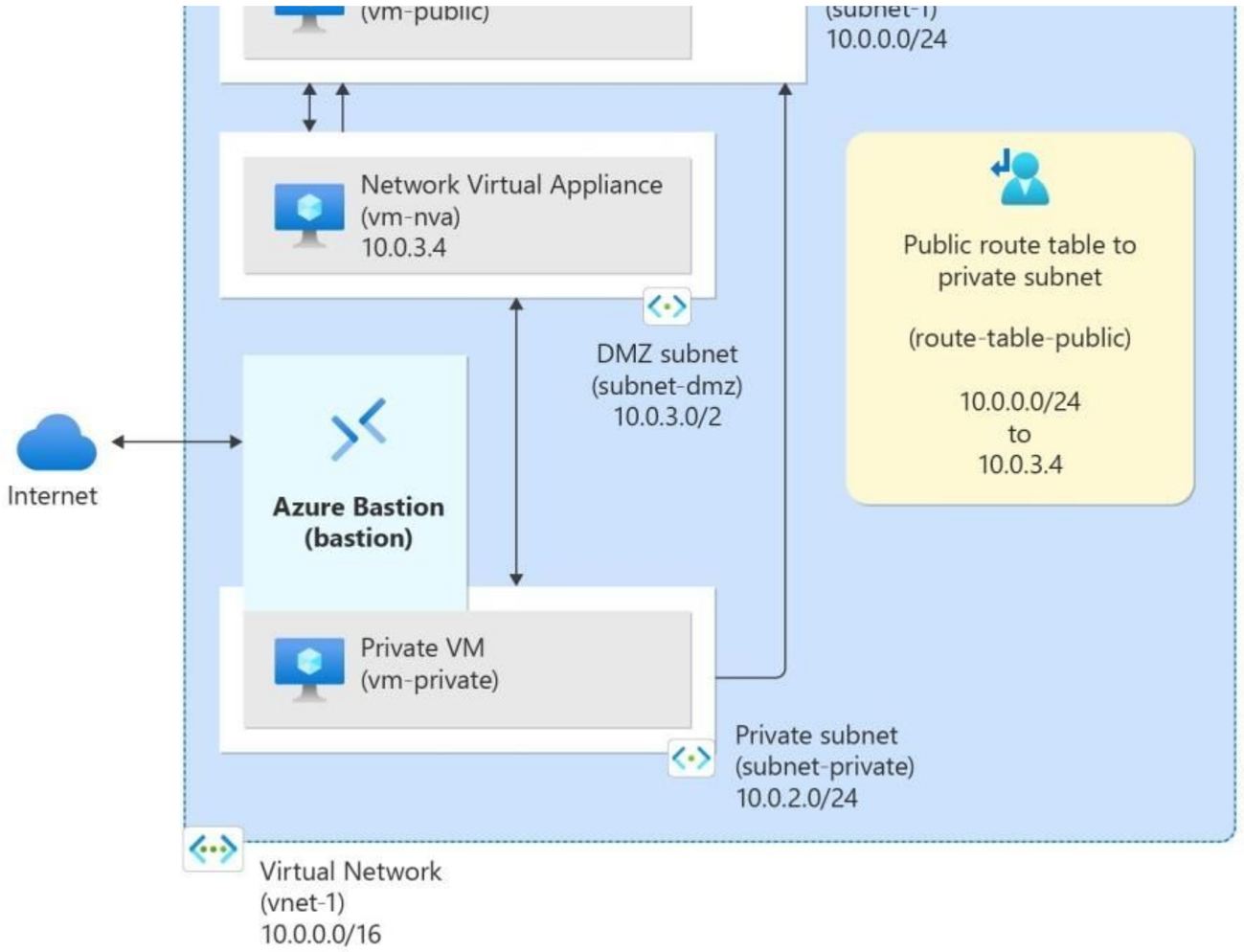
Step 8: Select + Associate.

Step 9: Enter or select the following information in Associate subnet:

Setting Value
Virtual network: Select VNET2
Subnet: Select subnet2-1.

Step 10: Select OK.

Note: Route network traffic with a route table using the Azure portal
Azure routes traffic between all subnets within a virtual network, by default. You can create your own routes to override Azure's default routing. Custom routes are helpful when, for example, you want to route traffic between subnets through a network virtual appliance (NVA).



Reference:
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal
https://learn.microsoft.com/en-us/answers/questions/1356750/internet-routing-via-azure-firewall

NEW QUESTION: 129
□□ □□ 1 - Litware. Inc.
□□
Litware Inc.□ □□□□ □□ □□□□□□ □□ □□ □□□ 20□□ □□□ □□□ □□ □□□□□. □□□□□ □□□□□, iOS □ □□□ 10 □□□ □□□□□.
□□ □□:
□□□□□ □□
□□□□□ □□□□□□ litwareinc.com□□□ □□□ Active Directory □□□□□ □□□, Azure AD Connect□ □□□□ litwareinc.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□□□.
□□ □□□□ □□□ □ VPN □□□ □□□□ Vnetl□□□ □□ □□□□□ □□□□□.

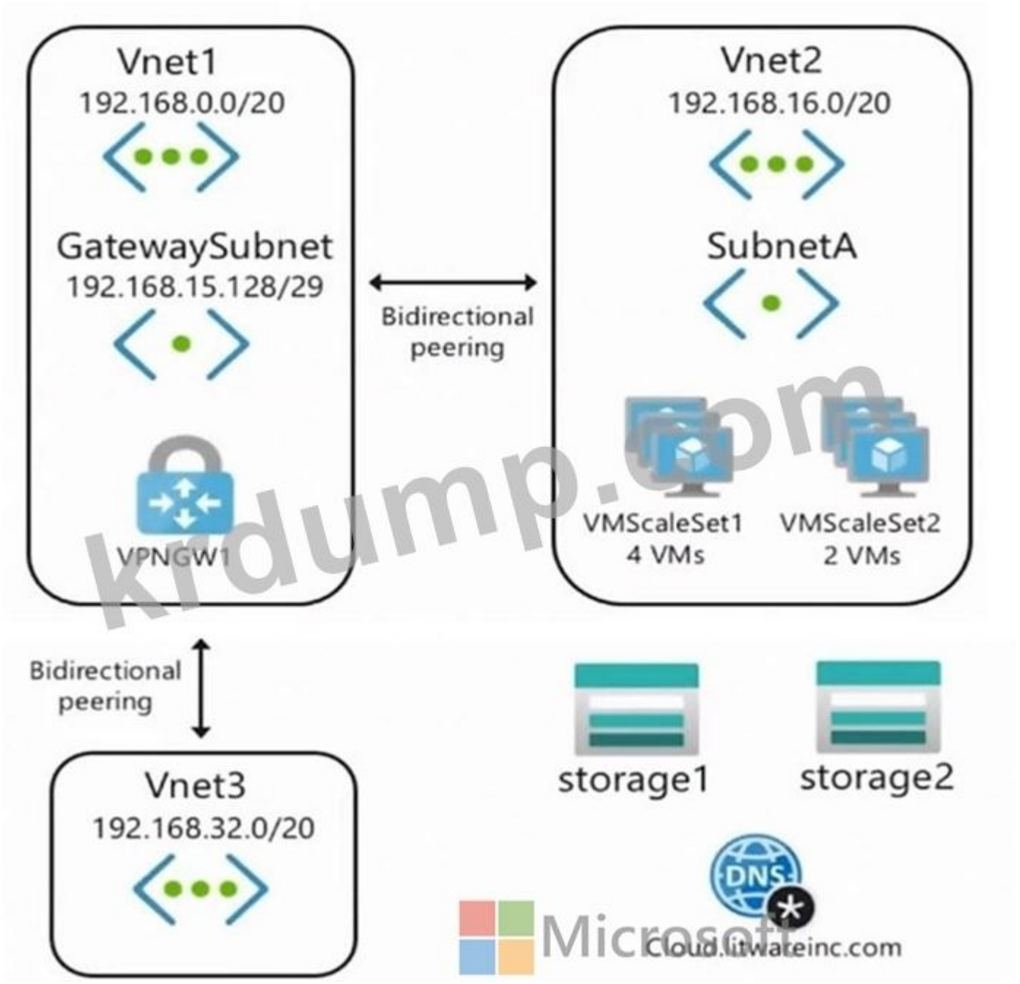
Azure □□

Litware□ litwareinc.com Azure AD □□□□ □□□ Sub1□□□ Azure □□□ □□□□ □□□□. Sub1□□ □□ □□ □□□ □□□ □□ □□ Azure □□□ □□□□ □□□□ □□□□.

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

□□ □□ Azure □□□ □□□ □□□□□□ □□□□ □□□□□□ □□ □□□□.

Vnet1□ Vnet2 □□□□ □□□ □□□□ □□□□ □□□□. Vnet1□ Vnet3 □□□□ □□□ □□□□ □□□□ □□□□. □□ Vnet2□ Vnet3□ □□ □□□ □ □□□□.



□□ □□:

□□□□ □□□□

Litware□ □□ □□ □□ □□□ □□□□ □, □□□ □ □□□ □□□□□□ □□□.

□□ □□□□ □□ □□

Litware□ □□□ □□ □□ □□□□ □□ □□□ □□□□□.

- Vnet2 □ Vnet3□ □□ □□□ 0.0.0.0/0□ □□□□ □□□□□.

ExpressRoute □□□ □□ □□□ □□□□□□ □□□□□.

- cloud.litwareinc.com □□□ □□□□ □□□ □□□□□ □□□□□□.

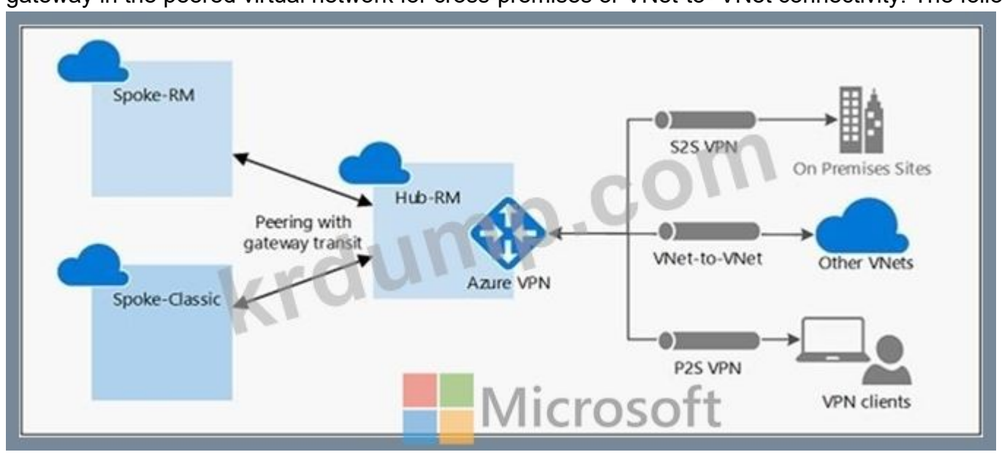
□□□□□ □□□□ □□□□□□□.

- Azure □□ □□□ DNS □□□ cloud.litwareinc.com □□□ □□□□ □□□□□.
- □□□ □□ □□□ □□□□ □□□□ □□□ □□□□□□.

□□□.

- VMScaleSet1□□ VMScaleSet2□□ TCP □□ 443□ □□ □□□□ □□□□□.

□□.
□□□□□ □□□□ □□ □□
Litware□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□□.
- □□□□ □□□□ □□□ □ P2S(Point-to-Site) VPN□ □□□□ Vnet1□ □□□ □ □□□ □□□. □□□ Azure AD□ □□ □□□□□ □□□.
- □□□ □□□□□□ □□ □□ □ □□□ □□ □□
□□ □□□□□ □□□□□ □□□.
- □□□ □□□□□□ Azure □□ □□□□□ □□□□ □□□.
ExpressRoute FastPath □□□ □□□□□.
- Vnet2□ Vnet3 □□ □□□□ Vnet1□ □□ □□□□□□ □□□.
PaaS □□□□ □□ □□
Litware□ □□□□ □□□(PaaS)□ □□□ □□□□ □□ □□□ □□□ □□ □□□□□.
- storage1 □□□ □□□□□□ □□ □□□ □□ □□□□ □□□.
storage1□ □□ □□□□□□ □□□□ □□ □□□ □□□ □ □□□□.
- storage2 □□□ Vnet2 □ Vnet3□□ □□ □□□□ □□□.
storage2□ □□ □□□□□□ □□□□□.
Vnet2□ Vnet3□ □□□□ □□□. □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □□□□ □□□.
□□□□ □□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. Vnet2 □ Vnet3□ □□□□□ □□ □□□□□ □□□ □□□□□.
B. Vnet1□□ □□□□□ □□ □□□ □□□ □□□□□.
C. Vnet1□□ □□□□ □□□ □ □□ □□□□□ □□□ □□□□□.
D. Vnet1□□ □□□□□ □□□□□ □□□ □□□ □□□□□.
E. Vnet2 □ Vnet3□ □□□□□ □□□□□ □□ □□□ □□□□□.
Answer: A,D (LEAVE A REPLY)
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, Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

NEW QUESTION: 130

□□□ □□

contoso.com□□□ Azure □□□□ DNS □□□ □□□, □ □□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

Name	IP address
Vnet1	10.1.0.0/16
Vnet2	10.2.0.0/16

□□ □□□□ □□ □□ □□□ □□□□□ □□□□.

□□ □□ □□□ □□ □□□ □□□□□.

Name	IP address
VM1	10.1.10.10
VM2	10.2.10.10
VM3	10.2.10.11

contoso.com □□□ □□ □□□ □□□□ □□□□□.

- □□: VM1
- IP □□: 10.1.10.9

□□ □ □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	○	○
Deleting VM1 will delete all VM1 records automatically	○	○
Changing the IP address of VM3 will update the DNS record of VM3 automatically	○	○

Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	○	○
Deleting VM1 will delete the VM1 record automatically	○	○
Changing the IP address of VM3 will update the DNS record of VM3 automatically	○	○

Explanation:
Box 1: No
The manual DNS record will overwrite the auto-registered DNS record so VM1 will resolve to
10.1.10.9.
Box 2: No
The DNS record for VM1 is now a manually created record rather than an auto-registered record.
Only auto-registered DNS records are deleted when a VM is deleted.
Box 3: No
This answer depends on how the IP address is changed. To change the IP address of a VM manually, you would need to select `Static' as the IP address assignment. In this case, the DNS record will not be updated because only DHCP assigned IP addresses are auto-registered.
Reference:
https://docs.microsoft.com/en-us/azure/dns/dns-faq-private

NEW QUESTION: 131
□□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
- Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678
□□ □□ Azure □□□ Azure □□□□□□ □□□□□□ □□□ □□□□□. □□ □□□□□□ □□□□□□□ □ □□□□□□ □□□(WAF)□ □□□□ □□□□□.
□□□ □□□□□□ □□□□□□ □□□ □ □□ □□□ □□□□ □□□. □ □□□ 131.107.150.0/24 □□□ IP □□□□ □□ □□□ □□□□ □□□. □ □□□ □□□□ □□ □□□□□□ □□□□□□ □□□□□□ □□ □ □□□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.
Answer:

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

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

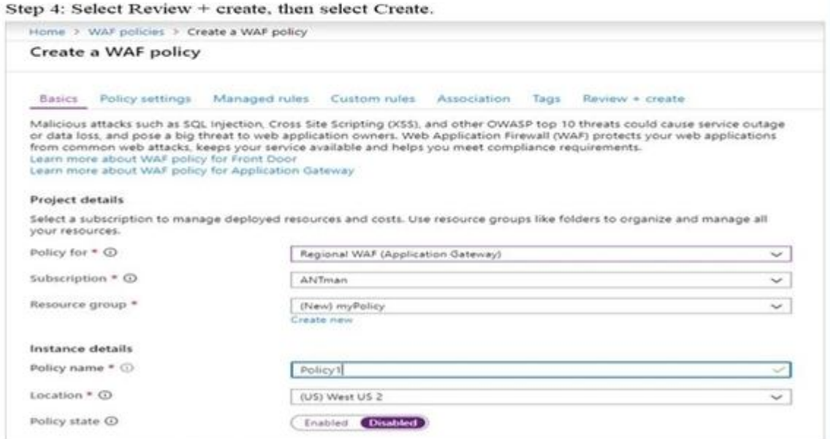
Step 1: On the upper left side of the portal, select Create a resource. Search for WAF, select Web Application Firewall, then select Create.

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

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

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

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

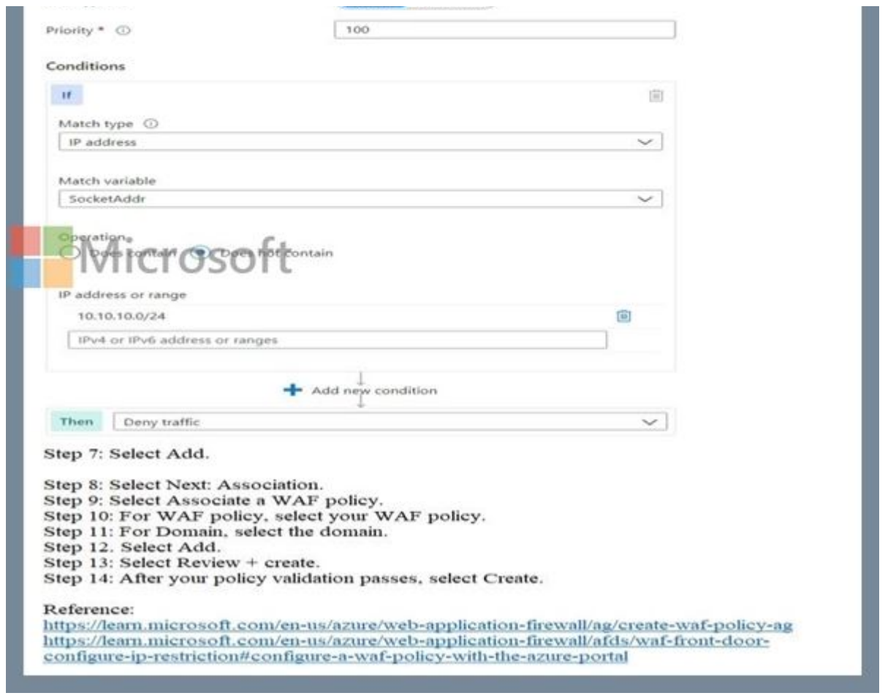


Part 2: Configure WAF rule

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

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

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



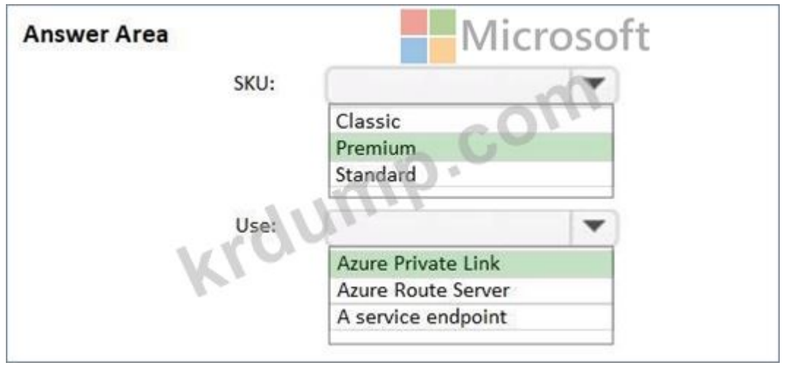
Step 7: Select Add.

Step 8: Select Next: Association.
Step 9: Select Associate a WAF policy.
Step 10: For WAF policy, select your WAF policy.
Step 11: For Domain, select the domain.
Step 12. Select Add.
Step 13: Select Review + create.
Step 14: After your policy validation passes, select Create.

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

NEW QUESTION: 132
□□□ □□
□□ □□ □□ □□ □□ □□□ □□ □□ Azure □□ □□□□ □□□ Azure □□□ □□□□. □□ □□□□ □□ □□ □□□ □□□□ □□□□□.
Azure Front Door□ □□□□ □□ □□□□ □□ □□□□ □□□ □□□□□.
□□ □□□ □□ SKU□ □□□□, □□□ □□ □□□□ □□□□ □□□□□ □ □□□ □□□□ □□□□ □□□. □□□□ □□□ □□□□□ □□□.
□□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.
□□: □□ □□□ 1□□□□.
Answer Area

Answer:



NEW QUESTION: 133

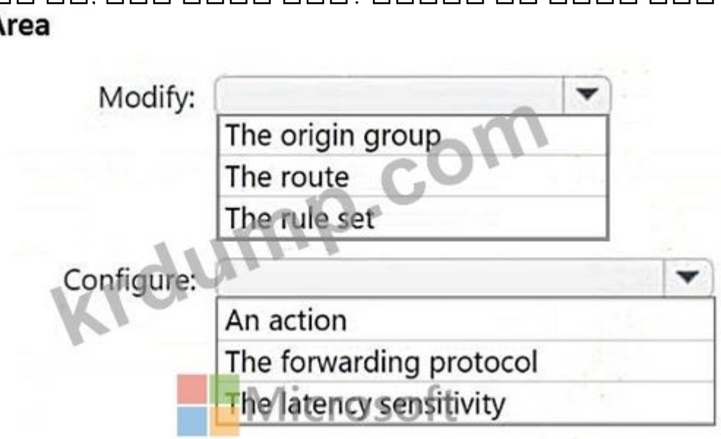
□□□ □□

□□□ Azure □□□ 6□□ Azure App Service □□ □□□□. □ □□□ □□ □□□ □□□ □□□ □□□ □□ Azure □□□ □□□□ □□□□.

□ □ □□□ □□ □□□□ □□ Azure Front Door□ □□□ □□□□□.

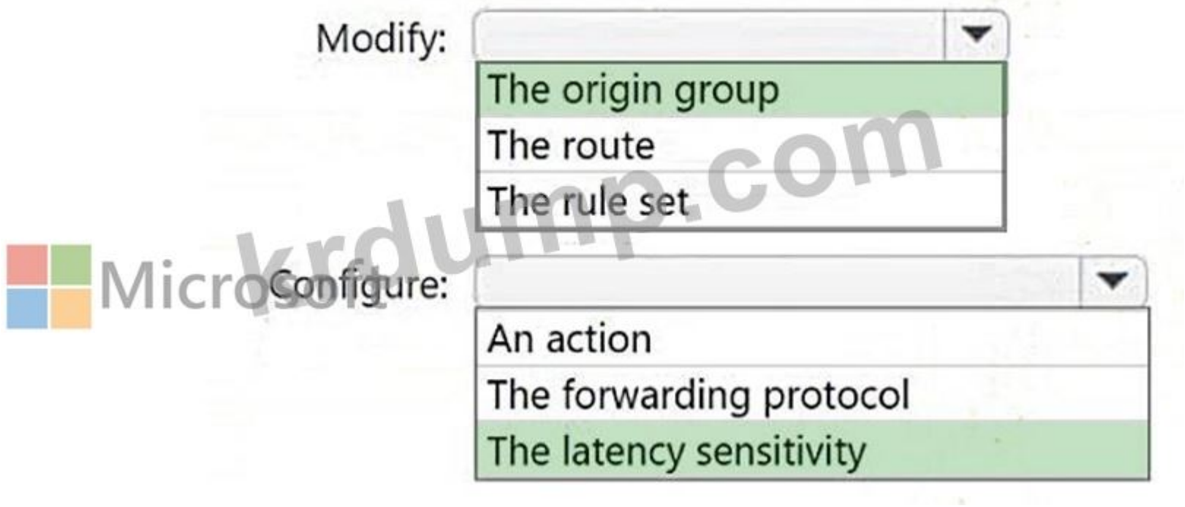
□□□ □□ □□ □□□ □□□□□ □□□□□ □□□□ □□□□ □□□ □□ App Service □□□ □□□□ □□□□□ □□ □□□. □□, □□ □□□ □□□□□ □□□.

□□□ □□□□ □□. □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:

Answer Area



NEW QUESTION: 134

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

Gateway1□□□ □□□ Azure □□ □□□□ NAT □□□□□□ □□□ □□□□□. □ □□□□ □□ □□ □□□ □□□□ □□□.

- VM1□ □□ IP □□□ □□□□ □□□□ □□□□□.
- VM2□ □□ IP □□□ □□□□ □□□□ □□□□□.
- □□□ □□□ □□□□□□ □□□.

Gateway1□ Vnet1□ □□□ □ □□□ □□□□ □□□.

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: 135
□□ □□□□□ □□□ Azure □□□ □□□□.
Azure VPN □□□□□□ 90□□ □□□ □ VPN □□□ □□□ □□□□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□ □ VPN □□□ □□□□□□ □□ □□ □□□ □□□ □□□□□ □□□.
Azure □□□□□□ □□□ □□□□□□.
- □□□ □□□□□□□.
□□ □□□□□ SKU□ □□□□ □□□?
A. VpnGw1AZ
B. VpnGw2AZ
C. VpnGw4AZ
D. VpnGw5AZ
Answer: C (LEAVE A REPLY)
Basic SKU supports max 10 S2S connections. SKUs 1, 2, and 3 support max 30 S2S connections. SKUs 4 & 5 support max 100 S2S. Of those 2, SKU4 minimizes the cost.
NEW QUESTION: 136
□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678
Azure Front Door□ □□□ □□□□ □□□□.
Front Door □□□□ □□□ □□□ □□□□ □□□. □ □□□ □□□ □□ □□□□ □□ 50□ □□□ □□□ □□□ □□□□ □□ □□□. □ □□□ □□□□ □□ □□□ Front Door □□□□□ □□□ □□□ □□□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.
Answer:

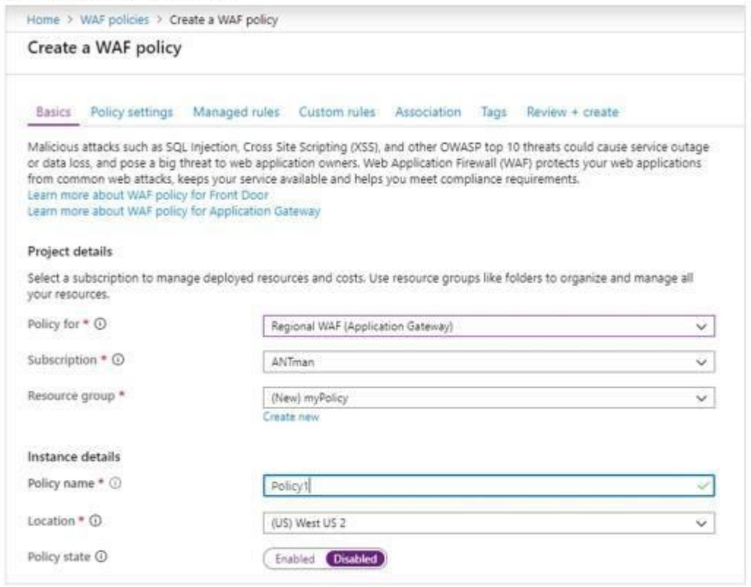
Configure a Web Application Firewall rate-limit rule
The Azure Web Application Firewall rate-limit rule for Azure Front Door controls the number of requests allowed from a particular source IP address to the application during a rate-limit duration.

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.

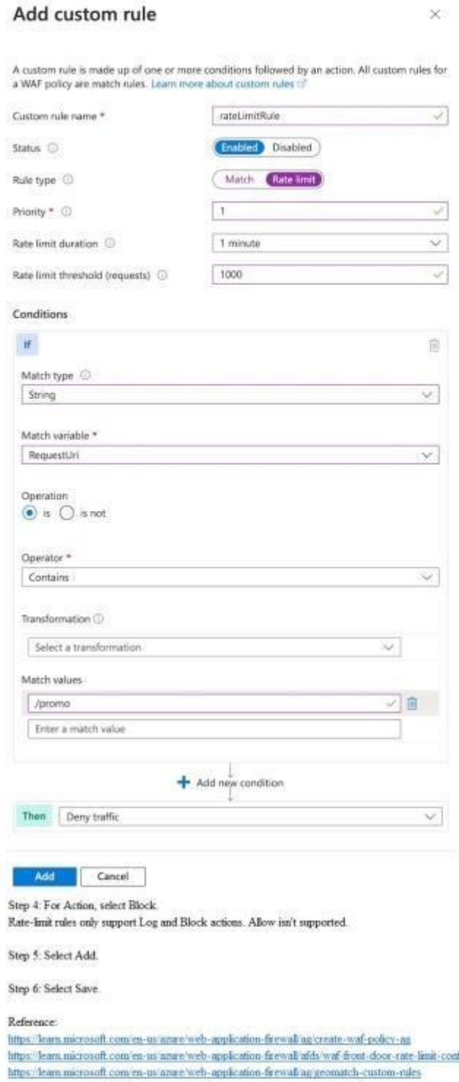
Step 2: Enter the information required to create a rate-limit rule:

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: 137
□□□ □□
□□□ □□ □□□□□ 10.1.0.0□□ 10.1.255.255□□□ IP □□ □□□ □□□□□.
□□□ □□ □□□□ □□□□ □□□ Azure □□ □□□□ □□□□ □□□ □□□□□.

- VNet1□□□ □□ □□□□
- VNet1□ □□□□□ □□□□ □□ □□□ □(S2S) VPN □□
- VNet1□ GatewaySubnet□ □□ □□ □□ □□□□□ □□□ □□□□□.

□□□□ □□□□□

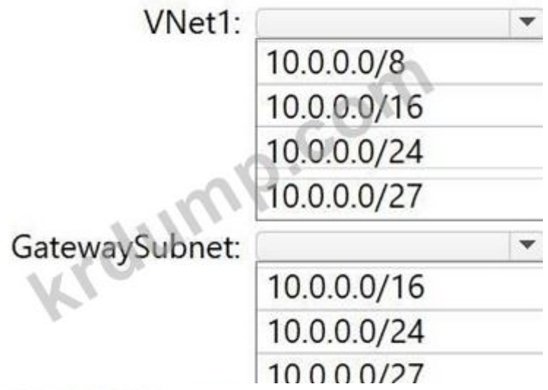
VNet1□ GatewaySubnet□ □□□ □□□ □□□□ □□□ □□□□. □□□□ □□□□ □□ □□ □□□ □□□□ □□□.

- VNet1□□ □□ □□□ IP □□ □□ □□□□□□.
- GatewaySubnet□□ □□ □□□ IP □□ □□ □□□□□□.

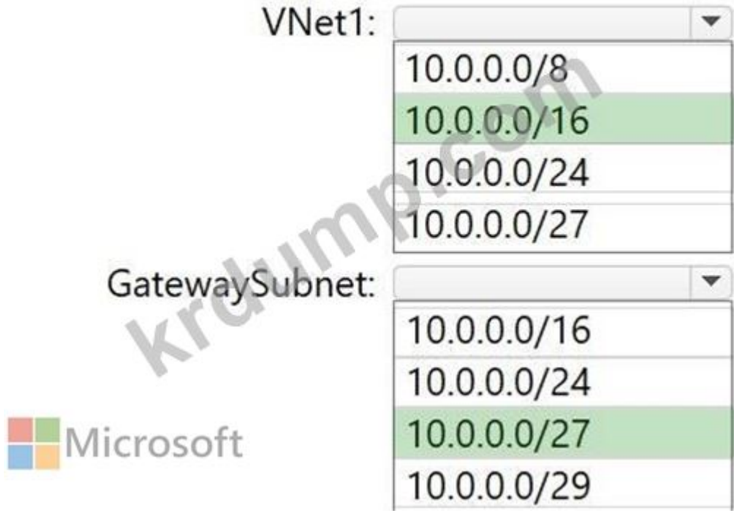
VNet1□ GatewaySubnet□ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area



Answer Area



NEW QUESTION: 138

Azure □□ □□□□ Vnet1□ □□□□.
Vnet1□ □□ □□□ □□ □□ Azure □□□ Azure SQL □□□□□ □□□□ □ □□□ □□ □□□.
□□ □□□ Azure Storage □□□□ □□□□□ □□□□ □□□□ □□□.
□□ □ □□ □□□□□ □□□□ □□ □□(NSG) □□□ □□□□ □□□? □ □□□ □□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. Vnet1□ IP □□ □□□ Sql.EastUS□ □□□ □ □□□□ □□ □□ □□
B. □□□ VirtualNetwork□□ □□□ Sql□ □□ □□
C. □□□ VirtualNetwork□□ □□□ 168.63.129.0/24□ □□ □□
D. □□□□□ □□ □ □□□□ Vnet1□ IP □□ □□□ □□□□ □□ □□
Answer: A,D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview

NEW QUESTION: 139
□□ □□ 3 - □□□ □□□□
□□
□□□□□(Proseware, Inc.)□ □□□□ □□□ □□ □□□□□□□ □□□ □ □□ □□□ □□□□□.
□□ □□. □□□□□ □□
Proseware□ corp.proseware.com□□□ □□□ □□□□□ Active Directory Domain Services(AD DS) □□□□□ □□□□ □□□, □ □□□□□ proseware.com□□□ □□□ Microsoft Entra □□□□ □□□□□□.
Proseware□ proseware.com□ □□□ Azure □□□ □□□□ □□□□.
Proseware□ □□ □□ □□(CA)□ □□□□ □□□□.
□□ □□. □□□□ □□□
□□ □□□□□ □□ □□ □□□ □□ □□□□ □ □□□□ □□□□ □□□□.

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□ ExpressRoute □□□ □□□□ Azure□ □□□□□.
SFONet□ □□□ □(S2S) VPN□ □□□□ Azure□ □□□□□.
□□ □□. Azure □□□
Azure □□□□ □□ □□ □□□ □□ □□□□ □ □□□□ □□□□ □□□□.

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

□□□□ VM1, VM2, VM3, VM4□□ □□□ □□ □□ 4□□ □□□□ □□□□. VM1□ VM2□ App1□□□ □□ □□□□□□.

VM3 □ VM4□ app2.proseware.com□□□ FQDN□ □□□□ □□□□ □ □□ App2□□ □ □□□□□□□ □□□□□□. □□□□ HTTP □□ HTTPS□ □□□□ app2.proseware.com□ □□□□□□.

VM1, VM2, VM4□ SpokeVNet□ □□□□ □□□□.

□□□□ □□ □□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □□□□.

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

□□□□ FD1□□□ Azure Front Door Standard □□□□ □□□□ □□□□. FD1□□ □□ □□□□□ □□□ □□□□ APPGW1□ □□□□ □□ □□ □□ □□□ □□□□ □□□□.

HubVNet□ ERGW1□□□ ExpressRoute □□□□□□ □□□□ NYCNet□ □□□□□.

□□□ □□ □□ □ □□ □□. □□□ □□ □□

Proseware□ □□□ □□ □□ □□□ □□□ □□□□□.

- PRDNS1□□□ □□□ Azure □□□□ DNS □□□□ HubVNet□ □□□□ PRDNS1□ SpokeVNet□ □□□□□.
- DNSRS1□□□ □□□ DNS □□□ □□ □□□ □□□□, DNSRS1□ PRDNS1□ □□□□□.
- Azure □□ □□□□ □□□□ □□□□ □□ □□□ □□□□□.
- □□□□□ □□□□□□ SUBNET-JUMPHOSTS□ TCP □□ 3389□ □□ □□□□ □□□ □□□□□.
- □□□□□ SpokeVNet□□ □□□□ TCP □□ 80 □□□ □□□□□.
- Azure Virtual Network Manager □□□ □□□□ NSG □□□□ □□ □□□□□ □□□.
- HubVNet□ NVA1 □ NVA2□□ □□□ □□□□ □□ □□□□□□(NVA) □ □□ □□□□□.
- HubVNet□ LBGW1□□□ □□□ □□□□□ □□ □□□□ □□□□□.
- NVA1 □ NVA2□ □□□□ LBGW1□ LBS1□□ TCP □□ 443, 1433 □ 1434□ □□□□ □□□□□ □□□□□.

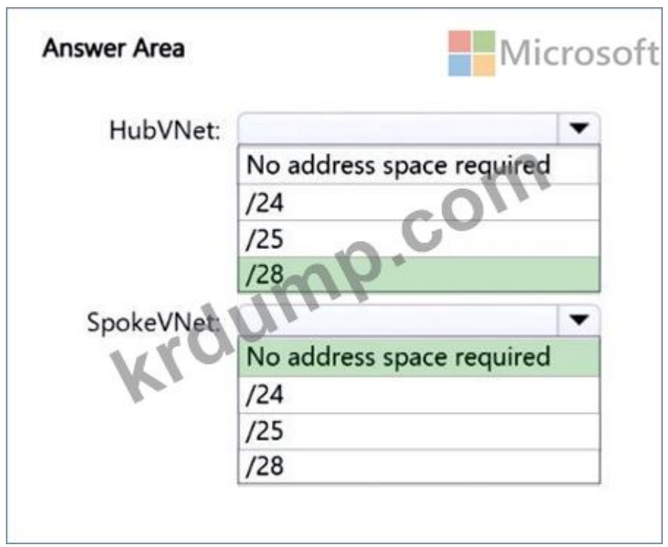
- App2□ □□□ □□ □□□□ FD1□ □□□□ □□□□□ □□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□ □□ □□□ □□□□□.
- Azure Virtual Network Manager □□□ □□□□ □□□□□□.
- NYCNet□ SFONet □□ □□□□ ExpressRoute □□ □ S2S VPN□ □□ □□□□□□.
- Windows 11 □□□ □□ □□□□ P2S(Point-to-Site) VPN□ proseware.com □□ □□□ □□□□ HubVNet□ □□□ □ □□□ □□□□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□ □□ □□□ □□□□□.
- □□□ □ □□ CA□ □□□□□□.
- APPGW1□ □□ □□□□□ □□ □□□ □□ □ □□□□ □□□□□ □□□□.
- Azure□□ □□□□□ □□ □□ □□□ □□□ □□ □ □□□□ □□□□□ □□□□□□.
- app2.proseware.com□□ □□□□ □□ □□□ □□□□ FD1□ □□ □□□□□□ □□□□.
- NYCNet□ □□□□ □□□ □□ □□□□□□ □□□□ Azure □□□□ □□□□□ □□□□ □□□.
- HubVNet □ SpokeVNet□ □□□□ □□ □□□ □□□□ □□□□□□ □□□□ Azure □□□□ □□□□ □ □□□ □□□□□.
□□□ □□ □□ □ □□ □□. □□ □□ □□
Proseware□ □□□ □□ □□□□ □□ □□□ □□□□□.
- □□□□□ □□□□ □□□□ □□ □□□□□ □□□□ □ □□□ IP □□ □□□ □□□□□□.
- SpokeVNet□□ azure.proseware.com □□□□□□□ corp.proseware.com □□□□□□□ □□ □□ □□ □□□ PRDNS1□ □□□□ □□□□□.
- □□□ □ □□□ □□□ □□□□□□□.
□□□ □□
HubVNet □ SpokeVNet□ PRDNS1□ □□□□ □□ □□□ IP □□ □□□ □□□□ □□□. □□□□ □□□□ □□ □□□ □□□□ □□□.
□ □□ □□□□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area Microsoft

HubVNet:
- No address space required
- /24
- /25
- /28

SpokeVNet:
- No address space required
- /24
- /25
- /28

Answer:



NEW QUESTION: 140
Azure □□□□ VNet1, VNet2, VNet3, VNet4□□ □□□ □□ □□□□ 4□□ □□□□ □□□□.
□□ □□□□ □□□□ □□□□ □□ □ □□□ □□□□□ □□□ □□□□□.
VNet1□ □□ □□□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□ □ □□□ □□ □□□ □□□□□.
- □□□□ □□□□ □□□□□□.
□□□□ □□□ □□□□ □□□?
A. Azure VPN □□□□□
B. Azure □□□ □□
C. Azure Private Link
D. Azure □□□
Answer: D (LEAVE A REPLY)
If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.
You can also use a VPN gateway to route traffic between spokes, although this choice affects latency and throughput. For configuration details, see Configure VPN gateway transit for virtual network peering.
https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli

NEW QUESTION: 141
□□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678
□□□ □□□ □□□ □□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□ □□□□ □□□□. □□□ □□ □□□ ny.contoso.com□□□ □□□ □□□ □□□□ □□□ □ □□□□.
□□□ □□□ □□□ de.contoso.com□□□ □□□ □□□ □□□□ □□□ □ □□□□.
□ □□□ □□ □□□□□ □□ □□□ □□□ □□□□ □□□. □□□□ □□□□ □□□□ □□□□ de.contoso.com□□, □ □ □□ □□□□ ny.contoso.com□□ □□□□□□ □□ □□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.

Answer:


Rewrite HTTP request and response headers with Azure Application Gateway - Azure portal

Sign in to Azure
Step 2: Sign in to the Azure portal with your Azure account.

Configure header rewrite
In this example, we'll modify a redirection URL by rewriting the location header in the HTTP response sent by a backend application.

Step 2: Select All resources, and then select your application gateway.

Step 3: Select Rewrites in the left pane.

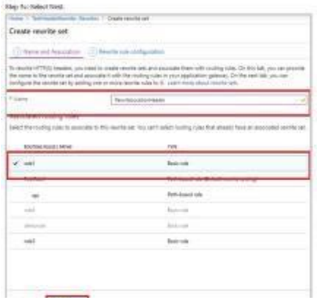
Step 4: Select Rewrite set.

Step 5: Provide a name for the rewrite set and associate it with a routing rule.

Step 6: Enter the name for the rewrite set in the Name box.

Step 7: Select one or more of the rules listed in the Associated routing rules list. You can select only rules that haven't been associated with other rewrite sets. The rules that have already been associated with other rewrite sets are dimmed.

Step 8: Select Next.



Step 4: Create a rewrite rule

Step 4a: Select Add rewrite rule

Step 4b: Enter a name for the rewrite rule in the Rewrite rule name box. Enter a number in the Rule sequence box.

Step 5: In this example, we'll rewrite the location header only when it contains a reference to sitenewsites.net. To do this, add a condition to evaluate whether the location header in the response contains sitenewsites.net

Step 5a: Select Add condition and then select the box containing the If instructions to expand it.

Step 5b:
In the Type of variable to check list, select HTTP header.

In the Header type list, select Response.

Because in this example we're evaluating the location header, which is a common header, select Common header under Header name.

In the Common header list, select Location.

Under Case-sensitive, select No.

In the Operator list, select equal (=).

Step 5c: Enter a regular expression pattern. In this example, we'll use the pattern (https?)://(.*)sitenewsites.net(.*)$. [Enter in sitenewsites]

Step 5d: Select OK.

Step 6: Add an action to rewrite the location header:

Step 6a: In the Action type list, select Set.

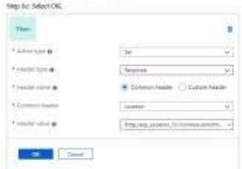
In the Header type list, select Response.

Under Header name, select Common header.

In the Common header list, select Location.

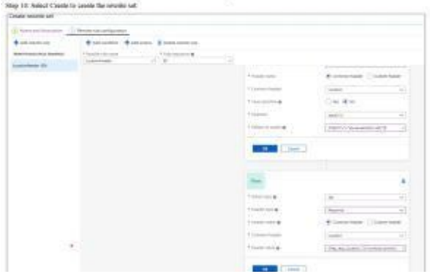
Step 6b: Enter the header value. In this example, we'll use {http_resp_Location_1}.sitedrive.com/{http_resp_Location_2} as the header value. This value will replace sitenewsites.net with sitedrive.com in the location header. [Enter exactly like in the example: {http_resp_Location_1}.sitedrive.com/{http_resp_Location_2}]

Step 6c: Select OK.



Step 9: Repeat steps 6 to 8c but in step 8c Enter the sitedrive.com instead of ey.contoso.com.

Step 10: Select Create to create the rewrite set.



NEW QUESTION: 142
□□□□ fabrikam.com□□□ □□ DNS □□□ □□□□□ Server□□ □□□ □□□□□ DNS □□□ □□□□.
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□□□ □□□□□ □□□□ □□□ □ VPN(S2S)□ □□□□ □□ □□ □□□□□ □□□□ □□□□ □ □□□□.
□□ □□ □□□ □□□□ Azure DNS □□□□ □□□ □□□□ □□□□ □□□.
- □□ □□□□□ □□□ □□□□ □□ □□□ □□□□ □□□.
fabrikam.com□ DNS □□□□□.
- Server1□ □□ □□□□ DNS □□□ □□□ □ □□□ □□□.
contoso.com.
- □□□□ □□□ □□ □□□ □□□□□ □□□.
□□□□ □ □□ □□□ □□ □ □□□□?
A. 1
B. 2
C. 3
D. 4
Answer: A (LEAVE A REPLY)
Private DNS zone is global. Private DNS resolver is restricted to the location of the VNET, but it can lookup any address in the private DNS zone as long as it's linked. So 1 private DNS resolver should be sufficient.

NEW QUESTION: 143
Azure □□□□ WebApp1□□□ □□□ Azure App Service □ □□ FDProfile1□□□ □□□ Azure Front Door □□□□ □□□□. FDProfile1□ □□ □□□ □□□ □□□ □□□□□.
https://www.contoso.com□□ WebApp1□□.
WebApp1□□ □□□□ □□□ https://www.contoso.com/users/* □ □□□ □□□ □□□□□ □□ □□□.

FDProfile1□□ □□□ □□□□ □□□?

A. □□

B. □□ □□

C. □□

D. □□□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 144

https://learn.microsoft.com/en-us/azure/frontdoor/front-door-route-matching?pivots=front-door-standard-premium

□□□□□

□□□ □□□ □□□□

□□□ □□ □□ □□□ □□ □□□ □□□□□□.

- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx

Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

- □ □□□□: 12345678

Azure □□□□ □□□□ fabrikam.com□□□ □□□□ □□ DNS □□□□ □□□ □□□□□.

wvw.fabrikam.com□ 131.107.2.50□□ □□□□□ □□□□ □□□.

□ □□□ □□□□□ Azure □□□ □□□□□□.

Answer:

Create an Azure DNS zone [already done] and record using the Azure portal

Create a DNS record
DNS records are created for your domain inside the DNS zone. A new address record, known as an 'A' record, is created to resolve a host name to an IPv4 address.

To create an 'A' record

Step 1: In the Azure portal, under All resources, open the fabrikam.com DNS zone. You can enter fabrikam.com in the Filter by name box to find it more easily.

Step 2: In the Add a record set window, enter or select the following values:

Step 3: At the top of the fabrikam.com DNS zone page, select + Record set.
Name: Type www. This record name is the host name that you want to resolve to the specified IP address.
Type: Select A. 'A' records are the most common, but there are other record types for mail servers ('MX'), IP v6 addresses ('AAAA'), and so on.
TTL: Type 1. Time-to-live of the DNS request specifies how long DNS servers and clients can cache a response.
TTL unit: Select Hours. The time unit for the TTL entry is specified here.
IP address: Type 131.107.2.50. This value is the IP address that the record name resolves to. In a real-world scenario, you would enter the public IP address for your web server.

Step 4: Select OK to create the A record.

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

NEW QUESTION: 145
□□□ □□
Azure □□□□ Vnet1□ Vnet2□□ □ □□ □□ □□□□□ □□□□ □□□□.
fabrikam.com□□□ □□□ □□ DNS □□□ □□□□□. □□ □□□ □□ DNS □□ □□□ □□□ □□ □□□□□.

Name server 3 : ns3-06.azure-dns.org.

Name server 4 : ns4-06.azure-dns.info.

Tags (change) : Click here to add tags

You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value
@	NS	172800	ns1-06.azure-dns.com. ns2-06.azure-dns.net. ns3-06.azure-dns.org. ns4-06.azure-dns.info.
@	SOA	3600	Email: azuredns-hostmaster.microsoft.com Host: ns1-06.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1
appservice1	A	3600	131.107.1.1
www	CNAME	3600	appservice1.fabrikam.com

fabrikam.com□□□ □□□ □□□□ DNS □□□ □□□□. □□ □□□ □□□□ DNS □□ □□□ □□□ □□ □□□□ □□□□.

Private DNS zone

+ Record set → Move ⌄ 🗑 Delete zone ↻ Refresh

^ Essentials JSON View

Resource group (change) : rg1

Subscription (change) : Subscription1

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

Tags (change) : Click here to add tags

You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.co... Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False

Subscription (change) : Subscription1

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

Tags (change) : Click here to add tags

You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value	Auto registered
			Email: azureprivatedns-host.microsoft.co... Host: azureprivatedns.net	

@	SOA	3600	Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
appservice1	A	3600	131.107.100.10	False
server1	A	3600	131.107.100.1	False
server2	A	3600	131.107.100.2	False
server3	A	3600	131.107.100.3	False
www	CNAME	3600	appservice1.fabrikam.com	False

□□ □□□□ □□ □□□ □□ □□ □□□□ □□□ □□□□ □□□□.

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
Queries for www. fabrikam.com from the internet are resolved to 131.107.1.1.	○	○
Queries for server1.fabrikam.com can be resolved from the internet.	○	○
Queries for www. fabrikam.com from Vnet2 are resolved to 131. 107.100. 10.	○	○

Answer:

Answer Area

Statements	Yes	No
Queries for www. fabrikam.com from the internet are resolved to 131.107.1.1.	○	○
Queries for server1.fabrikam.com can be resolved from the internet.	○	○
Queries for www. fabrikam.com from Vnet2 are resolved to 131. 107.100. 10.	○	○

Explanation:
Box 1: Yes
DNS queries from the internet use the public DNS zone. In the public DNS zone, www.fabrikam.com is a CNAME record that resolves to appservice1.fabrikam.com which resolves to 131.107.1.1.
Box 2: No
DNS queries from the internet use the public DNS zone. There is no DNS record for server1.fabrikam.com in the public DNS zone.
Box 3: No
The private DNS zone is linked to VNet1, not VNet2. Therefore, resources in VNet2 cannot query the private DNS zone.

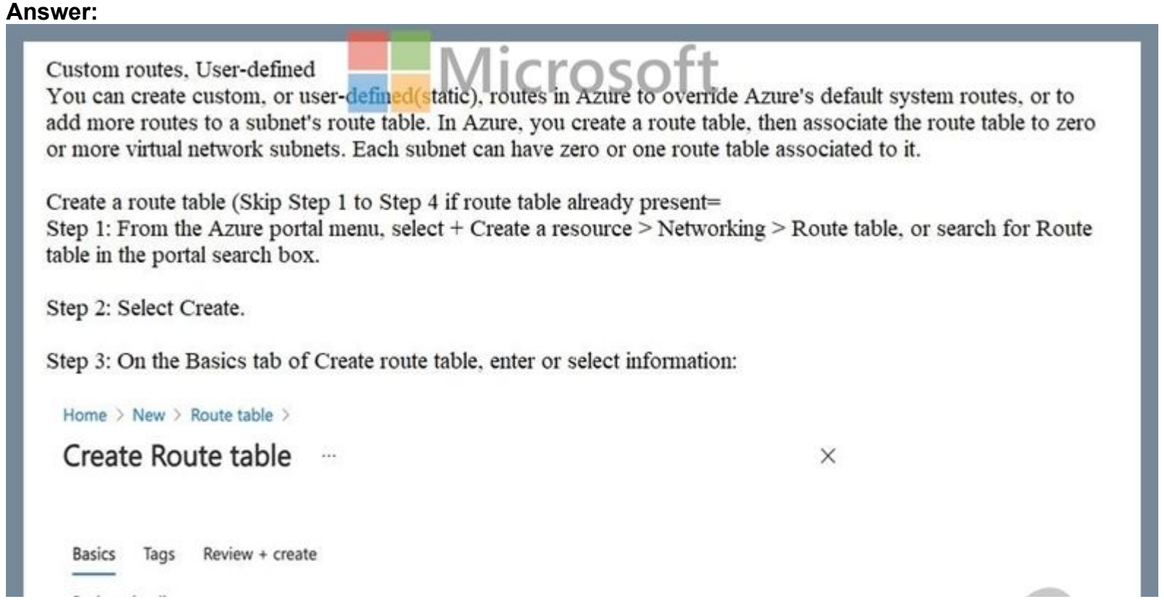
NEW QUESTION: 146
□□□□□

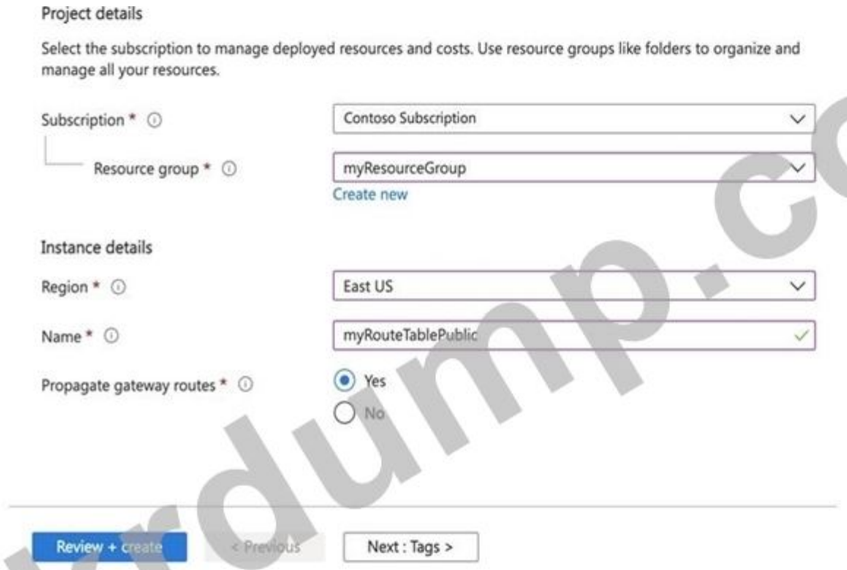
□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
- Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678

□□□ 1-2□ □□□□ □□□ □□□□□. □□ □□□□ IP □□□ 10.1.2.4□□□.
□□□ 1-1□□ 192.168.10.0/24 IP □□ □□□ □□□ □□□□ □□□ 1-2□ □□□ □□□□ □□ □□□□□□ □□ □□□. □ □□□□ □□ □□□ □□□□□ □□□□ □□ □□□□ □□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.

Answer:





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.
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: 147
□□ □□ Azure □□□ □□ □□ □□□ □□□ Azure □□□ □□□□.
□□□ □□□ □□□□ □□□.
□□ □□□ □ □□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
(□ □□ □□□□□.)

□□: □□□ □□□ □□□ 1□□ □□□□□.
A. Azure Monitor □□ □□
B. □□ □□ □□ □□
C. □□ □□
D. Azure Sentinel □□ □□
E. Azure Monitor □□□ □□ □□
Answer: B,C (LEAVE A REPLY)
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-

NEW QUESTION: 148
Site1□□□ □□□ □□□□□ □□□□□ □□□□.
VNet1□□□ □□ □□□□□ storage1□□□ □□□□ □□□ □□□ Azure □□□ □□□□.
Site1□ VNet1□ □□□ □(S2S) VPN□ □□□□ □□□□ □□□□.
Site1□ □□□□ S2S VPN□ □□□□ storage1□ □□□ □ □□□ □□ □□□. □□□□ □□ □□□ □□□□□ □□□.
VNet1□ □□□ □□□□ □□□?
A. Azure □□□□□□ □□□□□
B. □□□ □□□□□
C. □□□ □□□□□
D. Azure Private Link □□□
Answer: C (LEAVE A REPLY)

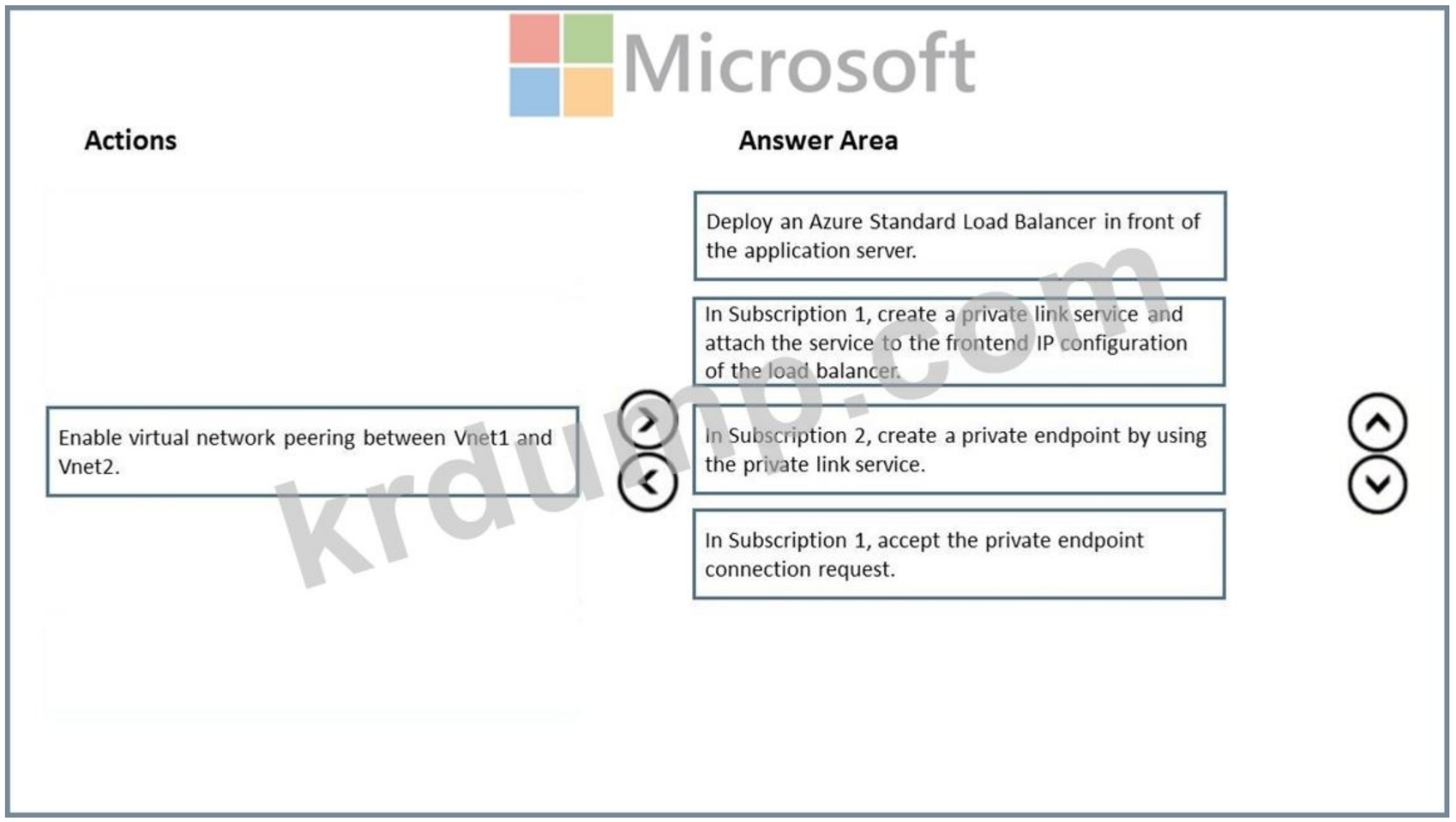
NEW QUESTION: 149
□□□ □ □□ □□
Subscription1□ Subscription2□□ □ □□ Azure □□□ □□□□. Subscription1□□ Vnet1□□□ □□ □□□□□ □□□□ □□□□.
Vnet1□□ □□□□□□ □□□ □□□□ □□□□. □□2□□ Vnet2□□ □□□ □□ □□□□□ □□□□ □□□□.
Vnet2□ □□ □□□ □□□□ □□□□□□ □□□□ Vnet1□ □□□□□□ □□□ □□□□ □ □□□ □□ □□□.

Actions

- In Subscription 1, accept the private endpoint connection request.
- In Subscription 1, create a private link service and attach the service to the frontend IP configuration of the load balancer.
- Enable virtual network peering between Vnet1 and Vnet2.
- Deploy an Azure Standard Load Balancer in front of the application server.
- In Subscription 2, create a private endpoint by using the private link service.

Answer Area

Answer:



Explanation:

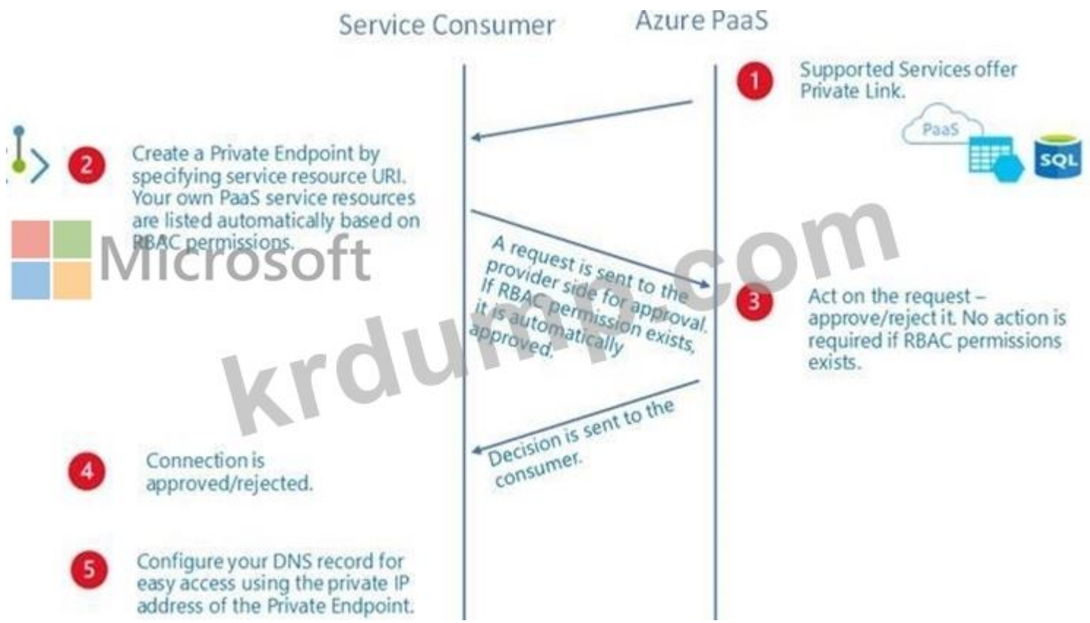
Step 1: Deploy an Azure Load Balancer in front of the application server Configure your application to run behind a standard load balancer in your virtual network.

Step 2: In Subscription 1, create a private link service and attach the service to the frontend IP configuration of the load balancer.

Create a Private Link Service referencing the load balancer above.

Step 3: In Subscription 2, create a private endpoint by using the private link service.

Private Link service can be accessed from approved private endpoints in any public region. The private endpoint can be reached from the same virtual network, regionally peered VNets, globally peered VNets and on premises using private VPN or ExpressRoute connections.



Step 4: In Subscription1, accept the private endpoint connection request.

Network connections can be initiated only by clients that are connecting to the private endpoint.

Not:

Incorrect: Enable virtual network peering between Vnet1 and Vnet2.

Reference:

https://docs.microsoft.com/en-us/azure/private-link/private-link-service-overview

https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview

NEW QUESTION: 150

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

VM1□ VM2□ □□□□1□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

- VM1□ VM2□ □□ □□□□ □□□ □□□□ □□□□ □□□□□.
- storage1□ □□□□□ □□ □□□□ □□□□□□.

□□□ □□□□ □□□?

A. □□□□ □□ □□(NSG)

B. □□□ □□□□□ □□

C. □□□ □□

D. □□□ □□□□□

Answer: B (LEAVE A REPLY)

Virtual Network (VNet) service endpoint policies allow you to filter egress virtual network traffic to Azure Storage accounts over service endpoint, and allow data exfiltration to only specific Azure Storage accounts. Endpoint policies provide granular access control for virtual network traffic to Azure Storage when connecting over service endpoint.
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview

NEW QUESTION: 151
□□□□ □□□□, □□□, □□ □ IP □□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□□. □ □□□□ □□□ □□ □□ □□□□ □□□□□ □□□ □□□ □□□□ □□□.
□□□□: □□□□ □□□ □□□ □□ □□ □□□ □□□ □□ □□ □□ □□□ □□ □□□□□ □□□.
□□ □□. Basic □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)
Basic is chosen for the scenario where all the requests from different domains must be accepted and moved to the backend pools. On the other hand, where incoming requests must be moved to the different backend pools depending upon the host names or host header, you need to select a multi-site listener. In this case, you should mention a hostname that will match the new incoming request.
Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/configuration-listeners?WT.mc_id=modinfra-33046-thmaure

NEW QUESTION: 152
□□ □□ 2 - □□□ □□□□
□□
□□□ □□□□□ □□□□□□□ □□□ □□ □□□□ □□□ □ □□□ □□□□□.
Contoso□ □□ Azure □□□ □□□□□ Azure□□ □ □□ □□ □□□□□ □□□□ □□□□.
□□ □□:
Azure □□□□ □□□
Contoso□ contoso.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. □□ Azure □□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

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**

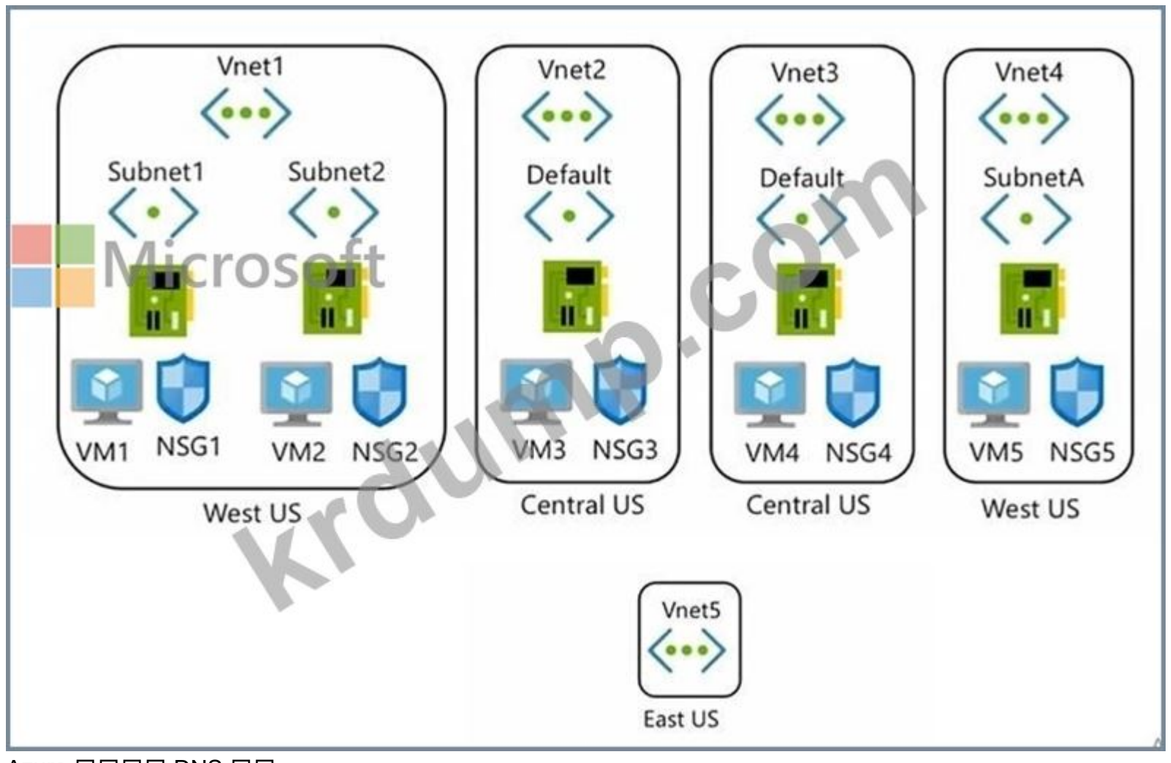
Vnet1□□ GW1□□□ □□□ □□ □□□□ □□□□□□ □□□□ □□□□.
Azure □□ □□
Azure □□□□ □□ □□ □□□ □□□ Windows Server 2019□ □□□□ □□ □□□ □□□□ □□□□.

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

NSG(□□□□ □□ □□)□ □□ □□□ □□□□ □□□□□□ □□□□ □□□□. □ NSG□□ □□□□□ RDP □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□□. □ □□ □□□ □□□□ ICMP □□□□ □□□□ □.

ASG1□□□ □□□□□□ □□ □□□ VM1□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□□□ □□□ □□□□□



Azure □□□□ DNS □□

Azure □□□□ □□ □□ □□□ Azure □□□□ DNS □□□ □□□□ □□□□.

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

Zone1.contoso.com□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

□□ Azure □□□

Azure □□□□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.

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

□□ □□:

□□ □□□□ □□ □□

Contoso□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□.

- □□ □□ □□□ Vnet6□□□ □□□ □□ □□□□□ □□□□, □□ □□□□□ □□ □□□□ □□□ □□□□□□□.

Vnet6□ □□□□ □ □□ □□□□ □□

Vnet6□ □□□ □ □□ □□ □□

Vnet6□ □□ VPN □□ □□□ □□□□□.

Vnet6□ □□□□ KeyVault1, DB1 □ Vnet1□ □□□□ □ □□□ □□□□□.

□□□□□□□ □□ □□□□

- Vnet4□ Vnet5□ □□ □□□□ □□ □□□ □ □□□ □□□.

□□□□□□□ □□ □□□□□ □□.

- VM-Analyze□□ □□□ □□ □□□ Subnet1□ □□□□□. VM-Analyze□ Subnet2□□ □□□ □□□□ □□□□ □□□□ □□□.

□□□.

□□□□ □□ □□ □□

Contoso□ □□□ □□ □□□□ □□ □□ □□□ □□□ □□□□.

- P2S(Point-to-Site) VPN □□□□ □□ Azure Active Directory(Azure AD) □□□ □□□□□.
- NSG3 □ NSG4□ □□ NSG □□ □□□ □□□□□□.
- Vnet1/Subnet1□ □□□ NSG10□□□ □□□ NSG□ □□□□□.

□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.

□□□.

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

- Vnet1/Subnet2□ □□□ NSG11□□□ □□□ NSG□ □□□□□.

□□□ □□ □□ □□□ □□□ □□ □□□□□ □□ □□□ □□□□□.

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

□□□ □□

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

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.	○	○

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.

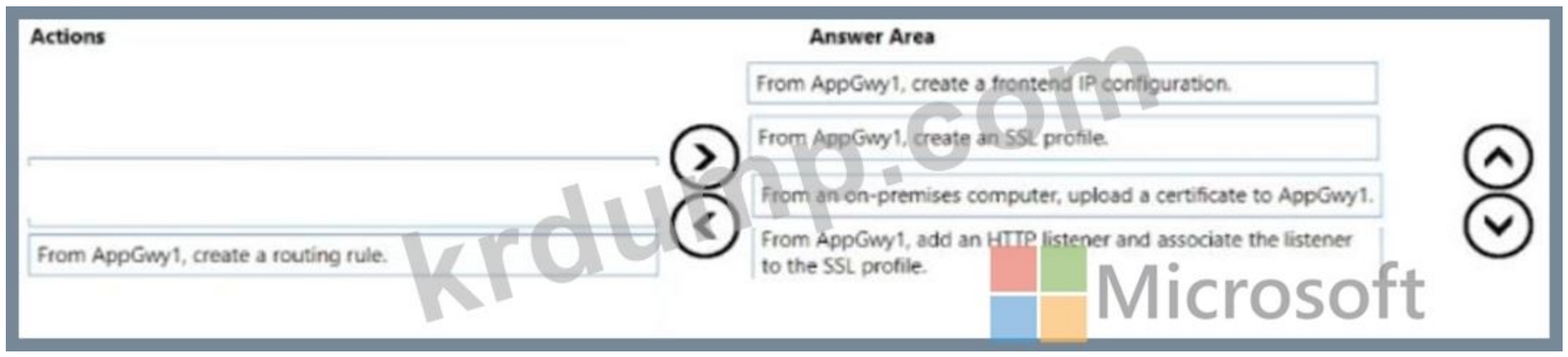
NEW QUESTION: 153
□□□ □ □□ □□
□□□□□ □□□□□□ □□ □□ □□(CA)□ □□ contoso.com□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□.
Azure □□□ □□□□ □□□□.
AppGwy1□□□ □□□ Azure □□□□□□ □□□□□□ □□□□ □□ □□□ □□□□□.

- HTTP □□□□ □□□□□.
- □□□□ □□□ □□□ □□□□□.

□□□□ □□□ □□□□□ contoso.com□□ □□□□ □□□ □□ □□ □□□ □□□□□ AppGwy1□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.

Answer:



Explanation:

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

NEW QUESTION: 154

Subnet1□□□ □□□□ □□□ Azure □□ □□□□□ □□□□. Subnet1□ NSG1□□□ □□□□ □□ □□(NSG)□ □□□□ □□□□. NSG1□ □□□□□ □□□□ □□ □□ □□□□□ □□□□ □□□□□.

Subnet1□□ Azure Cosmos DB □□□□ □□□□ □□ □□ □□□ □□□□ □□□□.

□□ □□□ Azure Cosmos DB□ □□□ □ □□□ NSG1□□ □□□□□ □□ □□□ □□□□ □□□.

□□□□ □□□ □□□□ □□□?

A. □□□ □□

B. □□ □□□□□

C. □□□ □□

D. □□□□□□ □□ □□

Answer: A (LEAVE A REPLY)

What is service tag in Azure?

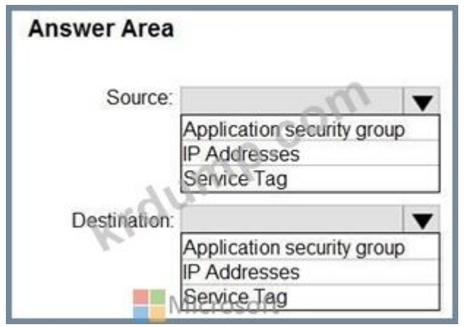
Image result for azure service tags

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: 155
□□□ □□
Azure □□□ □□□□. □ □□□□ □□ Azure SQL Database □□□□ 5□□ □□□□□ □□□ VNet1□□□ □□ □□□□□ □□□□ □□□□. □□ □□□□ NSG1□□□ □□□□ □□ □□(NSG)□ □□□□ □□□□.
NSG1□ □□□ □□ □□□ □□□ □□□ □□□□ □□ □□□□□ □□□□ □□□□□.
□ □□□□□ 50□□ □□ □□□ □□□□□. □□ □□ □□□□ SQL Server □□□□□ □□□□□ Azure SQL Database □□□□ □□□□□ □□□□□.
□□ □□ □□□□□ SQL Server□ Azure SQL Database □□□□ □□□ □ □□□ NSG1□ □ □□□□□ □□□ □□□□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□□.
- SQL □□□□□ □□□ □ NSG1□ □□ □□ □□□ □□□□□□.
□□ □□□ □□□ □□□□□□□.
- □□ □□ □□□□□ SQL Server□ Azure SQL Database □□□□ □□□ □ □□□ □□□□.
□□□ □□ □□□ □□ □ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

NEW QUESTION: 156
□□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
- Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678

storage12345678 □□□□ □□□ VNET1□ □□□□□□ □□□ □□□□□ □□□□ □□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.

Answer:

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.

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

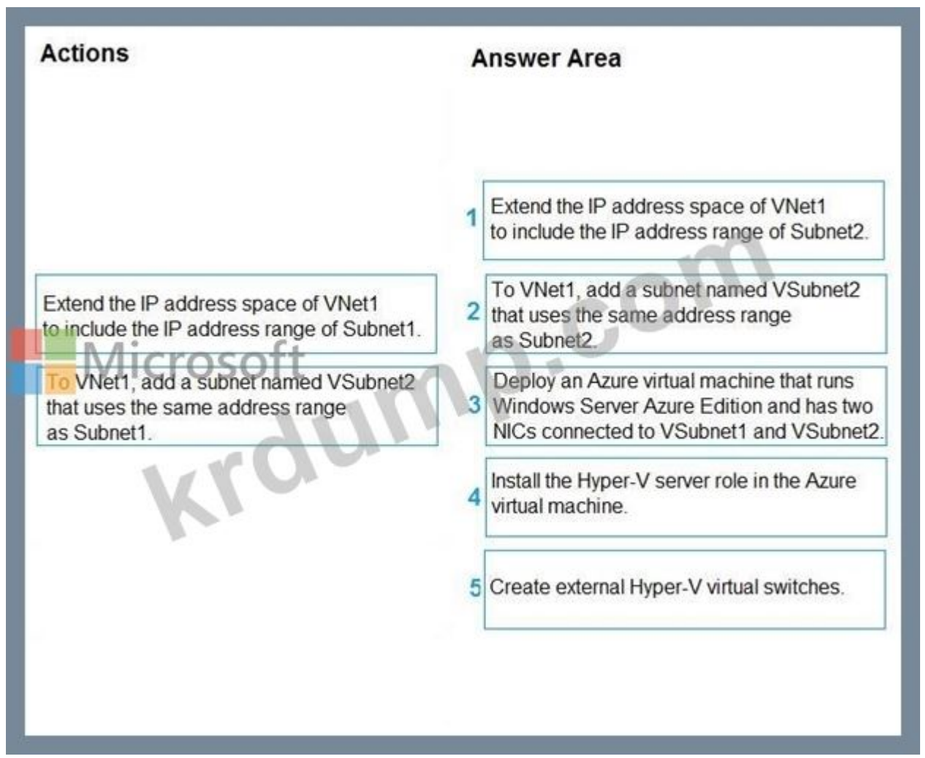
NEW QUESTION: 157
□□□ □ □□ □□
□□□□□ □□□□□□ Subnet□ Subnet2□□ □ □□ □□□□ □□□□. Subnet2□□ VM1□ VM2□□ □ □□ □□ □□□ □□□□ Hyper-V □□□□ □□□□. VM1□ VM2□ Subnet2□ □□□□ □□□□.
VNet1□□□ Azure □□ □□□□□ □□□, □ □□□□□□ GatewaySubnet□ VSubnet1□□□ □□□□ □□□□. VNet1□ □□□ □(S2S) VPN □□□ □□□□ □□□□□ □□□□□ □□□□ □□□□.
VM1□ VNet1□□ □□□□□□□□ VM1□ □□ IP □□□ □□□ □□□□□. VM2□ Subnet2□ □□□ □□□□□.
□□□□□□□ □□□ □ VM1□ VM2□ □□□ □ □□□ □□□ □□□□ □□□.
□□ □□ □□ □□□ □□□□ □□□□ □□□. □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.

Actions

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

Answer Area

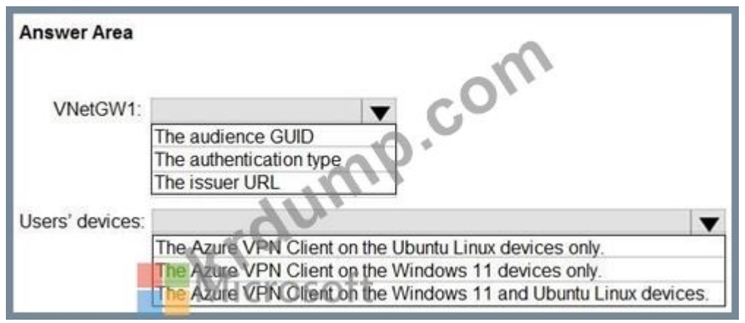
1
2
3
4
5



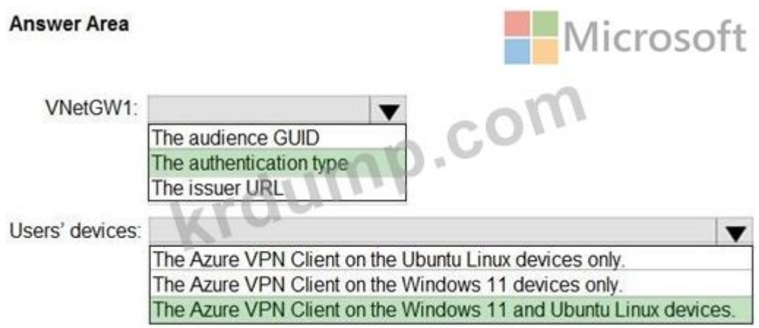
NEW QUESTION: 158
□□ VNet □□□ □□□□ □□□□□ □□ □□ □□□ VNet□ □□□ □ □□□□. □□ □□□ VNet□□ VNet □□□ □□□ □ □□□□□ □□□□ □□□□□ □□ Azure □□□□ □□ □ □□ □□□ □□□□ □□□?
A. □□□ □□□(UDR)
B. □□□ □□ □□□
C. □□ □□□
D. □□□
E. □□□□ □□ □□(NSG)
Answer: (SHOW ANSWER)
Outbound traffic can be blocked with an NSG that is located on your integration subnet. Here, the inbound rules do not apply as VNet Integration can't be used to support the inbound access to your application.
Option A is incorrect. A route table can be placed on the integration subnet to direct/deliver outbound traffic at desired locations.
Option B is incorrect. Azure DNS offers name resolution with the help of Microsoft Azure infrastructure and is not a related Azure Networking feature.
Option C is incorrect. Traffic Manager is a Load balancing solution.
Option D is incorrect. Front Door is also a load balancing solution.
Option E is correct. NSGs help in blocking outbound traffic.
Reference:
https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet?WT.mc_id=modinfra-33046-thmaure

NEW QUESTION: 159
□□□ □□

Windows 11 □□ □□ Ubuntu Linux 22.04 □□□ □□□□ □□ □□□□ □□ □ □□□□. □ □□□□ □□□□ □□□ Azure VPN □□□□□□ □□□□ □□□□.
VNetGW1□□□ □□□ Azure VPN □□□□□□ □□□ Azure □□□ □□□□.
Windows 11 □□□□ Microsoft Entra □□ □□□ □□□□ □□□□ VNetGW1□ □□ P2S(Point-to-Site) VPN □□□ □□□□□. □□□ Ubuntu Linux □□□□ P2S VPN □□□ □□□ □ □□□□.
Ubuntu Linux □□□□ VNetGW1□ P2S VPN □□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□□ □□□□□ □□□ □□□□□ □□□. □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

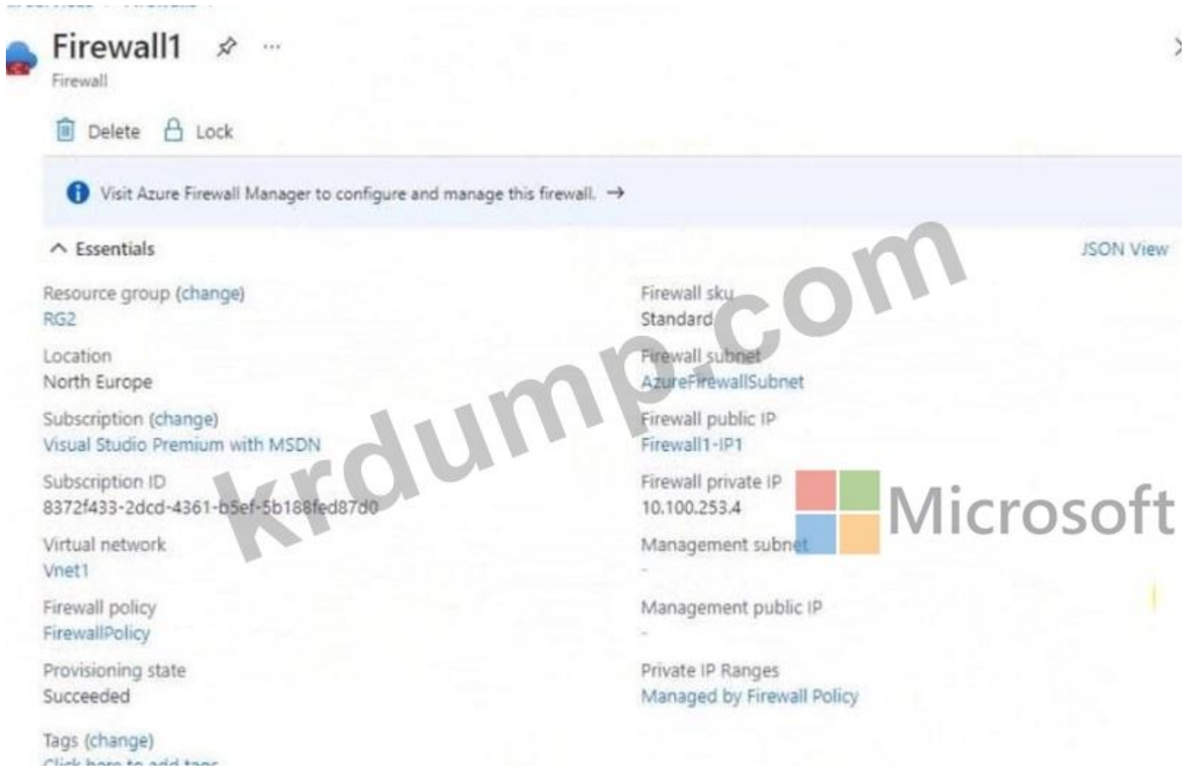


Answer:

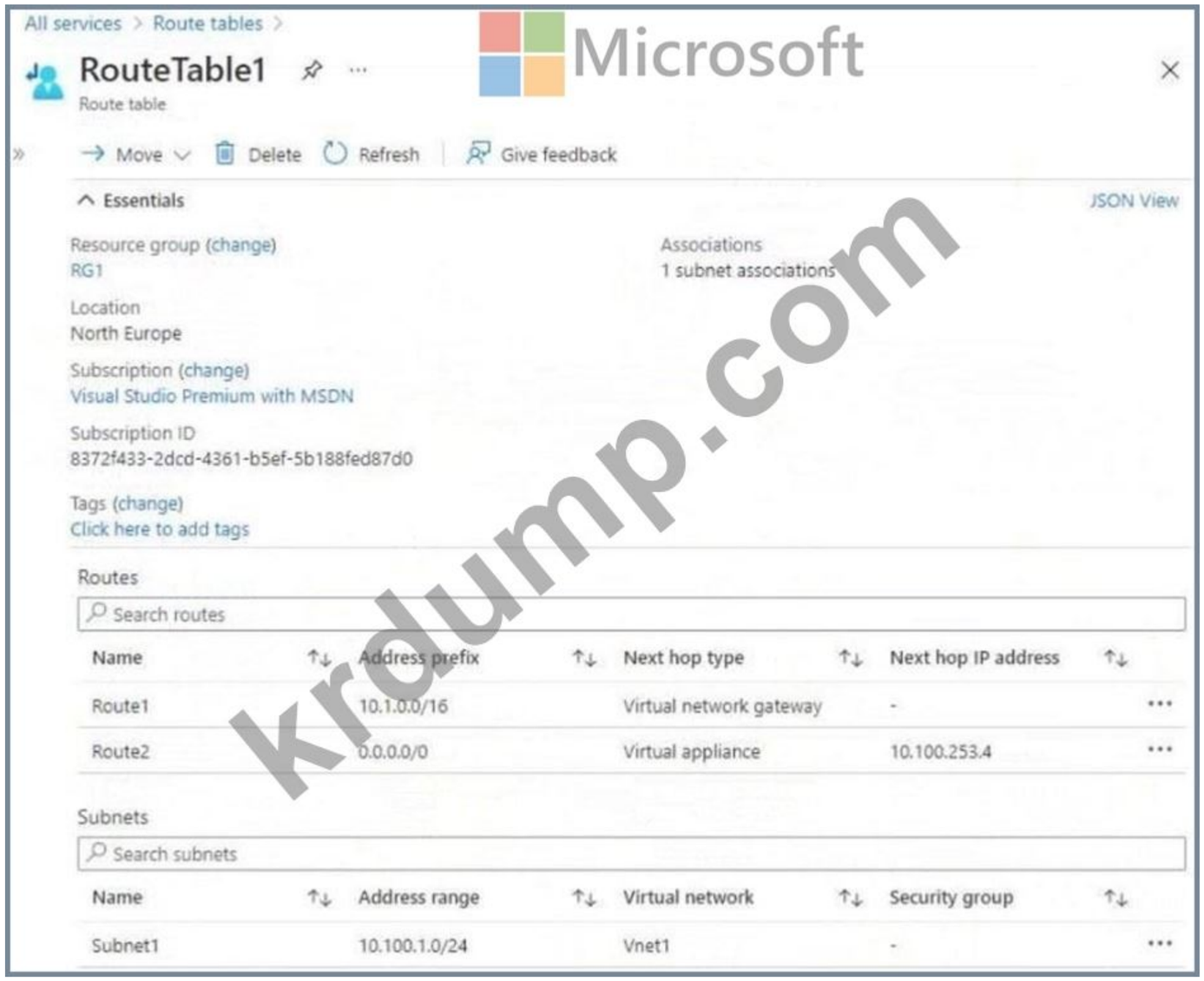


NEW QUESTION: 160
□□□ □□
□□□□ □□□ □□□ □□□□ □□□□□ □□□□□□.

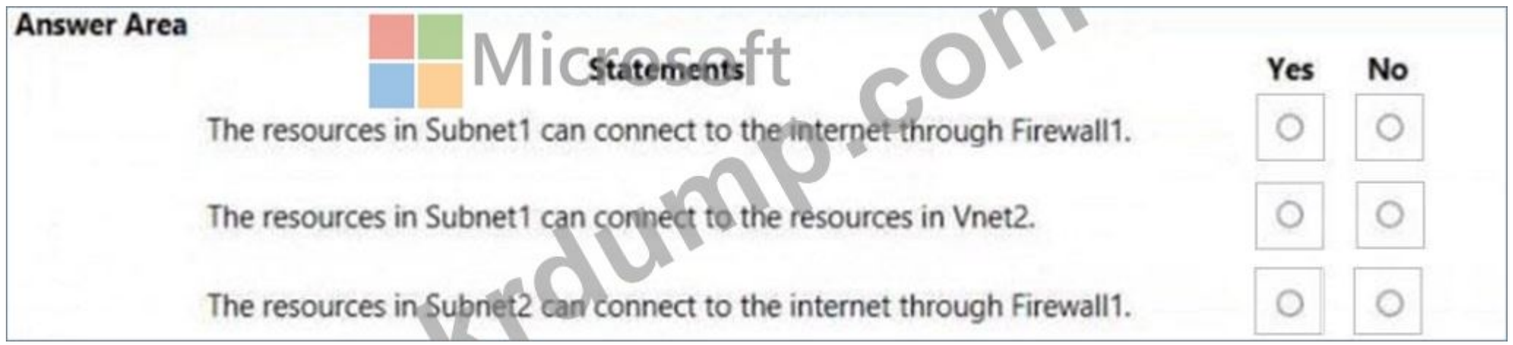
Firewall1 □□□ Azure □□□□ □□ □□□□.



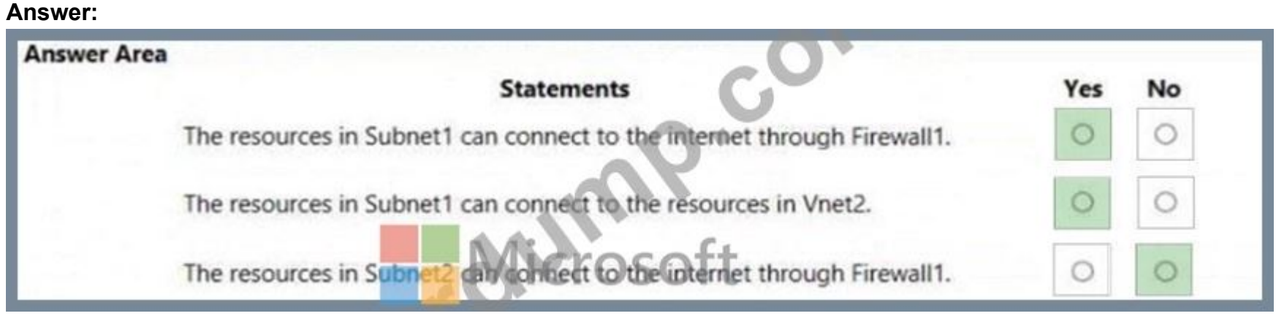
RouteTable1 □□□ □□□ □□□□ □□□□.


All services > Route tables >
RouteTable1
Route table
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Resource group (change)
RG1
Location
North Europe
Subscription (change)
Visual Studio Premium with MSDN
Subscription ID
8372f433-2dcd-4361-b5ef-5b188fed87d0
Tags (change)
Click here to add tags
Associations
1 subnet associations
Routes
Search routes
Name
Address prefix
Next hop type
Next hop IP address
Route1
10.1.0.0/16
Virtual network gateway
-
Route2
0.0.0.0/0
Virtual appliance
10.100.253.4
Subnets
Search subnets
Name
Address range
Virtual network
Security group
Subnet1
10.100.1.0/24
Vnet1
-

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: Yes

Resources in Subnet1 will use the Route2 and its Next hop ID address to the Firewall to reach the Internet.

Box 2: Yes

Yes, with network network peering.

Box 3: No

Resources in Subnet2 can only reach resources in Subnet1, as gateway transit for virtual network peering has not been configured.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

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

NEW QUESTION: 161

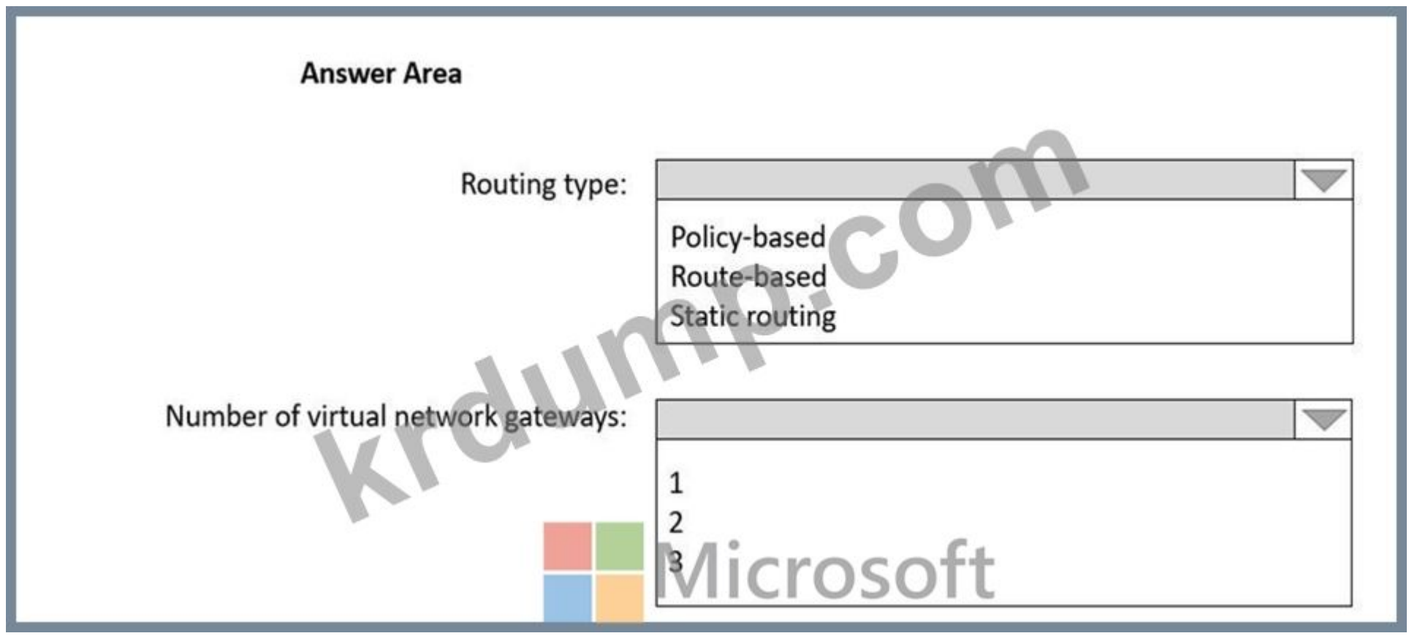
□□□ □□

□□□□□ □□□□□ Azure □□□ □□□□ □□□.

□□ □□□□ ExpressRoute□ □□□□ □□, ExpressRoute □□ □□ □ □□□ □ VPN □□□ □□□□□□ □□□ □□□□ □□□.

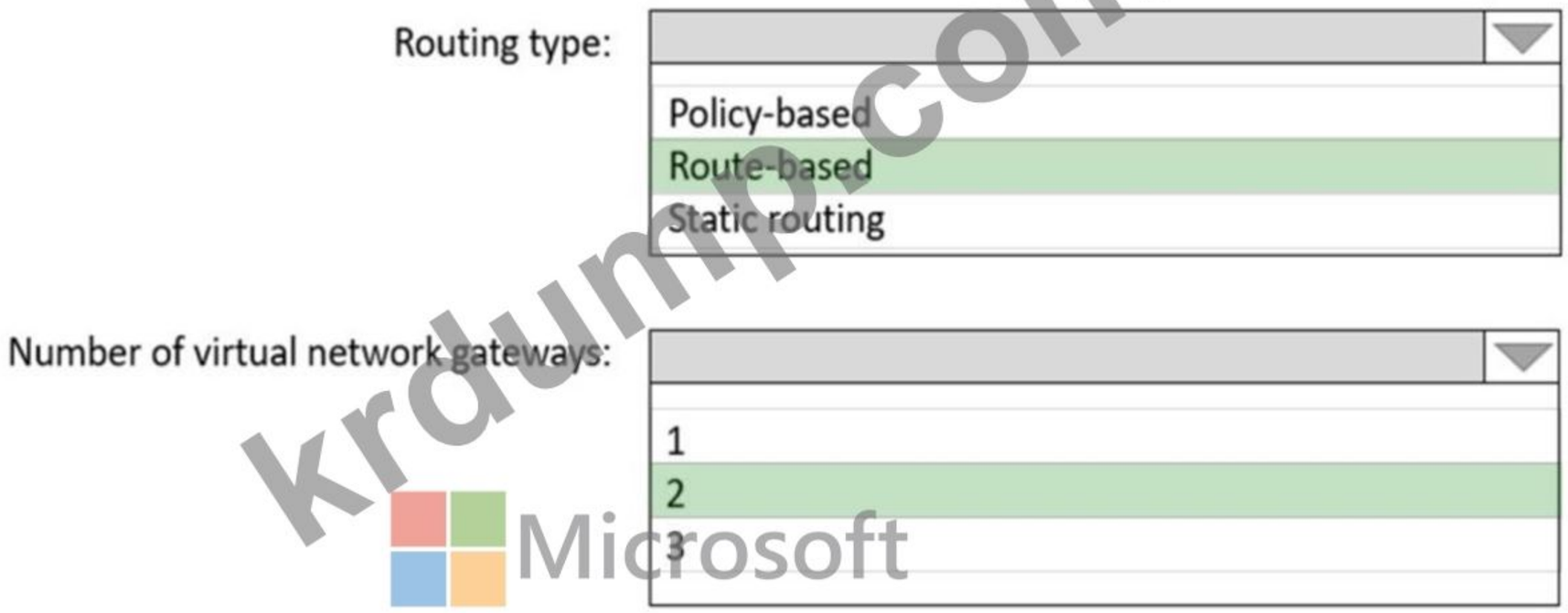
□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.


Answer Area
Routing type:
Policy-based
Route-based
Static routing
Number of virtual network gateways:
1
2
3
krdump.com
Microsoft

Answer:

Answer Area



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: 162
AGW1□□□ Azure □□□□□□ □□□□□□ □□ □ □□□□□□ Rule1□□□ □□□ □□□ □□□□.
1□ http://www.contoso.com□ □□□□ Pool1□□□ □□□ □□ □□□□□. Pool1□ VMSS1□□□ Azure □□ □□ □□ □□□ □□□□ □□□.
VMSS2□□ □ □□ □□ □□ □□ □□□ □□□□□.
AGW1□ □□□□ http://www.adatum.com□ □□ □□ □□□□ VMSS2□ □□□□ □□□. □□□□ http://www.contoso.com□ □□ □□□ □□□□ Pool1□ □□□□□ □□ □□□.
□□ □ □□ □□□ □□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ 1□□ 1□□□□.
A. □□□ □□ □□□□□.
B. HTTP □□□ □□□□□.

C. HTTP □□□ □□□□□.
D. □□□□ □□□□□.
E. □□□ □□□□□.
Answer: A,D,E (LEAVE A REPLY)
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

NEW QUESTION: 163
100□□ □□□□ □□ □□(NSG)□ □□□ Azure □□□ □□□□.
□□ NSG □□□ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□?
A. □□ □□
B. □□ □□
C. Azure □□□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/network-watcher/nsg-flow-logs-overview

NEW QUESTION: 164
□□□ □ □□□□, □□□□□ □□ □□□□ □□□ Azure □□ □□□ □□□□ □□ □□□□ □□□□.
□□ □ Azure Front Door □□ □□□ □□□□ □□□□ □ □□□ □ □□ □□□ □□□□□?
A. DNS □□ □□□ □□ □□□ □□□□, □ □□ Azure □□□ □□□□ □□□□ □□□□ □□□□ □□ □□□□ □□□□ □□□□□.
B. □□□ □□□ 7 □□ □□□ □□□ □□□□ □□□□ □□□□□□ □□ □□□□(ADC)□ □□□□ □□ □□□ □□□□□.
C. □□ TCP □ UDP □□□□□ □□ □□□ □ □□□□ □□□ 4 □□ □□□ □□□(□□□□ □ □□□□□).
D. □□□ 7 □□□ □□□□ □ □□□□□□□ □□□ □□ □□□ □ □□□ □□ □□□□ □□□□ □□□□□□ □□ □□□□(ADN)
Answer: D (LEAVE A REPLY)
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: 165
□□□ Azure □□□□ □□□ □□ □□□□ □□□□ □□□□.
- Vnet1□□□ □□□ □□ □□□□
- subnet1□ AzureFirewallSubnet□□□ □□□ □□□ □ □
- FW1□□□ □□□ □□ Azure □□□
- Subnet1□ □□□ RT1□□□ □□□ □□□ □□□

- RT1□□ 0.0.0.0/0□ FW1□□ □□□□□ □□
Windows Server□ □□□□ □□ 10□□ Subnet1□ □□□ □, □□ □□ □□ □□□ □□ □□□□□ □□ □□ □□□□□□.
□□ □□□ □□□□ □ □□□ □□ □□□.
□□□ □□ □□□?
A. NAT □□□□□□ □□□□□.
B. FW1□□ Azure Key Management Service(KMS)□□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□□.
C. Subnet1□ □□ 1688□ □□ □□□□□ □□□□ □□□□ □□□□ □□ □□(NSG)□ □□□□□.
D. □□□□□ NAT □□□ □□ Azure □□ □□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
In Azure, Windows virtual machines need access to the Azure Key Management Service (KMS) to activate their licenses. By default, KMS activation uses TCP port 1688. Since all outbound traffic in Subnet1 is routed through the Azure Firewall (FW1) due to the 0.0.0.0/0 route, the firewall needs a rule to allow outbound access to KMS.

NEW QUESTION: 166
□□□ □□
□□□□ GW1□□□ □□□ □□□□□ VPN □□□□□□□ □□□□.
VPNGW1□□□ □□□ Azure VPN □□□□□□ □□□ Azure □□□ □□□□.
VPNGW1□ GW1□ □□□□□.
VPNGW1 □ GW1□□ □□□□ IKEv2 □□□ □□□□□ □□□□ □□□.
□□ PowerShell cmdlet□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

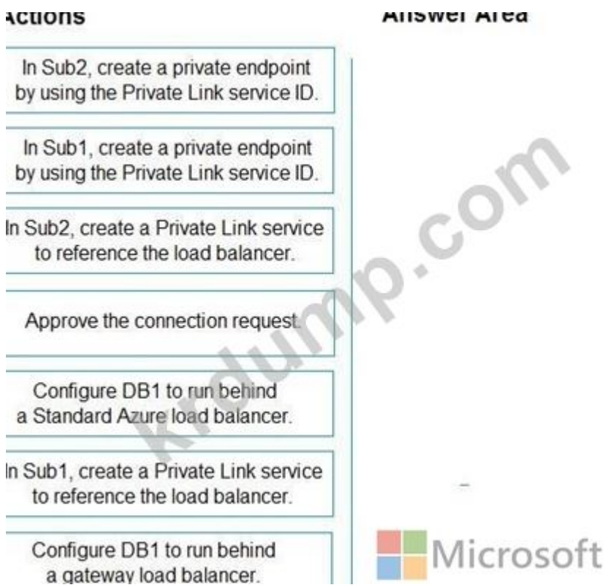
To configure the use of IKEv2 encryption:
- New-AzIpsecPolicy
- New-AzIpsecTrafficSelectorPolicy
- Set-AzFirewallPolicy

To apply the new policy:
- New-AzVirtualNetworkGatewayPolicyGroup
- Set-AzVirtualNetworkGateway
- Set-AzVirtualNetworkGatewayConnection

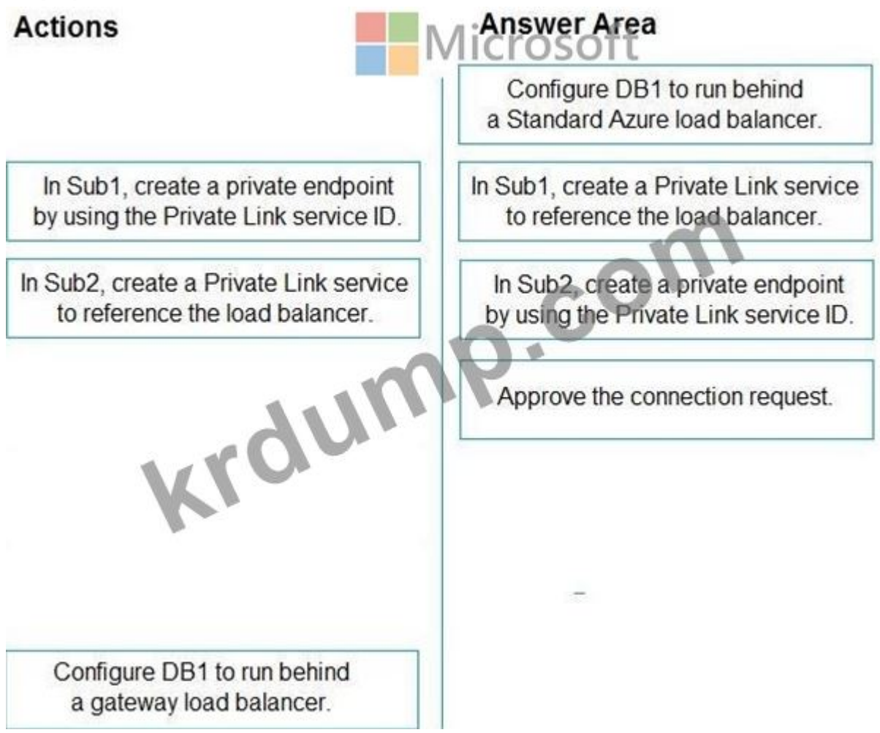
Answer:

NEW QUESTION: 167
FD□□ □□□ Azure Front Door □□□□□ □□□, □ □□□□□□ OG1□□□ □□□ □□ □□□ □□□□.
OG1□ □□ □□ □□□□ □□□□ □□□. □□□□ □□ □□□□ □□ □□□□ □□□ □□ □□□□□ □□□.
□□ HTTP □□□□ □□□□ □□□?
A. □□
B. □□
C. □□
D. □□
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: 168
□□□ □ □□ □□
Sub1□ Sub2□□ □ □□ Azure □□□ □□□□. □ □□□ □□□ Microsoft Enterprise □□□□ □□□□ □□□□. Sub1□□ App1□□□ □□ □□□□□ □□ □□ □□ □□□ □□□□ □□□□. Sub2□□ VNet1□□□ □□ □□□□□ □□□□ □□□□.
Azure Private Link □□□□ □□□□ VNet1□ App1□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

Reference:

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

NEW QUESTION: 169

□□□ □□

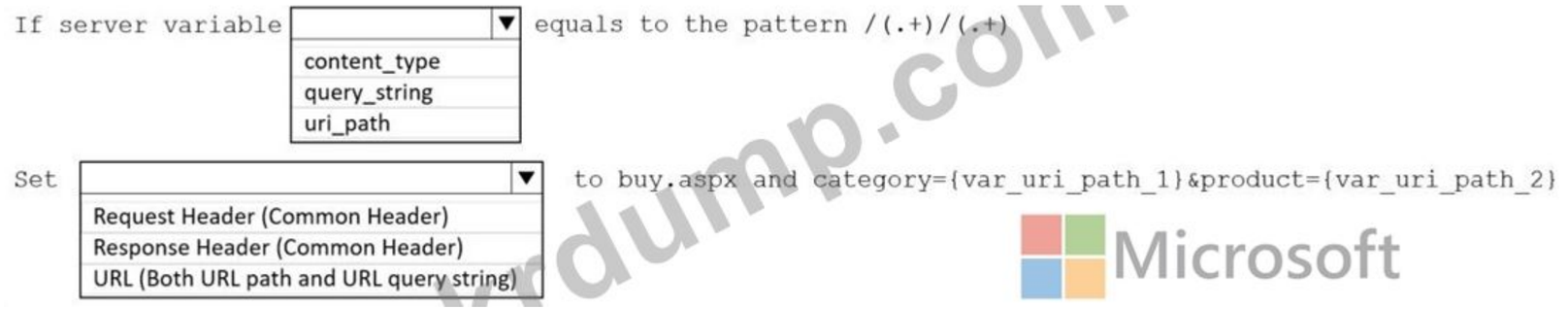
AppGw1□□□ □□□ Azure □□□□□□ □□□□□□ □□□□.

AppGw1□ □□ URL □□□ □□□ □□□□ □□□. □ □□□ https://www.contoso.com/fashion/shirts□□ □□□□ □□□ URL□ □□ URL□ □□□□□ □□□.

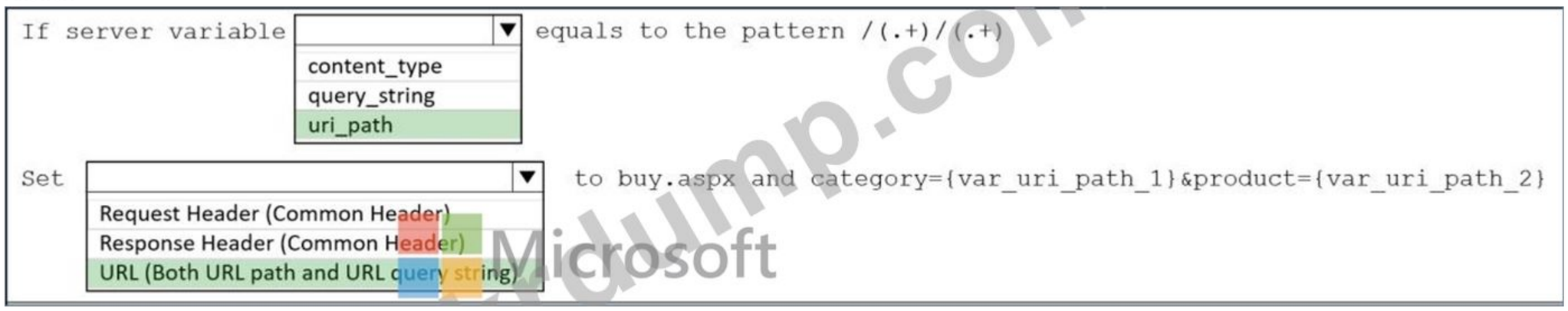
https://www.contoso.com/buy.aspx?category=fashion&product=shirts.

□□□ □□□ □□□□ □□□? □□□□ □□□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-url-portal#configure-url-rewrite

NEW QUESTION: 170

VNet1□□□ Azure □□ □□□□□ □□□, □ □□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Is a gateway subnet	Description
Subnet1	No	Has connected virtual machines
Subnet2	No	Has no connected resources
GatewaySubnet	Yes	None

AppGW1□□□ □□□ Azure □□□□□□ □□□□□□ VNet1□ □□□□ □□□.

AppGW1□ □□□ □□□ □ □□□?

B. □□□2 □□

A. □□□□□□ □□□□ □□

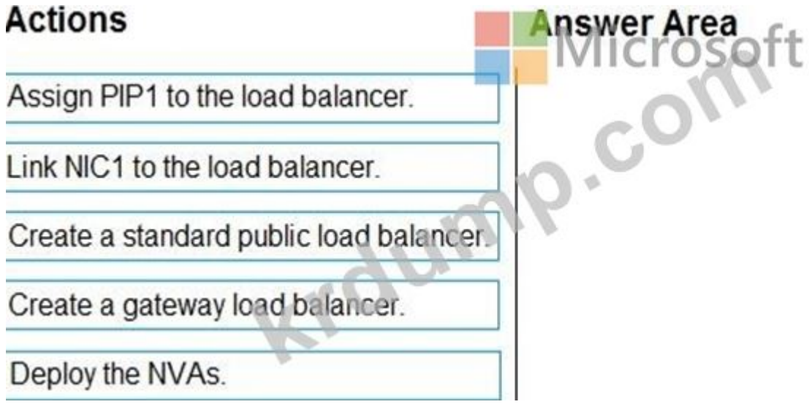
C. □□□1 □□ □□□2□ □□

D. Subnet2 □□ GatewaySubnet□ □□
E. □□□1, □□□2 □ □□□□□□□□
Answer: C (LEAVE A REPLY)
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. You can't mix v1 and v2 Azure Application Gateway SKUs on the same subnet.
https://learn.microsoft.com/en-us/azure/application-gateway/configuration-infrastructure

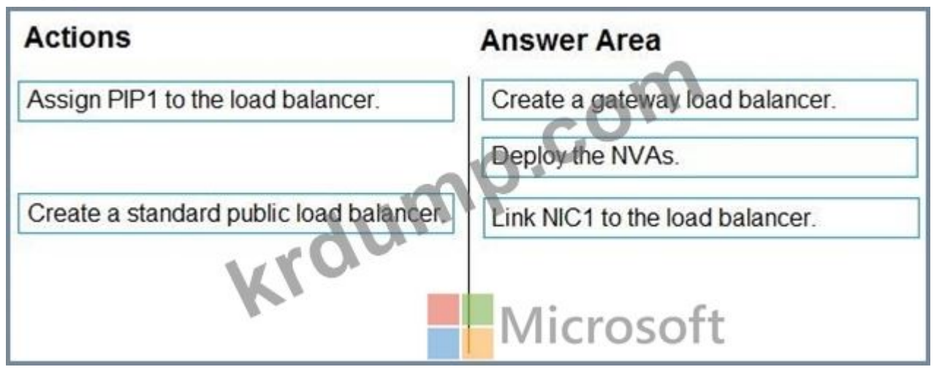
NEW QUESTION: 171
AppGW1□□□ Azure □□□□□□ □□□□□□ □□□, □ □□□□□□ App1□□□ □□□ □□ □□□ □□□□□.
App1□ □□ □□□□ □□ □□□ □□□□ □□□.
AppGW1□□ □□□ □□□□ □□□?
A. HTTP □□
B. □□ □□
C. □□
D. □□□
Answer: B (LEAVE A REPLY)
Application Gateway allows you to add, remove, or update HTTP request and response headers while the request and response packets move between the client and back-end pools.

NEW QUESTION: 172
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□ □ □□□□.
□ □□□□ □□□ □□□ □□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.
Azure □□□ VWAN1□□□ □□□ Azure □□ WAN□ □□□□. VWAN1□□ Hub1□□□ □□□ □□□ □□□□.
Hub1□ □□ □□□ '□□□□ □□'□□□.
Hub1□ □□ □□□ '□□□'□□ □□□□ □□□ □□□□ □□□.
□□ □□: Azure □ □□□□□□ □□□(WAF)□ □□□□□.
□□□ □□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
WAF is for web application, while Azure Firewall is for VNETs which is needed for hub.

NEW QUESTION: 173
□□□ □ □□ □□
VM1□□□ □□ □□□ □□□ Azure □□□ □□□□. VM1□□ NIC1□□□ NIC□ PIP1□□□ □□ IP □□□ □□□□. PIP1□ NIC1□ □□□□ □□□□.
□□□□ □□ □□□□□□(NVA)□ 4□ □□□ □□□□□.
□□□□□ PIP1□□ □□□□ □□ □□□□ NVA□ □□ □□□□□ □□ □□□.
□□ □□□□ NVA □□□ □□ □□□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

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

NEW QUESTION: 174

□□□□□

□□□ □□□ □□□□

□□□ □□ □□ □□□ □□ □□□ □□□□□□.

- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com

- Azure □□: xxxxxxxxxx
Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678
VNET1□ VNET2□ □□ □□ □□□ contosoazure□□ □□□ DNS □□□ □□□□ □□□□□ □□ □□□. □□, VNET1□ VNET2□ □□ □□ □□□ □ □□ □□□□□ □□ □□ □□□ □□□ □□□ □ □□□ □□ □ □□.
□ □□□ □□□□□ Azure □□□ □□□□□□.
Answer:

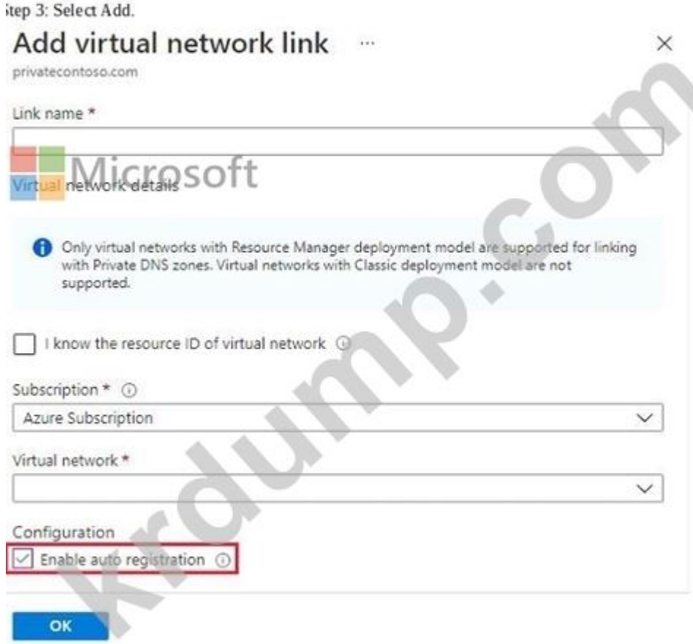
What is the auto registration feature in Azure DNS private zones?
The Azure DNS private zones auto registration feature manages DNS records for virtual machines deployed n a virtual network. When you link a virtual network with a private DNS zone with this setting enabled, a DNS record gets created for each virtual machine deployed in the virtual network.

For each virtual machine, an A record and a PTR record are created. DNS records for newly deployed virtual machines are also automatically created in the linked private DNS zone. When a virtual machine gets deleted, any associated DNS records also get deleted from the private DNS zone.

Step 1: Locate the DNS zone contosoazure

Step 2: On the left pane, select Virtual network links.

Step 3: Select Add.



Step 4: Type myLink for the Link name.

Step 5: For Virtual network, select VNET1.

Step 6: Select the Enable auto registration check box.
To enable auto registration, select the checkbox for "Enable auto registration" when you create the virtual network link.

Step 7: Select OK.

Step 8: Repeat procedure for VNET2.

Reference:
https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration
https://learn.microsoft.com/en-us/azure/dns/private-dns-getstarted-portal#link-the-virtual-network

NEW QUESTION: 175
Azure □□ □□□ □□□ □□□□□□□ □□□□ □□□□□□□ □□□ □□□ □□□□ □□□.
□□ Azure Network Watcher □□□ □□ □□□□ □□□?
A. □□ □□□
B. □□ □□

C. NSG □□ □□
D. IP □□ □□
Answer: C (LEAVE A REPLY)
Traffic analytics examines raw NSG flow logs. It then reduces the log volume by aggregating flows that have a common source IP address, destination IP address, destination port, and protocol.
Reduced logs are enhanced with geography, security, and topology information and then stored in a Log Analytics workspace.\
https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics

NEW QUESTION: 176
Azure □□ □□□□□ □□□□ □□ IP □□ □□□ □□□□ □□□□.
□□□□□ IP □□□ □□□ □□□ □□□ □□□□□?
A. □□ □□ □□□
B. □□ □□
C. □□□ □□□□□
D. □□□ □□□□□ □□
Answer: (SHOW ANSWER)
An internal (or private) load balancer is used where private IPs are needed at the frontend only.
Internal load balancers are used to load balance traffic inside a virtual network.
https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

NEW QUESTION: 177
□□□□ □□□□□ DNS □□ □□□ □□□□ □□□□ □□, TLS(□□ □□ □□) □□□□ □□("SSL □□□□"), HTTPS/HTTP □□□ □□ □□ □□□□□□ □□ □□□ □□□□ □□□□. □□ □ □□ □□ □□□ □□ □□ □□□□□□□□?
A. □□□□□□ □□□□□
B. □□ □□□
C. □□□
D. PowerShell
Answer: B (LEAVE A REPLY)
Azure Traffic Manager is a DNS-based traffic load balancing solution that allows optimal distribution of the traffic to services across global Azure regions, offering high responsiveness and availability.
Option A is incorrect. An application gateway is recommended for scenarios like if you need to load balance between your servers in a region at the application layer.
Option B is correct. For scenarios like the given one, a traffic manager suits the best.
Option C is incorrect. Front door suits scenarios like if you want to optimize the global routing of web traffic and improve top-tier end-users performance and reliability via quick global failover.
Option D is incorrect. PowerShell is not a load balancing option.
Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

NEW QUESTION: 178
App1□□□ □□ □ □□ □□□ Azure □□□ □□□□. App1□ □□ Azure □□□ □□ □□□□□□.
□□□ □□□ □□□ □□□□□ □□□□ □□□□ □□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.
- URL□ □□□□ □□□ □□□ □□ □□□□ □□□□□ □□□ □□□□□.
□□□ □□□□□.
- □□ □□□ □□ □□□ □□□□□.

- □□□□ □□ □□□ □□□□□□.
□□ □□□ □□□ □□□□ □□□?
A. Azure □□ □□□
B. Azure Traffic Manager
C. Azure □□□ □□ □□□□(CDN)
D. □□□ □□□
Answer: D (LEAVE A REPLY)
* 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

NEW QUESTION: 179
□□□ □□
□□□ Azure □□□□ □□ □□ □□□ □□□ □□□ □□□□ □□□□.

Name	Location
RG1	East US
RG2	East US
RG3	UK West

□□ □□ □□ □□ □□ □□□□□ □□□□.

Name	Location	IP address space	Resource group
Vnet1	East US	10.1.0.0/16	RG1
Vnet2	West US	10.2.0.0/16	RG2
Vnet3	UK West	10.1.0.0/16	RG3

□□ □□ □□□□ □□ □□□□.

Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.1.1.0/24

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Statements	Yes	No
Vnet1 can be moved to RG3.	○	○
Three hundred virtual machines can be deployed to the East US Azure region.	○	○
A new virtual network named Vnet2 can be created in RG2 in the East US Azure region.	○	○

Answer:

NEW QUESTION: 180

Site1□□□ □□□□□ □□□ □□□ □□, □ □□□ □□□□ FW1□□□ □□□□ □□□□. FW1□ □□□□ □□□□□.

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

□□□ □ □□□ □□□□ Site1□ Hub1□ □□□ □□□□□.

FW1□ □□ □□□ □ □□□ □□□□ □□□.

VWAN1□□ □□□ □□□□ □□□?

A. VPN □□□

B. □□ □□□□ □□

C. □□□□ □□ □□□□□□(NVA)

D. □□□ VPN □□

Answer: (SHOW ANSWER)

https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal#site

NEW QUESTION: 181

□ □ App1□ Azure Front Door □□□□ FD1□ □□ Azure □ □□□□□□ □□□(WAF)□ □□□ Azure □□□ □□□□. FD1□ App1□ □□□□ □□□□□.

□□ IP □□□ App1□□ □□□□□□ □□ □□□ □□□□ □□□□ □□, □□ □□□□ □□□□ □□□□ □□□□ □□□. □□, □□ □□□ □□□□□ □□□□□□ □□□.

□□□□ □□□ □□□□ □□□?

A. IP □□ □□

B. WAF □□ □□

C. □ □□ □□ □□

D. □□ □□ □□

Answer: (SHOW ANSWER)

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:

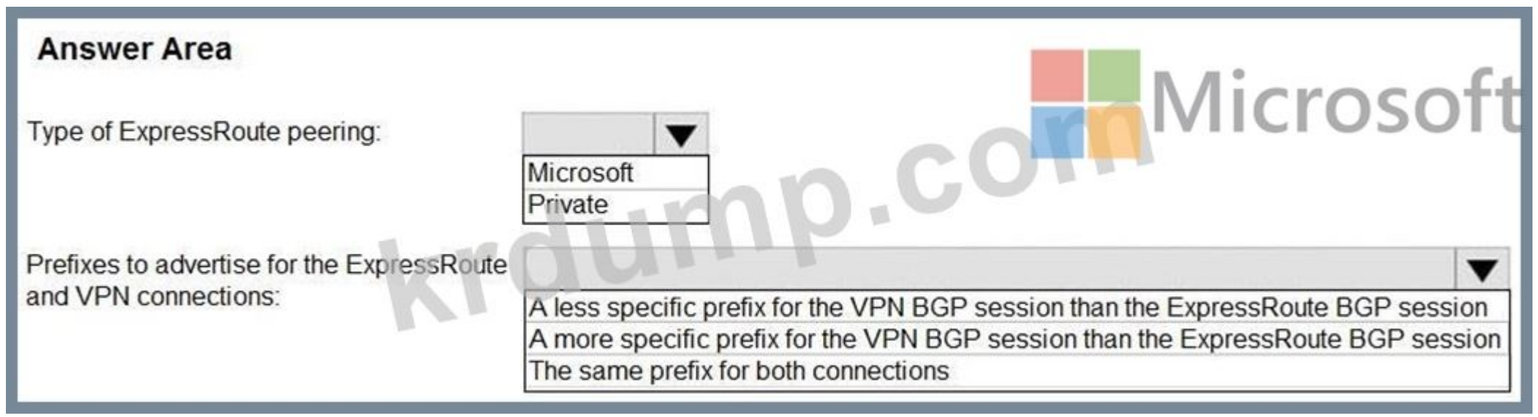
3.1 To apply the limit to all incoming traffic, use a condition that is always true, such as checking if the RemoteAddr is Any or using a wildcard (*) for the IP address.
3.2 Alternatively, target specific high-risk paths (e.g., /api/login) by matching the RequestUri.
Reference:
https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit

NEW QUESTION: 182
□ □□□□□ NSG1□□□ □□□□ □□ □□(NSG)□ □□□□ □□□□.
Vnet1□ □ □□□□ □□□□ □□□□ □□□□□ □□ □□□□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□□ NSG1□ □□□□□.
NSG1□□ 131.107.1.15 IP □□□ □□ □□ □□□□ □□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□. □ □□□ □□ □□ □□□ □□□□ □□□.
- □□□□□ □□ □□□ 131.1071.15□□ □□□ □□□□□ □□□□.
- □ □□□□ □□□ □ NSG1□ □□ □□ □□□ □□□□□□.
□□ □□ □□□□ □□□□ □□□ □□□□ □□□?
A. □□□□□□ □□ □□
B. □□□ □□
C. □□ □□□□
D. IP □□
Answer: A (LEAVE A REPLY)
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

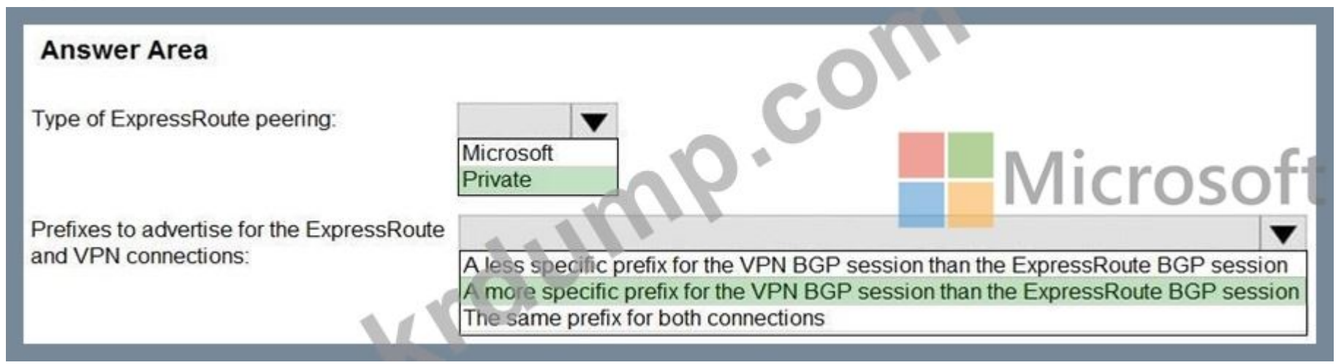
NEW QUESTION: 183
AppGW1□□□ Azure □□□□□□ □□□□□□ □□□, □ □□□□□□ App1□□□ □ □□□□ □□□ □□ □□□□□.
App1□ □□ □□□ □□ □□ □□□ □□□□ □□□.
AppGW1□□ □□□ □□□□ □□□?
A. URL □□□ □□
B. □□□
C. □□ □□ □□
D. HTTP □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 184
□□□ □□
VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□.
□□□□□ □□□□□ VNet1 □□ □□□□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□ □□ □□□□ □□□□ ExpressRoute□ □□ □□□□□ □□□.
□□.

- □□ □□ □□□□ □□□□ □□□ □ VPN(S2S)□ □□□□ □□□□□ □□□.
□□□□ □□□ □□□□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



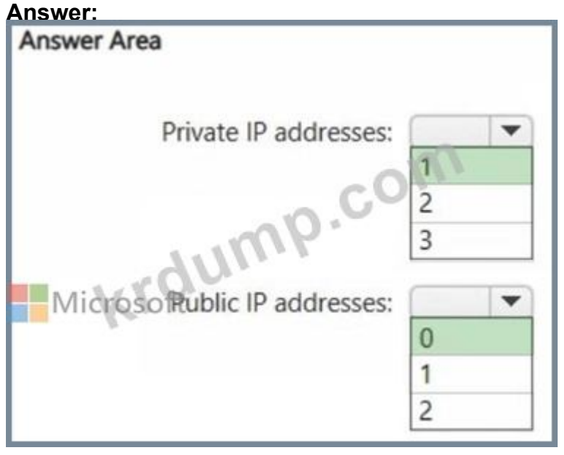
NEW QUESTION: 185
□□ □□□ 50□□ TCP □□□ UDP □□ □□□□ □□□□ □□□ □□□□ App1□□□ □□□□□□□ □□□□.
10□□ Azure □□ □□□ App1□ □□□□□.
□□ □□ □□□□ App1□ □□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□ □□□□□ □□□.
□□□□ □□□ □□□□ □□□?

A. Floating IP□ □□□□ Azure Standard Load Balancer
B. □□ □□□□ □□ Azure Application Gateway V2
C. □□ □□□ □□□□ □□□□ Azure Application Gateway v2
D. □□□□(HA) □□□ □□□□ Azure □□ □□ □□ □□

Answer: D (LEAVE A REPLY)
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: 186
□□□ □□
VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□.
VNet1□ AppGw1□□□ □□□ Azure Application Gateway v2 □□□□□ □□□□ □□□.
AppGw1□□ □□ □□□ 1□□ □□□□□ □□□ 2□□ □□□□□. □□□□ VNet1□□□ □□ □□□□□.
AppGw1□ □□□ □□ IP □□ □□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:



NEW QUESTION: 187
□□□□□

□□□ □□□ □□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
- □□□ □□□ □□□□□ '□□□' □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
- □□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
- Azure □□□ □□: User-12345678@cloudslice.onmicrosoft.com
- Azure □□: xxxxxxxxxx
Azure □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
- □ □□□□: 12345678
□□□ □□□ □□□□□□ □□ □□ □□□ □□□□□ □□□□□ □ □□ □□□ □□□□ □□□□. □□□ □□□□ □□□ ny.contoso.com□□□ □□□ □□□ □□□□ □□□ □ □□□□.
□□□□□□ □□□ □□□ ca.contoso.com□□□ □□□ □□□ □□□□ □□□ □ □□□□.
□□□□ □□ □□□ □□ □□ □□□ □□□□□ Azure □□□□ □□□□ □□□.
□□□□ □□□ □□□□□ □□□.
□ □□□ □□□□□ Azure □□□ □□□□□□.

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.

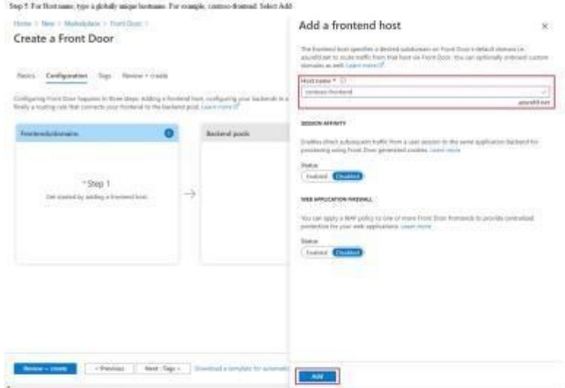
Step 2: On the Compare offerings page, select Explore other offerings. Then select Azure Front Door (classic). Then select Continue.

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.

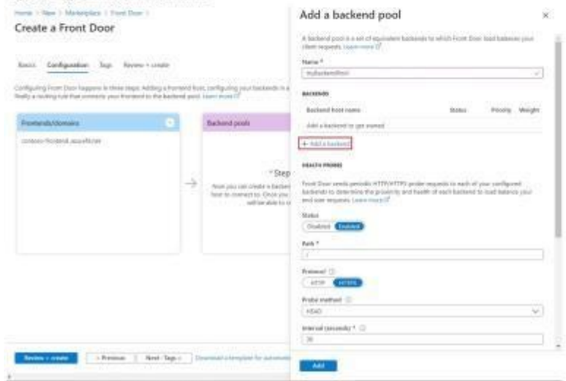
Step 5: For Host name, type a globally unique hostname. For example, contoso-frontend. Select Add.



Next, set up a backend pool.

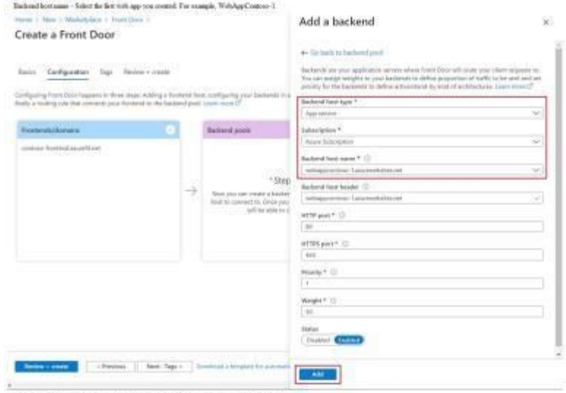
Step 1: Still in Create a Front Door, in Backend pools, select + to open the Add a backend pool page.

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



Step 1: 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.



Step 4: Select Add a backend again. Provide or select the following information and select Add.

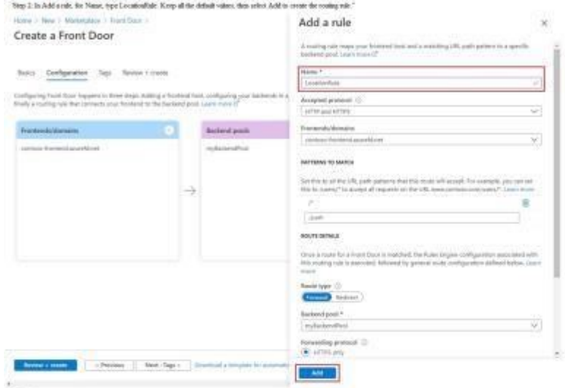
Step 5: Select Add on the Add a backend pool page to finish the configuration of the backend pool.

Phase 3: Create a routing rule

Lastly, create a routing rule. A routing rule links your frontend host to the backend pool. The rule routes a request for contoso-frontend.azurefd.net to myBackendPool.

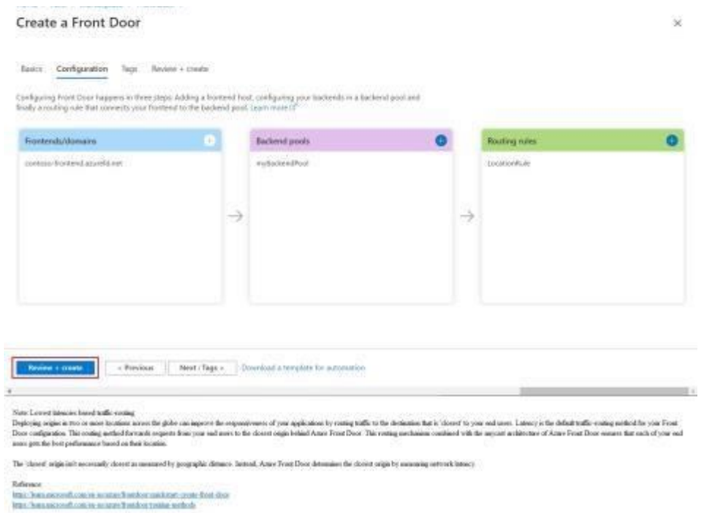
Step 1: Still in Create a Front Door, in Routing rules, select + to set up a routing rule.

Step 2: In Add a rule, for Name, type LocationRule. Keep all the default values, then select Add to create the routing rule.*



Warning
It's essential that you associate each of the frontend hosts in your Azure Front Door with a routing rule that has a default path /*. This means that you need to have at least one routing rule for each of your frontend hosts at the default path /* among all of your routing rules. Otherwise, your end-user traffic may not be routed properly.

Step 3: Select Review + create and verify the details. Then, select Create to start the deployment.

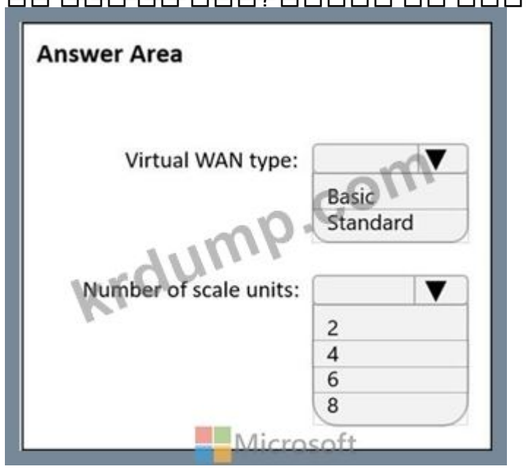


NEW QUESTION: 188
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□ □□ □ □□, □□ □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □□ □□□ □□ □□□ □□□□ □□□□.
Vnet1□ Vnet2□□ □ □□ Azure □□ □□□□□ □□□□.
P2S(Point-to-Site) IKEv2 VPN□ □□□□ Vnet1□ □□□□ Client1□□□ Windows 10 □□□ □□□□.
Vnet1□ Vnet2 □□□ □□ □□□□ □□□□ □□□□□. Vnet1□ □□□□□ □□□ □□□□□.
Vnet2□ □□ □□□□□□ □□□ □ □□□□.
Client1□ Vnet2□ □□□ □ □□□ □□ □□ □□□□□.
Client1□ Vnet2□ □□□ □ □□□ □□□□ □□□.
□□ □□: Vnet1□ □□□□□□ □□□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)
About Point-to-Site VPN routing
If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

NEW QUESTION: 189
NSG1□□□ □□□□ □□ □□□ □□□□.
NSG1□ □□ □□□□ □□ □□(NS) □□ □□□ □□□□□ □□□. □□□□ □□ □□□ □□□□ □□□.
□□□ □□ □□□□ □□□?
A. □□ □□ v2 Azure Storage □□
B. Azure Log Analytics □□ □□

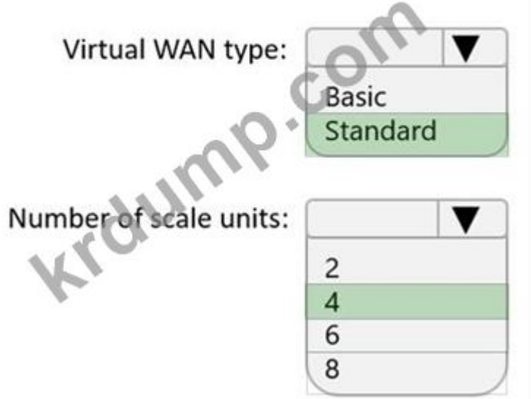
C. □□ □□ v1 Azure Storage □□
D. □□□□ □□ □□ Azure □□□□ □□
Answer: A (LEAVE A REPLY)
Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG. Flow data is sent to Azure Storage accounts from where you can access 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: 190
□□□ □□
Azure Virtual WAN□ □□□ □□□□□.
□□ □□ □□□ □□□□ □□ WAN □□□ □□□□ □□□.
- □□□ □ VPN □□□ □□□□ □□ WAN □□□ □□□ □ □□ □□ 10□ □□□□ □□□□□.
- ExpressRoute □□□□ 8Gbps□□ □□□□□.
- □□□ □□□□□□
□□: □□ □□□ 1□□□□
□□ □□□ □□ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:

Answer Area

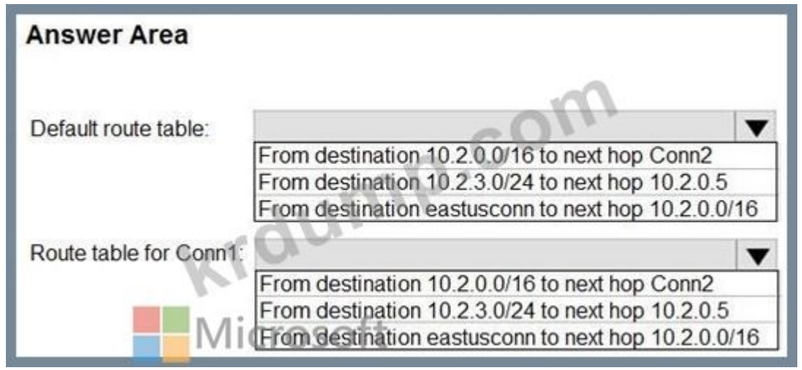


Explanation:
Box1: Standard
Basic virtual WAN supports Site-to-site VPN only
Standard virtual WAN supports
ExpressRoute
User VPN (P2S)
VPN (site-to-site)
Inter-hub and VNet-to-VNet transiting through the virtual hub
Azure Firewall
NVA in a virtual WAN
Box 2: 4
8 Gig Express Route. 2 GB per ER scale unit. 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: 191
□□□ □□
Hub1□□□ □□□ □□□□ VWAN1□□□ Azure □□ WAN□ □□□ □□□□□. VWAN1□□ □□ □□ □□□ □□ □□□□□ □□□□□.

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

VNet1□ □□□ □□□□ VNet3□ □□□ □□□□ □□□ □ □□□ □□ □□□.
VWAN1□ □□□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

NEW QUESTION: 192
□□□ □□
□□ □□ Azure □□□ st1□□□ □□□□ □□□ □□□ Azure □□□ □□□□.
□□ □□ □□ □□ □□ □□□□□ □□□□.

Name	Location	IP address space
Vnet1	UK West	10.1.0.0/16
Vnet2	East US	10.2.0.0/16
Vnet3	West US	10.3.0.0/16

□□ □□ □□□□ □□ □□□□.

Name	Virtual network	IP address range	Subnet resources
Subnet1-1	Vnet1	10.1.1.0/24	Five virtual machines that each has one private IP address
Subnet2-1	Vnet2	10.2.1.0/25	Five virtual machines that each has one private IP address
Subnet3-1	Vnet3	10.3.1.0/26	Five virtual machines that each has one private IP address

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
You can deploy Azure Bastion to Subnet1-1.	○	○
You can deploy 100 additional virtual machines to Subnet2-1.	○	○
You can change the IP address range of Subnet3-1 to 10.3.1.0/16.	○	○

Answer:

Answer Area

Statements	Yes	No
You can deploy Azure Bastion to Subnet1-1.	○	◯
You can deploy 100 additional virtual machines to Subnet2-1.	◯	○
You can change the IP address range of Subnet3-1 to 10.3.1.0/16.	○	◯

Explanation:

Box 1: No

Azure Bastion requires a dedicated subnet: AzureBastionSubnet.
You must create this subnet in the same virtual network that you want to deploy Azure Bastion to.
The subnet must have the following configuration:
Subnet name must be AzureBastionSubnet.
Subnet size must be /26 or larger.
https://learn.microsoft.com/en-us/azure/bastion/configuration-settings#subnet Box 2: Yes With /25 we have more than 100 IP's left to use.
Should not be a problem to deploy 100 additional VM's with a single IP.
Box 3: No
You can not change the IP address range of subnet3-1 range to 10.3.1.0/16.
Azure will give this error '10.3.1.0/16 is not a valid CIDR block' because its higher than the Vnet's IP address space of 10.3.0.0/16

NEW QUESTION: 193
□□□ □□
Azure □□□ □□□□. □□ □□□□ □□ □□ □□□ □□□ □ □□□□ □□□□□ □□ □□□ □□□□ □□□□.

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

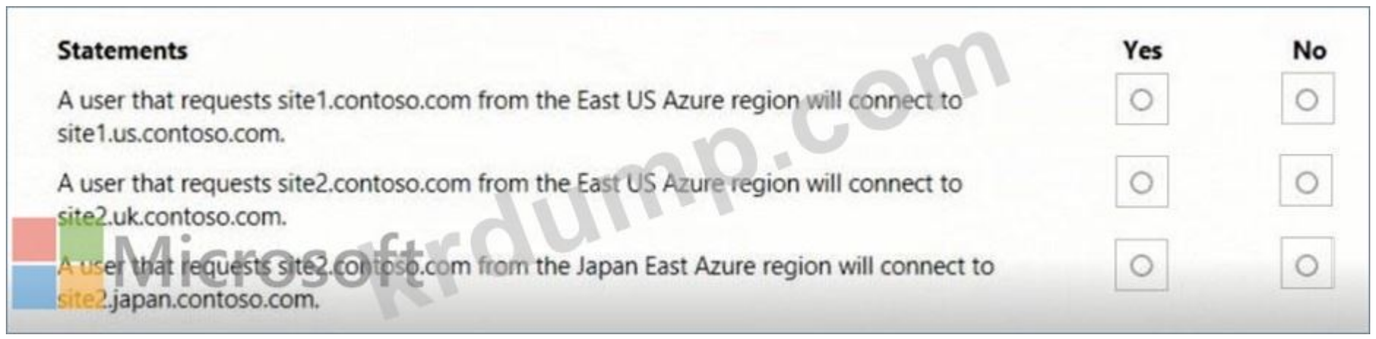
□□ □□ Azure Traffic Manager □□□□ □□ □□□□.

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

□□ □□ □□□ □□ □□ □□□□□□ □□□□.

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

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:

Box 1: No

VM1, which is hosting site1.contoso.com, is located in East US. The VM1 endpoint status is degraded. Endpoint monitoring health checks are failing. The endpoint isn't included in DNS responses and doesn't receive traffic.

When an endpoint has a Degraded status, it's no longer returned in response to DNS queries.

Instead, an alternative endpoint is chosen and returned. The traffic- routing method configured in the profile determines how the alternative endpoint is chosen.

Priority. Endpoints form a prioritized list. The first available endpoint on the list is always returned.

If an endpoint status is Degraded, then the next available endpoint is returned.

The user will connect to site2.us.contoso.com instead.

Box 2: No

VM3, which is hosting site2.contoso.com, is located in in East US. The VM3 endpoint status is CheckingEndpoint. The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

User will connect to site2.contoso.com, not to site2.uk.contoso.com

Box 3: No

VM3, which is hosting site2.contoso.com, is located in in East US. The VM1 endpoint status is CheckingEndpoint, which is OK (see above).

User will connect to site2.contoso.com, not to site2.japan.contoso.com

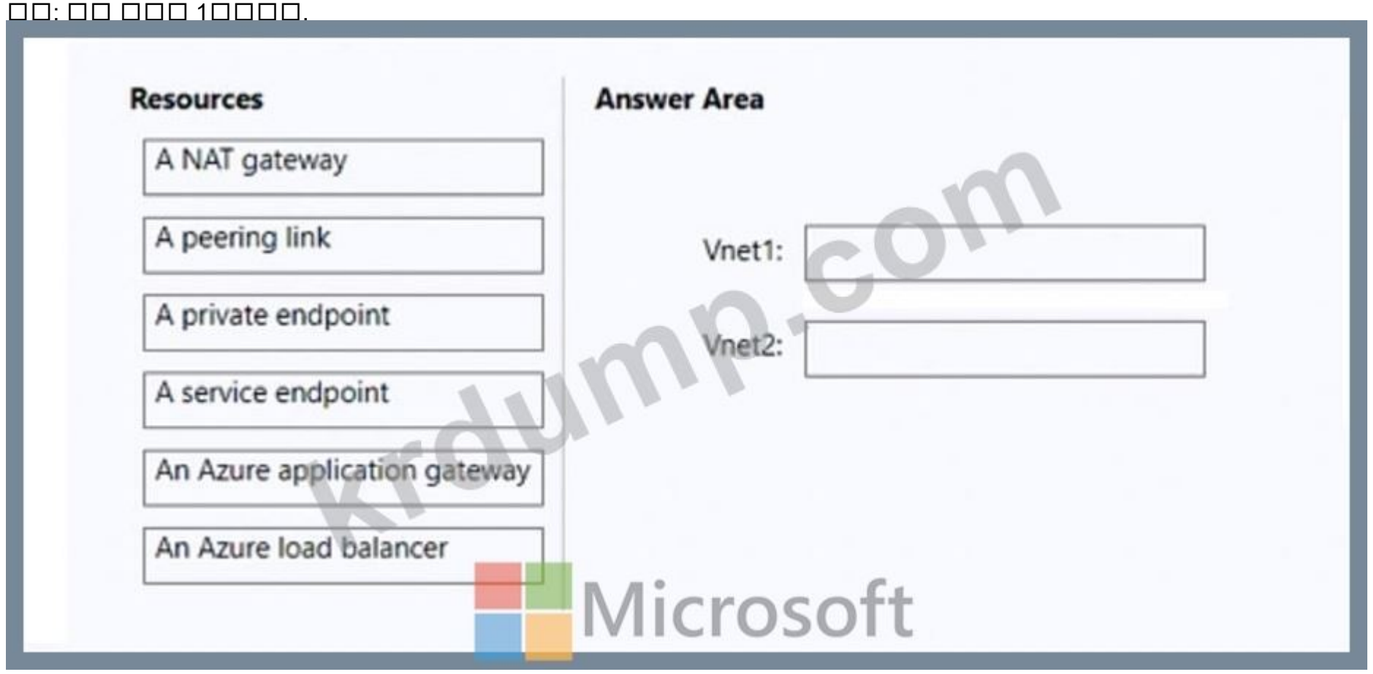
Reference:

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring

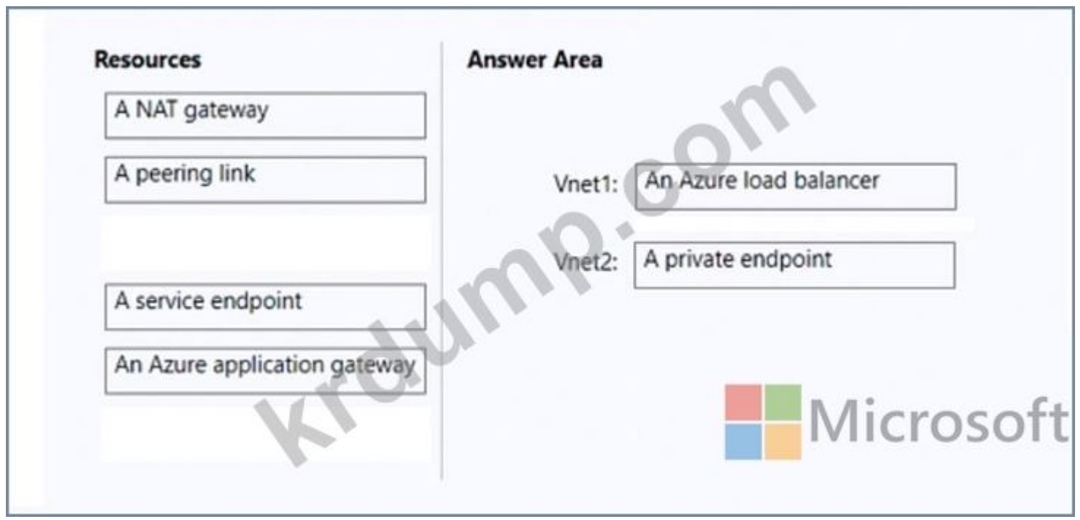
NEW QUESTION: 194

RG1□□□ □□□ □□□ VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□.
RG1□ Azure □□□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□ □□□?
A. AzureFirewallHub□□ □□□ □□ □□ □□□ □□□□□.
B. AzureFirewallNetwork□□ □□□ □ □□ □□□□□ □□□□□.
C. AzurFirewellRescurceGroup□□□ □□□ □ □□□ □□□ □□□□□.
D. VNet1□□ AzureFirewallSubnet□□□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
The first step is to create the AzureFirewallSubnet in VNet1 to meet the prerequisites for deploying Azure Firewall.

NEW QUESTION: 195
□□□ □ □□ □□
Azure □□□□ Vnet1□□□ □□ □□□□□ SQL1□□□ Azure SQL □□□□□□□ □□□□. SQL1□ Vnet1□ □□□□ □□□□□□ □□□ □□□□.
□□□□ Fabrikam, Inc.□□ □□□ □□□ □□□□. Fabrikam□ Vnet2□□ □□ □□□□□ VM1□□□ □□ □□□ □□□ Azure □□□ □□□□ □□□□. VM1□ Vnet2□ □□□□ □□□□.
Azure Private Link □□□□ □□□□ VM1□ SQL1□ □□□□ □ □□□ □□ □□□.
□ □□ □□□□□ □□□ □□□□ □□□? □□□ □□□□ □□□ □□□□ □□ □□ □□□□□ □□□□□□. □ □□□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□.
□□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □ □□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

To establish the private link service you need a load balancer in VNet 1 and for sure the private link service resource. In the partner company tenant you need an private endpoint that connects to this private link service. To answer the question correctly we might answer to create standard load balancer and private link service in vnet1 an pe in vnet2.

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

NEW QUESTION: 196

□□ □□ 2 - □□□ □□□□

□□

□□□ □□□□□ □□□□□□□□ □□□ □□ □□□□ □□□ □ □□□ □□□□□.

Contoso□ □□ Azure □□□ □□□□□ Azure□□ □ □□ □□ □□□□□ □□□□ □□□□.

□□ □□:

Azure □□□□ □□□

Contoso□ contoso.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. □□ Azure □□□□ □□ □□ □□□ □□ □□□□□ □□□□ □□□□.

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□□ GW1□□□ □□□ □□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□ □□

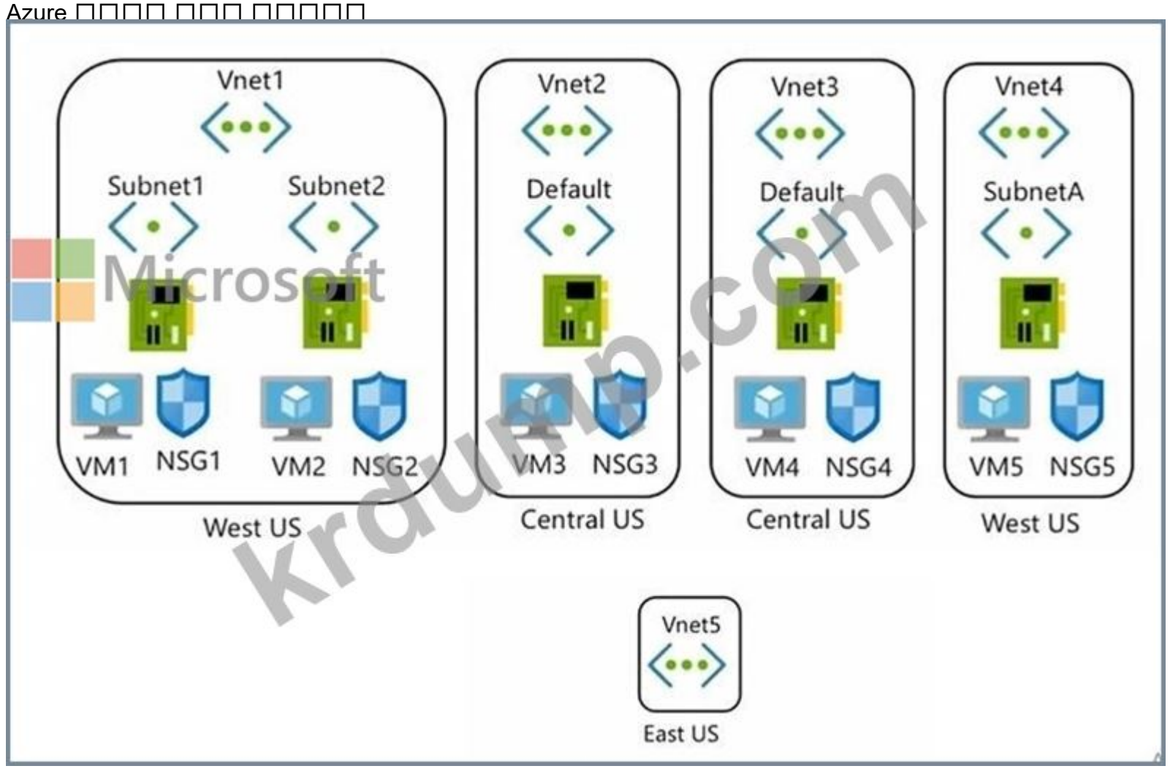
Azure □□□□ □□ □□ □□□ □□□ Windows Server 2019□ □□□□ □□ □□□ □□□□ □□□□.

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

NSG(□□□□ □□ □□)□ □□ □□□ □□□□ □□□□□□ □□□□ □□□□. □ NSG□□ □□□□□ RDP □□□ □□□□ □□□ □□ □□ □□□ □□□ □□□□. □ □□ □□□ □□□□ ICMP □□□□ □□□□ □.

ASG1□□□ □□□□□□ □□ □□□ VM1□ □□□□ □□□□□□ □□□□ □□□□.

Azure □□□□ □□□ □□□□□



Azure □□□□ DNS □□

Azure □□□□ □□ □□ □□□ Azure □□□□ DNS □□□ □□□□ □□□□.

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

Zone1.contoso.com□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□.

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

□□ Azure □□□

Azure □□□□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□ □□□□.

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

□□ □□:

□□ □□□□ □□ □□

Contoso□ □□□ □□ □□ □□□□ □□ □□□ □□□□ □□□.

- □□ □□ □□□ Vnet6□□□ □□□ □□ □□□□□ □□□□, □□ □□□□□ □□ □□□□ □□□ □□□□□□□.

Vnet6□ □□□□ □ □□ □□□□ □□

Vnet6□ □□□ □ □□ □□ □□

Vnet6□ □□ VPN □□ □□□ □□□□□.

Vnet6□ □□□□ KeyVault1, DB1 □ Vnet1□ □□□□ □ □□□ □□□□□.

□□□□□□□ □□ □□□□

- Vnet4□ Vnet5□ □□ □□□□ □□ □□□ □ □□□ □□□.

□□□□□□□ □□ □□□□□ □□.

- VM-Analyze□□ □□□ □□ □□□ Subnet1□ □□□□□. VM-Analyze□ Subnet2□□ □□□ □□□□ □□□□ □□□□ □□□.

□□□.

□□□□ □□ □□ □□

Contoso□ □□□ □□ □□□□ □□ □□ □□□ □□□ □□□□.

- P2S(Point-to-Site) VPN □□□□ □□ Azure Active Directory(Azure AD) □□□ □□□□□.
- NSG3 □ NSG4□ □□ NSG □□ □□□ □□□□□□.
- Vnet1/Subnet1□ □□□ NSG10□□□ □□□ NSG□ □□□□□.

□□□ □□ □□□ □□ □□ □□ □□□ □□□□□.

□□□.

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

- Vnet1/Subnet2□ □□□ NSG11□□□ □□□ NSG□ □□□□□.

□□□ □□ □□ □□□ □□□ □□ □□□□□ □□ □□□ □□□□□.

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

P2S VPN □□□□ □□ □□□□ □□ □□ □□□ □□□□□ GW1□ □□□□ □□□.

GW1□ □□ □ □□ □□□□ □□ □□ □□□ □□□□ □□□?

A. IKEv2 □ OpenVPN(SSL)

B. IKEv2

C. IKEv2 □ SSTP(SSL)

D. OpenVPN (SSL)

E. SSTP (SSL)

Answer: (SHOW ANSWER)

Azure AD authentication is supported for OpenVPN protocol connections only and requires the Azure VPN Client.

And also SSTP and IKEv2 don't support all client devices:

SSTP limited to Windows
IKEv2 limited to Mac devices

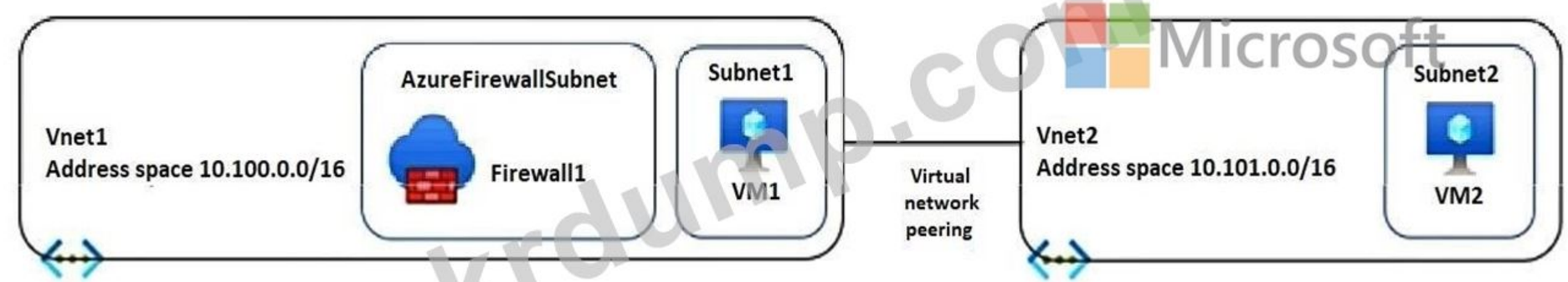
NEW QUESTION: 197

□□□ □□

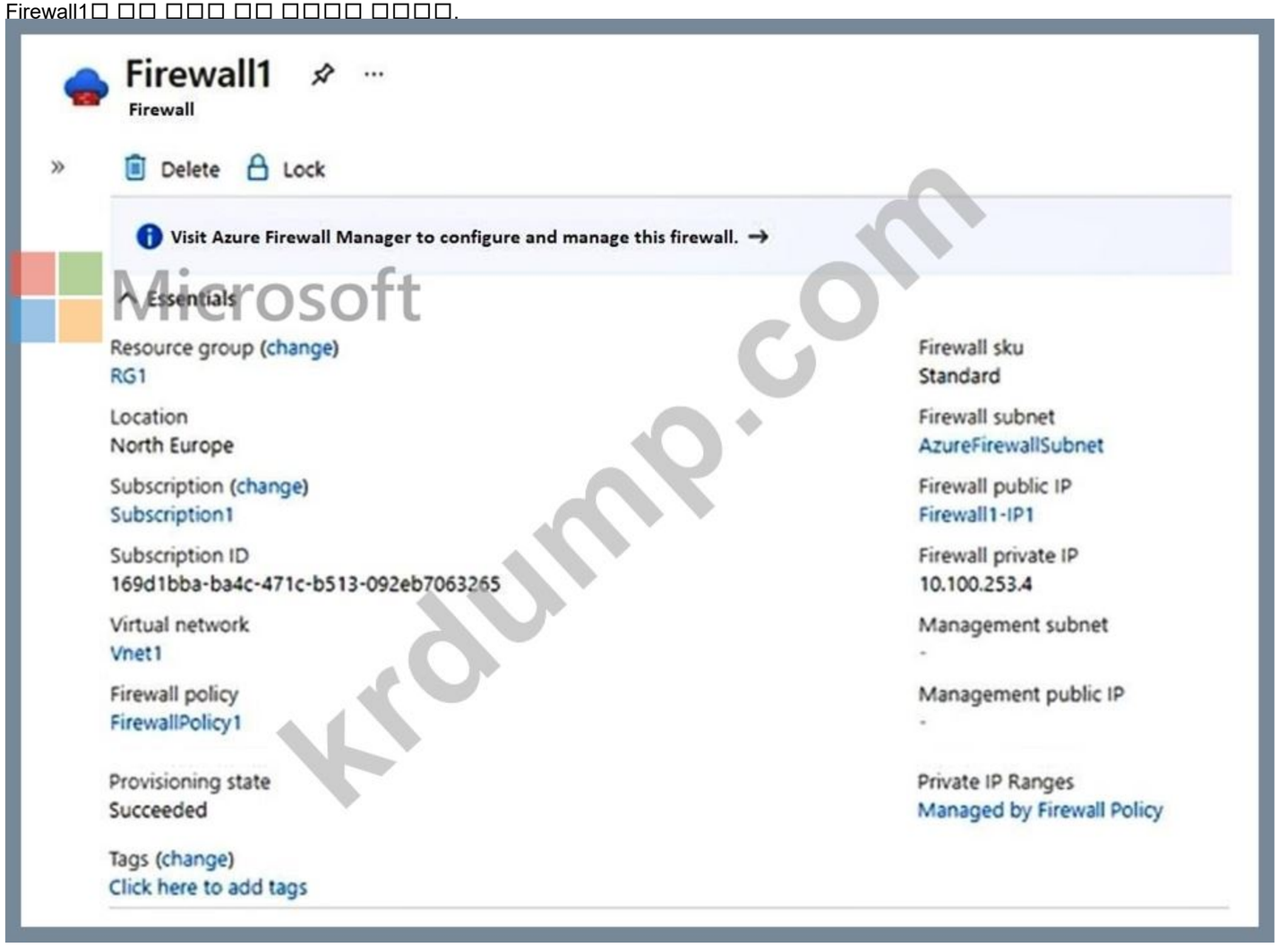
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type
Vnet1	Virtual network
Vnet2	Virtual network
Firewall1	Azure Firewall
Subnet1	Virtual subnet
Subnet2	Virtual subnet
VM1	Virtual machine
VM2	Virtual machine

□□ □□□□ □□□□□ □□ □□□ □□ □□□□.

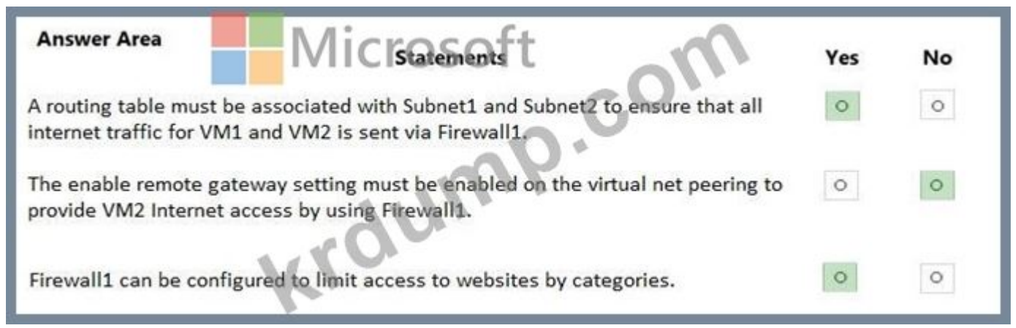


Firewall1□ □□ □□□ □□ □□□□ □□□□.



FirewallPolicy1□□ □□□ □□ □□□ □□□□ □□□□.
- Vnet1□ Vnet2□□ □□□□□ □□□ □□□□ □□□□□.
- Vnet1□ Vnet2 □□ □□ □□□□ □□□□□.
□□□ □□ □□□□ □□□□□, □□□ □□□□□, □□□ □□□ □□ □□□□ □□ □□(NSG)□ □□□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:



Explanation:
Box 1: Yes
You need to add User Defined Route to the Firewall Appliance from the subnets.
Box 2: No
The firewall is not a VPN Gateway, and we do not have any connection with On-Premises here.
Box 3: Yes
Azure Firewall can filter by web categories.
https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal
https://learn.microsoft.com/en-us/answers/questions/516530/how-to-set-up-a-multi-spoke-virtual-network-in-azu
https://learn.microsoft.com/en-us/azure/firewall/web-categories

NEW QUESTION: 198
□□ □□ □□□ □□□ □□ □□ Azure □□□ Azure App Service □□ □□□□.

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

□□ □□ □□□□ □□ □□□ □□ □□ VNet1□□□ □□ □□□□□ □□□□ □□□□ □ □□□ □□ □□□.
□□ □□□□ □ □ □□□□ □□□?

A. 0
B. 1
C. 2
D. 3
E. 6

Answer: C (LEAVE A REPLY)

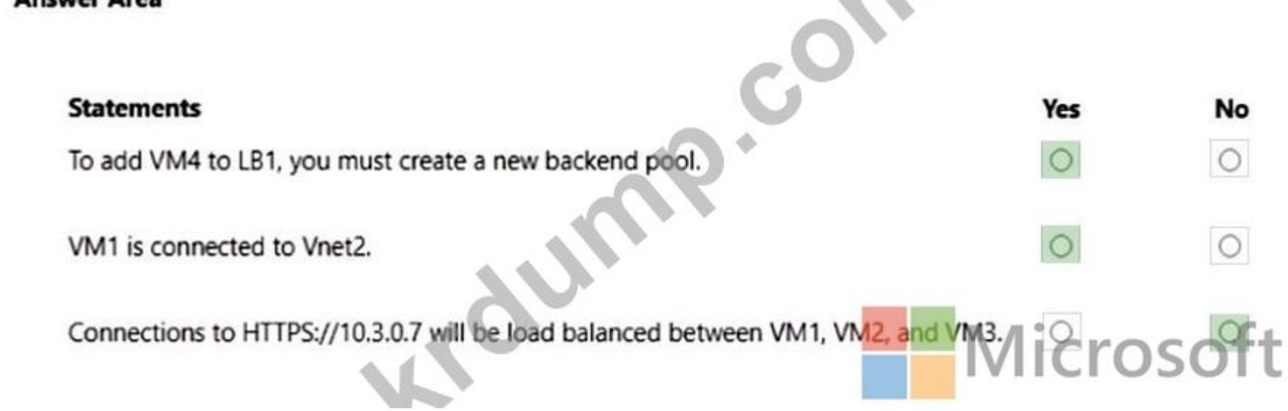
One per App Service Plan: The feature supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can only use the same virtual network integration to a specific subnet. 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: 199

□□□ □□
□□□ □□ □□□ □□ Azure □□ □□□□ □□□□.
- □□: LB1
□□: □□ 2□ □□ □□
- SKU: □□
- □□ IP □□: 10.3.0.7
- □□ □□□ □□: rule1 (Tcp/80)
- □□ □□□: probe1 (Http:80)
- NAT □□: □□□□ 0□
LB1□ □□□ □□ □□□ □□ □□□ □□□ □□□□.
- □□: backend1
- □□ □□□□: Vnet2
- □□□ □ □□: NIC
- IP □□: IPv4
- □□ □□: VM1, VM2, VM3
VM4□□ □□□ Azure □□ □□□ □□□, □□ □□ □□□ □□□□ □□□ □□□ □□□□.
- □□□□ □□□□□: vm4981
- □□ □□□□/□□□: Vnet3/Subnet3
- NIC □□ IP □□: 10.4.0.4
- □□ □□□□: □□□□

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

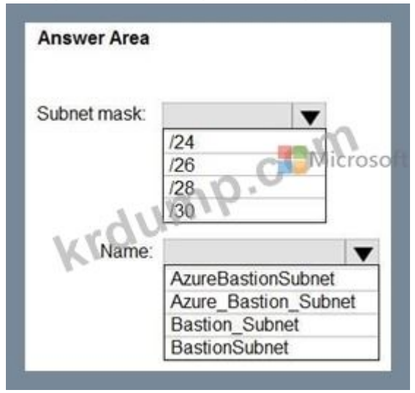
Answer:



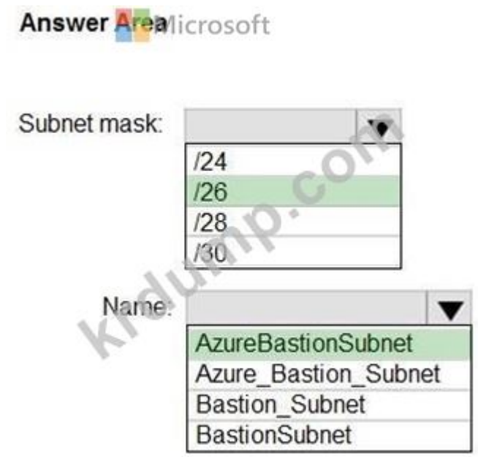
Explanation:
Box 1: Yes
In order to add VM4 to LB1, you must create a new backend pool that includes VM4's network interface (vm4981) in Vnet3/Subnet3.
Box 2: Yes
VM1 is a part of the backend pool "backend1" which is associated with the virtual network Vnet2.
Box 3: No
The load balancing rule "rule1" is configured to load balance traffic on TCP port 80, not HTTPS (TCP port 443). Therefore, connections to https://10.3.0.7 will not be load balanced by LB1.

NEW QUESTION: 200
□□□ □□
Azure □□□□ □□ □□ 20□□ VNet1□□□ □□ □□□□□ □□□□.
Azure Bastion□ □□□□ □□ □□□ □□ □□□□ □□□ □□□□□.
Azure Bastion□ □□□ □□□□ □□□□ □□□. □□□□ □□□□ □□□ IP □□ □□ □□□□□ □□□.
□□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: /26

To minimize the number of IP addresses used by an Azure Bastion subnet, configure it with the smallest allowed subnet size, which is /26 (or larger, like /25 or /24). This provides the minimum necessary IP addresses while still allowing for Bastion's scaling requirements.

Box 2: AzureBastionSubnet

Creating the AzureBastionSubnet:

When creating the subnet for Azure Bastion, name it AzureBastionSubnet.

Assign it a CIDR block of /26 (or larger, like /25 or /24).

Ensure this subnet is within the virtual network's address space.

For example, if your VNet has the address space 10.1.0.0/16, you could assign AzureBastionSubnet as 10.1.1.0/26.

Reference:

https://learn.microsoft.com/en-us/azure/bastion/configuration-settings