

Microsoft.AZ-700-KR.v2026-06-10.q144

□□□□:	AZ-700-KR
□□□□:	Designing and Implementing Microsoft Azure Networking Solutions (AZ-700 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	144
□□:	v2026-06-10
# □□ □:	109
# □□ □□□:	1440
https://www.krdump.com/Microsoft.AZ-700-KR.v2026-06-10.q144.html	

NEW QUESTION: 1

Azure [redacted] Vnet1[redacted] [redacted] [redacted]. Vnet1[redacted] 20[redacted] [redacted] [redacted] [redacted].

□□ □□ 500□. □ □□□□ □□□□ □□□□ □□□□□ □□□□ □□ □□□ □□□ □□□□ □□□□.

□ □ □ □ □ NSG1 □ □ □ □ □ □ □ □ (NSG) □ □ □ □ □ □ □ □ .

[illegible]

NS61 131.107.1.15 IP 000 00 00 0000 0000 0000 000 0000 0000 00 000 0000 000. 0 000 00 00 000 0000 000.

* □□□□□ □□ □□□ 131.107.1.15□□ □□□ □□□□□ □□□□.

* □ □ □ □ □ □ □ □ □ NSG1□ □ □ □ □ □ □ □ □ □ □ □ .

□□ □□ □□□□ □□□□ □□□ □□□□ □□□□ □□□?

A. ☐☐☐ ☐☐

B. IP ☐☐

C. □□□□□□ □□ □□

D. ☐☐ ☐☐☐☐

Answer: C (LEAVE A REPLY)

NEW QUESTION: 2

VM1□□□ □□ □□□ □□□ Azure □□□ □□□□. VM1□□ NIC1□□□ NIC□ PIP1□□□ □□ IP □□□ □□□□. PIP1□ NIC1□ □□□□□.

4□□ □□□□ □□ □□□□□□(NVA)□ □□□ □□□□□.

□□□□ PIP1□ □□□□ □□ □□□□ □□□□ NVA□□ □□□□ □□□. □□□□ NVA □□□ □□□□□ □□□□ □□□.

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

Actions

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

Answer Area

Microsoft

Answer:

Actions

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

Answer Area

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

Microsoft

Explanation:

Actions

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

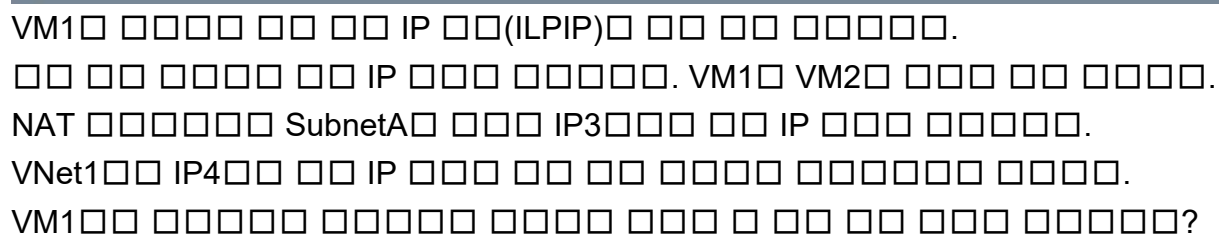
Answer Area

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

Microsoft

NEW QUESTION: 3

□□□□ Azure □□□ □□ □□□□.



- Answer: A (LEAVE A REPLY)**

Subscription1 Subscription2 Azure Vnet1 Vnet2
Subscription1 Vnet1
Subscription2 Vnet2
Vnet1 Vnet2
Vnet1 Vnet2
Vnet1 Vnet2

Actions

- Deploy an Azure Standard Load Balancer in front of the application server.
- In Subscription1, accept the private endpoint connection request.
- In Subscription1, create a private link service and attach the service to the frontend IP configuration of the load balancer.
- In Subscription2, create a private endpoint by using the private link service ID.
- Enable virtual network peering between Vnet1 and Vnet2.

Answer Area

Microsoft

>

<

Answer:

Actions

- Deploy an Azure Standard Load Balancer in front of the application server.
- In Subscription1, accept the private endpoint connection request.
- In Subscription1, create a private link service and attach the service to the frontend IP configuration of the load balancer.
- In Subscription2, create a private endpoint by using the private link service ID.
- Enable virtual network peering between Vnet1 and Vnet2.

Answer Area

- In Subscription1, accept the private endpoint connection request.
- Enable virtual network peering between Vnet1 and Vnet2.
- Deploy an Azure Standard Load Balancer in front of the application server.
- In Subscription1, create a private link service and attach the service to the frontend IP configuration of the load balancer.

Explanation:

Answer Area

Microsoft

- In Subscription1, accept the private endpoint connection request.
- Enable virtual network peering between Vnet1 and Vnet2.
- Deploy an Azure Standard Load Balancer in front of the application server.
- In Subscription1, create a private link service and attach the service to the frontend IP configuration of the load balancer.

NEW QUESTION: 5

Azure App Service □□□□□ 10□ □□□□. □ □□□□□ □□□ □□□ □□□□□□. □ □□□□□ □□ □□ Azure □□□□ □□□□. □□□□ □□ □□□ □□ □□ □□□□□ □□□□□ Azure Traffic Manager□ □□□□ □□□□. □□ □□□ □□□ □□□□ □□□□?

A. □□□

B. □□

- C. □□□□
D. □□□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 6

□□ 11
□□ □ VPN□ □□□□ □□□□□ VNET4□ □□□ □□□ □□ □□□□. VPN□ □□□□□ □□□□□□ Firewall 1□□□ □□□□ □□□□□.
□□□□□ □□□□□ □□□ □□□ □□□□□.
* □□ □□ □□: 10.10.0.0/16.
* □□□ 1 □□ IP □□: 10.10.1.1.
* □□□1 □□ IP □□: 131.107.50.60.
BGP□ □□□□ □□□□□.
□□□□□ □□□□□ IP □□ □□□ □□□ □ VPN□ □□□□ □□□ □□□□ □□□□. □ □□□ □□□□ □□ □□ □□□□ □□□□□□ □□□ □□□ □□□□□.

Answer:

See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for creating the object that will provide the IP addressing configuration of the on-premises network to the Site-to-Site VPN:

- * The object that you need to create is called a local network gateway. A local network gateway represents your on-premises network and VPN device in Azure. It contains the public IP address of your VPN device and the address prefixes of your on-premises network that you want to connect to the Azure virtual network 1 .
- * To create a local network gateway, you need to go to the Azure portal and select Create a resource. Search for local network gateway , select Local network gateway , then select Create 2 .
- * On the Create local network gateway page, enter or select the following information and accept the defaults for the remaining settings:
- * Name: Type a unique name for your local network gateway.
- * IP address: Type the public IP address of your VPN device, which is 131.107.50.60 in this case.
- * Address space: Type the internal address range of your on-premises network, which is 10.10.0.0/16 in this case.
- * Subscription: Select your subscription name.
- * Resource group: Select your resource group name.
- * Location: Select the same region as your virtual network.
- * Select Review + create and then select Create to create your local network gateway 2 .

NEW QUESTION: 7

□□□□□ □□□□□ 10.0.0.0/20□ IP □□ □□□ □□□□□.
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□□.

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

□□□□□ □□□□□ S2S(□□□□ □) VPN□ □□□□ HubVnet□ □□□□□.
AZFW1□□□□ Azure □□□□□ HubVNet□ □□□□□.
AZFW1□ □□□□□ □□□□□ SpokeVNet □□ □□ □□□□ □□□ □ □□□ □□□□ □□□□.

RT1000 000 00 000? 000 00 0000 000 000 000000 0000. 0 0000 0 0, 00 0 00 00 0000 00 0 0000. 0000 000 0 000 00 000 00 0000 000000 0 00 0000.

00: 00 000 10000.



Destinations

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

Answer Area

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

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

Answer:



Destinations

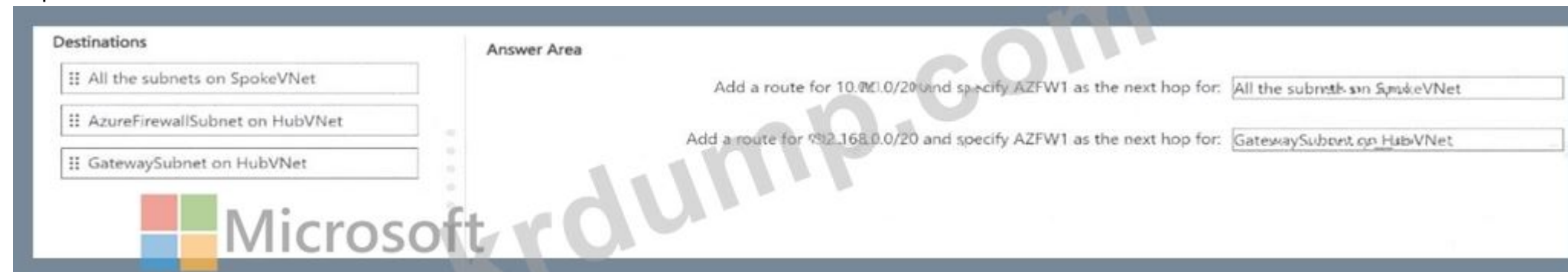
- ⋮ All the subnets on SpokeVNet
- ⋮ AzureFirewallSubnet on HubVNet
- ⋮ GatewaySubnet on HubVNet

Answer Area

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

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

Explanation:



Destinations

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

Answer Area

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

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

NEW QUESTION: 8

Frontend1000 00 0000000 Policy1000 Azure WAF(0 0000000 000) 000 00 Azure Front Door 000000 0000.

Policy10 "string1"0 0000 000 00 000 00000 00000000.

https://www.contoso.com/redirect1. Policy10 Frontend10 00000 0000.

00 0000 000 00000 000.

"string2"0 0000 000 00 Frontend10 00 000 00000 000000000 000.

https://www.contoso.com/redirect2.

00 0 00 000 000 000? 0 000 0000 000 000000.

00: 00 100 10000.


```

{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceId": "/SUBSCRIPTIONS/6efbb4a5-d91a-4e4a-b6bf-5bdd6efea73c/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_HEADERS:User-Agent\\\\\"' required. ",
      "data": "",
      "file": "rules\\REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "appl.contoso.com",
    "transactionId": "d654811d0hgq3ea198165hq/428d74h6",
    "policyId": "default",
    "policyScope": "Global",
    "policyScopeName": "Global"
  }
}

```

Which of the following is the correct interpretation of the log entry?
 The client IP is 137.135.10.24 and the WAF rule ID is 920300.
 The log entry indicates a warning message.

A. The client IP is 137.135.10.24 and the WAF rule ID is 920300.

B. The log entry indicates a warning message.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 11

2

Azure virtual machines are deployed to the France Central region and are in a network segment with an IP address range of 10.5.1.0/24. The virtual machines are unable to connect to the Internet.

Answer:

See the Explanation below for step by step instructions.

Explanation:

To deploy Azure virtual machines to the France Central region and ensure they are in a network segment with an IP address range of 10.5.1.0/24, follow these steps:

Step-by-Step Solution

Step 1: Create a Virtual Network in France Central

* Navigate to the Azure Portal .

- * Search for "Virtual networks" in the search bar and select it.
- * Click on "Create" .
- * Enter the following details :
- * Subscription : Select your subscription.
- * Resource Group : Select an existing resource group or create a new one.
- * Name : Enter a name for the virtual network (e.g., VNet-FranceCentral).
- * Region : Select France Central .
- * Click on "Next: IP Addresses" .

Step 2: Configure the Address Space and Subnet

- * In the IP Addresses tab , enter the address space as 10.5.1.0/24.
- * Click on "Add sub net" .
- * Enter the following details :
 - * Subnet name : Enter a name for the subnet (e.g., Subnet-1).
 - * Subnet address range : Enter 10.5.1.0/24.
- * Click on "Add" .
- * Click on "Review + create" and then "Create" .

Step 3: Deploy Virtual Machines to the Virtual Network

- * Navigate to the Azure Portal .
- * Search for "Virtual machines" in the search bar and select it.
- * Click on "Create" and then "Azure virtual machine" .
- * Enter the following details :
 - * Subscription : Select your subscription.
 - * Resource Group : Select the same resource group used for the virtual network.
 - * Virtual machine name : Enter a name for the VM.
 - * Region : Select France Central .
 - * Image : Select the desired OS image.
 - * Size : Select the appropriate VM size.
- * Click on "Next: Disks" , configure the disks as needed, and then click on "Next: Networking" .
- * In the Networking tab , select the virtual network (VNet-FranceCentral) and subnet (Subnet-1) created earlier.
- * Complete the remaining configuration steps and click on "Review + create" and then "Create" .

Explanation:

- * Virtual Network : A virtual network in Azure allows you to create a logically isolated network that can host your Azure resources.
- * Address Space : The address space 10.5.1.0/24 ensures that the VMs are in a specific network segment.
- * Subnet : Subnets allow you to segment the virtual network into smaller, manageable sections.
- * Region : Deploying the virtual network and VMs in the France Central region ensures that the resources are physically located in that region.

By following these steps, you can ensure that your Azure virtual machines in the France Central region are deployed within the specified IP address range of 10.5.1.0/24.

NEW QUESTION: 12

Azure □□□ □□ □□□□□ □□□□. □ □□ □□□□□□ Subnet1□ Subnet2□□ □ □□ □□□□ □□□□. AppGw1□□□ Azure Application Gateway v2 □□□□□ Subnet 1□ □□□□ □□ □□.

AppGw1 Subnet2 0000 000. 0000 00000 00000 000.

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

ANSWER AREA

Before moving AppGw1, run:

- Set-AzApplicationGatewayHttpListener
- Set-AzPublicIpAddress
- Stop-AzApplicationGateway

To move AppGw1, run:

- Set-AzApplicationGateway
- Set-AzApplicationGatewayListener
- Set-AzApplicationGatewayPrivateLinkConfiguration



Answer:

Answer Area

Before moving AppGw1, run:

- Set-AzApplicationGatewayHttpListener
- Set-AzPublicIpAddress
- Stop-AzApplicationGateway

To move AppGw1, run:

- Set-AzApplicationGateway
- Set-AzApplicationGatewayListener
- Set-AzApplicationGatewayPrivateLinkConfiguration



Explanation:

Answer Area

Before moving AppGw1, run: Stop-AzApplicationGateway

To move AppGw1, run: Set-AzApplicationGateway



NEW QUESTION: 13

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□ □□□ □□□□□.

VWAN1□□ □□□ □□□□ □□□?

A. ☐☐ ☐☐☐☐ ☐☐

B. □□□ VPN □□

C. VPN ☐☐☐

D. □□□□ □□ □□□□□□(NVA)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 14

□□□□ DC1□□□ □□□ □□□□□ □□□□□□ □□□, □ □□□□□□□ □□□ □ □□ □□□□.

Azure 100 10000. 00 0000 VNet1000 00 00000 ErGw3Az SKU0 0000 GW1000 00 000 ExpressRoute 00 0000 000000 0000 0000. GW10 VNet10 00000 0000.

DO□ Circuits□ ExpressRoute Standard □□□ □□□ VNet1□ □□□□□. DC1 □□□□ Circuit1□ □□□□□□ □□□□□. Circuit1 □□□□ □ □□□□□ □□□ □□□□□.

3 .

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

A. □□□□□ □□□ □□□ □□(BFD)□ □□□□□.

B. GW1□ □ □ □ □ - □ □ □ □ □ □ □ □ □ □ .

C. GW1 ☐ ☐ ☐ **SKU** ☐ **UrtraPerformance** ☐ ☐ ☐ ☐ ☐.

D. Circuit1 ☐ ☐ ☐ **FastPath** ☐ ☐ ☐ ☐ ☐.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

ERC1 ExpressRoute

Azure Backup ☐ Azure Cosmos DB ☐☐☐ ECR1☐ ☐☐ ☐-☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐ ☐☐☐. ☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐ ☐☐☐.

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

□□: □□ □□□ 1□□□□.

Answer Area

On the ExpressRoute circuit, configure:

Associate the ExpressRoute circuit with:

Microsoft peering
Azure private peering
Microsoft peering

A route filter and a single filter rule
A route filter and a single filter rule
A route filter and two filter rules
Two route filters and a single filter rule

Answer:

Answer Area

On the ExpressRoute circuit, configure:

- Microsoft peering
- Azure private peering
- Microsoft peering

Associate the ExpressRoute circuit with:

- A route filter and a single filter rule
- A route filter and a single filter rule
- A route filter and two filter rules
- Two route filters and a single filter rule

Explanation:



NEW QUESTION: 16

FD1□□ □□□□ □□□ □□□□□ APPGWI-WAFPolicy□ □□ □□□ □□ □□□ □□□□ □□□. □□□□ □□□ □□ □□□ □□□□ □□□. □□ □□ □□□ □□ □□□ □□□□ □□□?

- A. □□□ □ □□ □□
- B. IP □□ □ RemoteAddr
- C. □□□ □□ □ □□ □□
- D. □□□ □ RequestCookies

Answer: B ([LEAVE A REPLY](#))

AZ-700-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ AZ-700-KR □□! DumpTop □ □□ **AZ-700-KR** □□ □□□ □□□□□□, DumpTop AZ-700-KR □□ □□□ □□□□□□ □□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop AZ-700-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (330 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 17

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

- Vnet1□□□ □□ □□□□
 - Vnet1□ Subnet1□□□ □□□ □□□
 - Subnet1□ □□□□ VM1□□□ □□ □□
 - storage1, storage2, storage3□□□ □□□ □ □□ □□□□ □□
- VM1□ storage1□ □□□□ □ □□□ □□□□ □□□. VM1□ □□ □□□□ □□□ □□□□□ □□□□ □□ □□□.
- □□: □□□□ □□ □□(NSG)□ □□□□. MicrosoftStorage□ □□ □□□ □□□ □□□□ □□ □□□ Subnet1□ □□□□□. □□□ □□□ □□□□□?

- A. □□□
- B. □

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 18

VM1□□□ Azure □□ □□□ □□□□.

Azure Network Watcher□ □□□□ VM1□ □□ □□□□ □□□□ □□□□ □□□.

Which of the following is a valid Azure Storage account type?

- A. Block blob v2 storage account
- B. Block blob storage account
- C. VM1 storage account
- D. Block blob v2 storage account
- E. Blob storage, VM1 storage, Block Blob storage
- F. Block blob v2 storage, VM1 storage, Block Blob storage

Answer: F ([LEAVE A REPLY](#))

NEW QUESTION: 19

NSG1 is a network security group (NSG) in a virtual network.

Name	Resource	Prefix
NSG1	Subnet1	10.10.0.0/24
NSG2	Subnet2	10.10.1.0/24

NSG1 is configured with the following rules:

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

NSG2 is configured with the following rules:

Name	Subnet
VM1	Subnet1
VM2	Subnet1
VM3	Subnet2

NSG2 is configured with the following rules:

Rule 1: Allow traffic from VM1 to VM2 on port 8080.

Rule 2: Allow traffic from VM2 to VM3 on port 9090.

Rule 3: Allow traffic from VM3 to VM1 on port 9090.

Answer Area	
Statements	
VM3 can connect to port 8080 on VM1.	
VM1 and VM2 can connect on port 9090.	
VM1 can connect to VM3 on port 9090.	

Answer:

Answer Area



Statements

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

Explanation:

NO, NO, YES

1. VM3 can connect to port 8080 on VM1 : false, UserRule_DenyVirtualNetworkInbound
2. VM1 and VM2 can connect on port 9090: false, UserRule_DenyVirtualNetworkInbound
3. VM1 can connect to VM3 on port 9090: true

NEW QUESTION: 20

You are configuring a virtual network in Azure. The configuration is as follows.

Route table name	Route name	Prefix	Destination
RT1	Default Route	0.0.0.0/0	VirtualNetworkGateway
RT2	Default Route	0.0.0.0/0	Internet

The virtual network is configured as follows.

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

Two virtual machines are configured as follows.

Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

You are configuring a virtual network in Azure. The configuration is as follows.

The virtual network is configured as follows.

Two virtual machines are configured as follows.

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:

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:

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	☒	☐

Reference:

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

NEW QUESTION: 21

APPGW1 is a public IP address assigned to a virtual machine. The virtual machine is running a web application. How can you ensure that the application is secure?

- A. SSL certificate is issued by CA and the application is configured to use TLS encryption to communicate with the client.
- B. SSL certificate is issued by CA and the application is configured to use TLS encryption to communicate with the client.
- C. SSL certificate is issued by CA and the application is configured to use TLS encryption to communicate with the client.
- D. SSL certificate is issued by CA and the application is configured to use TLS encryption to communicate with the client.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 22

You are a system administrator for a company that has a web application running on Azure. The application is running on two virtual machines (VMs) in the West Europe region. The VMs are named App1eu and App1us. The application is configured to use the URL https://www.fabrikam.com. You need to ensure that the application is available in the East US region. What should you do?

Name	Location	Description
App1eu	West Europe	Production app service for a URL of https://www.fabrikam.com
App1us	East US	Standby app service for a URL of https://www.fabrikam.com

Azure Traffic Manager is a service that can be used to route traffic to the appropriate VM. You need to configure Traffic Manager to route traffic to the appropriate VM. What should you do?

- * https://www.fabrikam.com is the URL of the application. App1eu is the name of the VM in the West Europe region. App1us is the name of the VM in the East US region.
- * App1eu is the name of the VM in the West Europe region. https://www.fabrikam.com is the URL of the application. App1us is the name of the VM in the East US region.

You need to ensure that the application is available in the East US region. What should you do?
You need to ensure that the application is available in the East US region. What should you do?
You need to ensure that the application is available in the East US region. What should you do?

- A. Create a new Traffic Manager profile and configure it to route traffic to the appropriate VM.
- B. Create a new DNS record and configure it to route traffic to the appropriate VM.
- C. Create a new Traffic Manager profile and configure it to route traffic to the appropriate VM.
- D. Create a new DNS record and configure it to route traffic to the appropriate VM.

fabrikam.com is the URL of the application. CNAME is the name of the DNS record. What should you do?

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 23

You are a system administrator for a company that has a web application running on Azure. The application is running on two virtual machines (VMs) in the West Europe region. The VMs are named App1eu and App1us. The application is configured to use the URL https://www.fabrikam.com. You need to ensure that the application is available in the East US region. What should you do?

VNet1 is a virtual network that is connected to the Internet. VNet1 is connected to the Internet via a Gateway 1 ExpressRoute connection. You need to ensure that the application is available in the East US region. What should you do?

Fabrikam, Inc. is the company that owns the application. ExpressRoute is the name of the connection. VNet1 is the name of the virtual network. Azure is the name of the cloud provider. What should you do?

Answer Area

Answer:

Answer Area

Maximum number of ports:

Increase the number of:

Microsoft

Explanation:

Answer Area

Maximum number of ports: 128K

Increase the number of: Frontend IP addresses for LB1

NEW QUESTION: 25

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

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

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

Hub1□ □□ □□□ '□□□□ □□'□□□.

Hub1□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □□□.

□□□: Azure Front Door □□□□ □□□□□.

□□□ □□ □□□ □□□□□?

A. ☐

B. ☐

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 26

VNet1 is a virtual network in Azure. VNet1 has a single IP address space.

* IPv4: 192.168.0.0/24

* IPv6: fd0adbftdeca:deed:y48

Azure VPN is a virtual network in Azure. VNet1 is connected to Azure VPN.

VNet1 has a single IP address space. The IP address space is 192.168.0.0/24.

* The IP address space is 192.168.0.0/24.

* VPN is a virtual network in Azure. VNet1 is connected to VPN.

The IP address space is 192.168.0.0/24? The IP address space is 192.168.0.0/24.

IP: 192.168.0.0/24.



Answer:

Answer Area



Explanation:



NEW QUESTION: 27

App1 is a web application in Azure. App1 is connected to Azure App Service. App1 is connected to Azure App Service.

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

Which of the following is a valid configuration for Azure Traffic Manager?

* App1 is an Azure App Service endpoint.

* App1 is an Azure App Service endpoint.

* App1 is an Azure App Service endpoint.

Answer Area

Minimum number of Traffic Manager profiles required: 2

Routing method for the traffic in each region: Performance

Answer:

Answer Area

Minimum number of Traffic Manager profiles required: 2

Routing method for the traffic in each region: Performance

Explanation:

Answer Area

Minimum number of Traffic Manager profiles required: 2

Routing method for the traffic in each region: Performance

NEW QUESTION: 28

VM1 is an Azure VM.

Azure Network Watcher is used to monitor VM1. Which of the following is a valid configuration for the network watcher?

- A. VM1 is v2 VM and the network watcher is configured to monitor VM1.
- B. VM1 is v2 VM and the network watcher is configured to monitor VM1.
- C. VM1 is v2 VM and the network watcher is configured to monitor VM1.
- D. VM1 is v2 VM and the network watcher is configured to monitor VM1.
- E. VM1 is v2 VM and the network watcher is configured to monitor VM1.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 29

Scenario: A company is planning to migrate its on-premises data center to the cloud. The company has a large amount of data and a large number of servers. The company wants to migrate the data and servers to the cloud in a secure and efficient manner. The company wants to use Azure to migrate the data and servers. The company wants to use Azure to migrate the data and servers. The company wants to use Azure to migrate the data and servers.

The company wants to use Azure to migrate the data and servers. The company wants to use Azure to migrate the data and servers. The company wants to use Azure to migrate the data and servers.

The company wants to use Azure to migrate the data and servers. The company wants to use Azure to migrate the data and servers. The company wants to use Azure to migrate the data and servers.

- Vnet1 is a VNet in the Azure cloud.

- Vnet1 is a VNet in the Azure cloud.

- Subnet1 is a subnet in the VNet1.

- storage1, storage2, storage3 are storage accounts in the Azure cloud.

VM1 is a VM in the Azure cloud. VM1 is connected to storage1, storage2, and storage3. VM1 is connected to storage1, storage2, and storage3.

NSG1 is a network security group in the Azure cloud. NSG1 is connected to Subnet1. NSG1 is connected to Subnet1.

Which of the following is a valid configuration for the network security group?

- A. NSG1 is a network security group in the Azure cloud.
- B. NSG1 is a network security group in the Azure cloud.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 30

Azure is a cloud platform.

Azure Virtual WAN is a service that provides a secure and efficient way to connect on-premises networks to the cloud.

Which of the following is a valid configuration for the Azure Virtual WAN?

* 4Gbps is the maximum bandwidth for the Azure Virtual WAN.

* 8Gbps is the maximum bandwidth for the Azure Virtual WAN.

* 16Gbps is the maximum bandwidth for the Azure Virtual WAN.

Which of the following is a valid configuration for the Azure Virtual WAN?

Answer: A (LEAVE A REPLY)

Answer Area

For the S2S VPN gateway:

8
2
4
8
16

For the ExpressRoute gateway:

4
2
4
8
16

Answer:

For the S2S VPN gateway:

8
2
4
8
16

For the ExpressRoute gateway:

4
2
4
8
16

Explanation:

Answer Area

For the S2S VPN gateway: 8

For the ExpressRoute gateway: 4

NEW QUESTION: 31

RG1 is a resource group in VNet1. You need to configure Azure Firewall. Which resource should you create first?

- A. AzureFirewallNetworkInterface
- B. VNet1 AzureFirewallSubnet
- C. AzureFirewallResourceGroup
- D. AzureFirewallHub

Answer: (SHOW ANSWER)

AZ-700-KR is a new exam for Microsoft Azure. DumpTop has the latest AZ-700-KR questions! DumpTop has the latest **AZ-700-KR** questions and answers, DumpTop AZ-700-KR questions and answers are available. DumpTop AZ-700-KR questions and answers are available. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (330 Q&As Dumps, 30%OFF)

Special Discount: **KrDump**)

NEW QUESTION: 32

Two Azure subscriptions, Sub1 and Sub2, are used to create the following resources:

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

VNet1 and VNet2 are connected via a virtual network link.

VNet1 and VNet2 are connected via a virtual network link. An Azure Private Link is also created in Sub1.

Link1 is a virtual network link connecting VNet1 and VNet2.

* VM1 and VM2 are connected to VNet1 and VNet2 respectively.

* VM1 and VNet2 are connected via a virtual network link. The link is named Link1. The link is created in Sub1.

Link1 is a virtual network link connecting VNet1 and VNet2. The link is created in Sub1.

Link1 is a virtual network link connecting VNet1 and VNet2.

Resources

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

Answer Area

Microsoft

VNet1:

VNet2:

Answer:

Resources

A load balancer

A NAT gateway

A private endpoint

A routing server

A service endpoint

A virtual network gateway

Virtual network peering

Answer Area

VNet1 A private endpoint

VNet2 Virtual network peering

Explanation:

Resources

A load balancer

A NAT gateway

A private endpoint

A routing server

A service endpoint

A virtual network gateway

Virtual network peering

Answer Area

VNet1: A private endpoint

VNet2: Virtual network peering

NEW QUESTION: 33

□□□ 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. □□□ □□□□□
- B. Azure Private Link □□□
- C. □□□□□□ □□ □□
- D. □□ □□□□□ □□□□ □□

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 34

VM1 is an Azure virtual machine.

Azure Network Watcher is configured to monitor VM1. You want to monitor the connectivity of VM1 to the Internet.

Which network resource should you monitor?

A. Blob storage

B. VM1's network interface

C. VM1's network interface's IP configuration

D. Blob storage, VM1's network interface, and VM1's network interface's IP configuration

E. VM1's network interface's IP configuration and VM1's network interface

F. Blob storage and VM1's network interface's IP configuration

Answer: (SHOW ANSWER)

NEW QUESTION: 35

VNet1 is an Azure virtual network.

AppGw1 is an Azure Application Gateway v2 instance in VNet1. AppGw1 has two IP configurations. The first IP configuration is connected to VNet1. The second IP configuration is connected to a public IP address.

AppGw1 has two IP configurations. Which IP configuration should you use to connect AppGw1 to the Internet?

Answer Area

Private IP addresses: 2

Public IP addresses: 0

Microsoft

Answer:

Answer Area

Private IP addresses: 2

Public IP addresses: 0

Microsoft

Explanation:

Answer Area

Private IP addresses: 2

Public IP addresses: 0

Microsoft

NEW QUESTION: 36

Azure ☐☐☐ ☐ ☐ ☐☐☐☐.

☐ ☐☐☐ ☐☐ Azure ☐☐☐☐ ☐☐☐☐☐☐.

* □□□ □□ 1□ 50□□ □□ □□□ □□□□□.

* □□□ □□ 2□ 50□□ □□ □□□□ □□□□□.

* □□□ □□ 3□ 50□□ □□ □□□□ □□□□□.

□□ □ □□ □□ □□□□□ /25 □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer:

Answer Area

Virtual networks: 2

Subnets: 4

Microsoft

Explanation:

Answer Area



NEW QUESTION: 37

Azure 1000 10000. 00 00000 0000 00 0000 00 Azure 0000000 0000000 00000 00000.

* 00: AppGW1

* 00 00000 V2

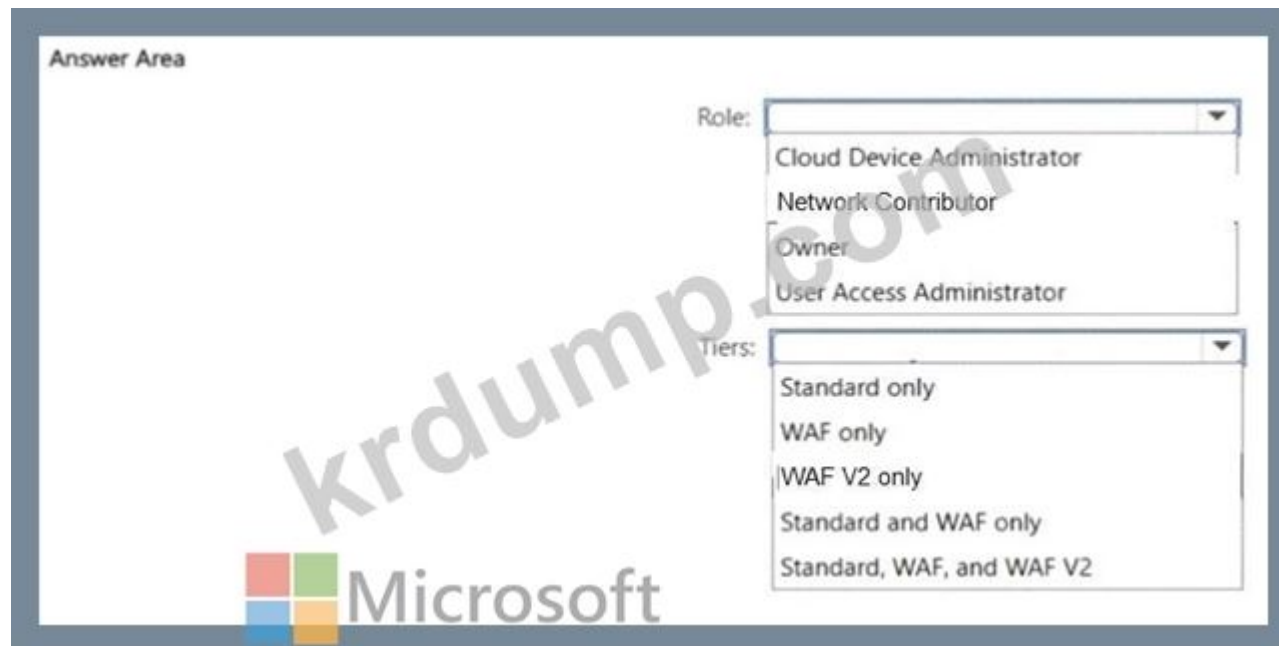
* 00 00 00: 000000

User1000 00000 000000.

User10 AppGW10 0000 0000 0 0000 00 0000. 00000 00 00 0000 00000 0000.

User10 00 0000 00000 00, AppGW10 00 00000 0000 0 00000? 000000 00 00000 0000 0000 000000.

00: 00 0000 100000.



Answer:



Explanation:

Answer Area



NEW QUESTION: 39

□□ 4

10.1.1.0/24 □□□ IP □□□ storage34280945.pnvatelinlcblob.core.windows.net □□□ □□□□ storage34280945 □□□□ □□□ □□□ □ □□□ □□□□ □□□.

Answer:

See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that connections to the storage34280945 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name stor-age34280945.pnvatelinlcblob.core.

windows.net:

- * To allow access from a specific IP address range, you need to configure the Azure Storage firewall and virtual network settings for your storage account. You can do this in the Azure portal by selecting your storage account and then selecting Networking under Settings 1 .
- * On the Networking page, select Firewall s and virtual networks, and then select Selected networks under Allow access from 1 . This will block all access to your storage account except from the networks or resources that you specify.
- * Under Firewall, select Add rule, and then enter 10.1.1.0/24 as the IP address or range. You can also enter an optional rule name and description 1 . This will allow access from any IP address in the 10.1.1.0/24 range.
- * Select Save to apply your changes 1 .
- * To map a custom domain name to your storage account, you need to create a CNAME record with your domain provider that points to your storage account endpoint 2 . A CNAME record is a type of DNS record that maps a source domain name to a destination domain name.
- * Sign in to your domain registrar's website, and then go to the page for managing DNS settings 2 .
- * Create a CNAME record with the following information 2 :
 - * Source domain name: stor-age34280945.pnvatelinlcblob.core.windows.net
 - * Destination domain name: stor-age34280945.pnvatelinlcblob.core.windows.net
- * Save your changes and wait for the DNS propagation to take effect 2 .
- * To register the custom domain name with Azure, you need to go back to the Azure portal and select your storage account. Then select Custom domain under Blob service 2 .
- * On the Custom domain page, enter stor-age34280945.pnvatelinlcblob.core.windows .net as the custom domain name and select Save 2 .

NEW QUESTION: 40

□ □ 8

```
storage34280945  VNET1
```

Answer:

See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that the storage34280945 storage account will only accept connections from hosts on VNET1:

* To restrict network access to your storage account, you need to configure the Azure Storage firewall and virtual network settings for your storage account. You can do this in the Azure portal by selecting your storage account and then selecting Networking under Settings 1 .

* On the Networking page, select Firewalls and virtual networks , and then select Selected networks under Allow access from 1 . This will block all access to your storage account except from the networks or resources that you specify.

* Under Virtual networks, select + Add existing virtual network. Then select VNET1 from the list of virtual networks and select the sub net that contains the hosts that you want to allow access to your storage account 1 . This will enable a service endpoint for Storage in the sub net and configure a virtual network rule for that subnet through the Azure storage firewall 2 .

* Select Add to add the virtual network and subnet to your storage account 1 .

* Select Save to apply your changes 1 .

NEW QUESTION: 41

□□□□□ □□□□ 3□ □□□□. □ □□□□□ □□ VPN □□□ □□□□.

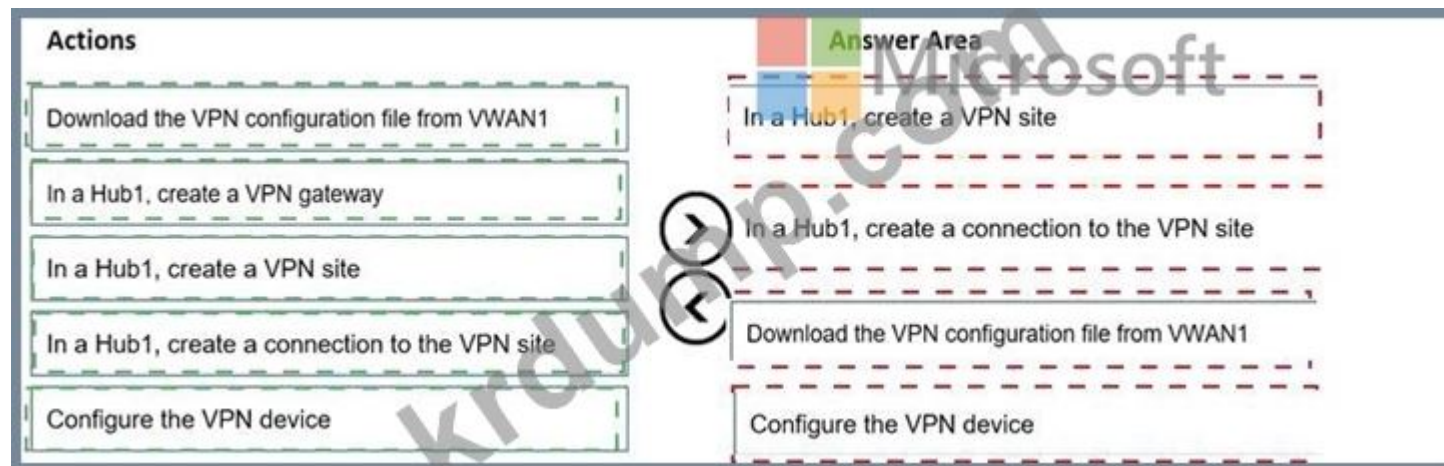
VWAN1000 Azure 00 WAN0 00, 0 WAN0 Hub1000 000 0000. Hub10 000 0 VPN 000 0000 0-0000 000 30 0 200 00000.

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

[illegible]

Actions	Answer Area
Download the VPN configuration file from VWAN1	
In a Hub1, create a VPN gateway	
In a Hub1, create a VPN site	
In a Hub1, create a connection to the VPN site	
Configure the VPN device	

Answer:



Explanation:



Reference:

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal>

NEW QUESTION: 42

Admin1 is a user in the RG1 resource group in the Azure subscription.

RG1 contains the NW1 Azure Network Watcher resource.

Admin1 wants to create a new resource in the RG1 resource group. What should Admin1 do?

Admin1 should create a new resource in the RG1 resource group.

A. Create a new resource in the RG1 resource group.

B. Create a new resource in the RG1 resource group.

C. Create a new resource in the RG1 resource group.

D. Create a new resource in the RG1 resource group.

Answer: (SHOW ANSWER)

NEW QUESTION: 43

Admin1 is a user in the VNet1 resource group in the Azure subscription.

Admin1 wants to create a new resource in the VNet1 resource group. What should Admin1 do?

Admin1 should create a new resource in the VNet1 resource group, Azure subscription, and the VNet1 resource group.

Admin1 should create a new resource in the VNet1 resource group.

Answer Area

Virtual machine: Windows Server 2022 Datacenter: Azure Edition

Tool: Windows Admin Center

Answer:

Answer Area

Virtual machine: Windows Server 2022 Datacenter: Azure Edition

Tool: Windows Admin Center

Explanation:

Answer Area

Virtual machine: Windows Server 2022 Datacenter: Azure Edition

Tool: Windows Admin Center

NEW QUESTION: 44

<https://www.contoso.com> Azure Active Directory (AAD) tenant.

contoso.com.

contoso.com. The application is configured to use the AAD tenant. The application is configured to use the AAD tenant. The application is configured to use the AAD tenant.

contoso.com. The application is configured to use the AAD tenant. The application is configured to use the AAD tenant. The application is configured to use the AAD tenant.

com. The application is configured to use the AAD tenant. The application is configured to use the AAD tenant. The application is configured to use the AAD tenant.

com. The application is configured to use the AAD tenant. The application is configured to use the AAD tenant. The application is configured to use the AAD tenant.

- A. 100 Mbps.
- B. 100 Gbps.
- C. 100 Mbps.
- D. 100 Gbps.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 45

100 Mbps 30 Mbps.

100 Mbps Azure WAN 100 Mbps Azure WAN. 100 Mbps WAN 100 Mbps 1Gbps 100 Mbps 100 Mbps 100 Mbps.

100 Mbps 100 Mbps (S2S) VPN 100 Mbps 100 Mbps WAN 100 Mbps.

100 Mbps 100 Mbps 3Gbps 100 Mbps. 100 Mbps 100 Mbps 100 Mbps.

100 Mbps?

- A. Azure 100 Mbps VPN 100 Mbps.
- B. 100 Mbps 100 SKU 100 Mbps.
- C. 100 Mbps 100 Mbps.
- D. 100 Mbps 100 Mbps 100 Mbps.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 46

100 Mbps 100 Mbps 100 Mbps Azure 100 Mbps.

Name	Type	Description
VWAN1	Azure Virtual WAN	Standard Virtual WAN
Hub1	Azure Virtual WAN hub	Hub for VWAN1
VNet1	Virtual network	Connected to Hub1
VNet2	Virtual network	Connected to Hub1
VNet3	Virtual network	Peered with VNet2
NVA1	Virtual machine	Hosts a routing appliance deployed to VNet2

NVA1 Hub1 100 Mbps BGP 100 Mbps.

BGP 100 Mbps 100 Mbps Hub1 100 Mbps VNet1 VNet3 100 Mbps 100 Mbps 100 Mbps. 100 Mbps 100 Mbps 100 Mbps.

100 Mbps 100 Mbps? 100 Mbps 100 Mbps 100 Mbps 100 Mbps.

100: 100 Mbps 100 Mbps.

Answer Area

On Hub1, propagate routes from connections to VNet1 and VNet2 to:

- | | |
|--|----------------------------------|
| A custom route table and associate the routes with the same custom route table | ☒ |
| A custom route table and associate the routes with the defaultRouteTable | ☐ |
| A custom route table and associate the routes with the same custom route table | ☐ |
| The defaultRouteTable and associate the routes with the defaultRouteTable | ☐ |

On VNet3, implement:

- User-defined routes
- Azure Route Server on a dedicated subnet
 - Azure VPN Gateway on a dedicated subnet
 - User-defined routes

Answer:

Answer Area

On Hub1, propagate routes from connections to VNet1 and VNet2 to:

- | | |
|--|---|
| A custom route table and associate the routes with the same custom route table |  |
| A custom route table and associate the routes with the defaultRouteTable | |
| A custom route table and associate the routes with the same custom route table | |
| The defaultRouteTable and associate the routes with the defaultRouteTable | |

On VNet3, implement:

- User-defined routes
- Azure Route Server on a dedicated subnet
 - Azure VPN Gateway on a dedicated subnet
 - User-defined routes

Explanation:

Answer Area

On Hub1, propagate routes from connections to VNet1 and VNet2 to:

- A custom route table and associate the routes with the same custom route table

On VNet3, implement:

- User-defined routes

AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-700-KR ☐☐! DumpTop ☐ ☐☐ **AZ-700-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐
☐☐ ☐☐☐ ☐☐☐☐☐☐☐. ☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop AZ-700-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (**330 Q&As Dumps**, **30%OFF**)

Special Discount: **KrDump**)

NEW QUESTION: 47

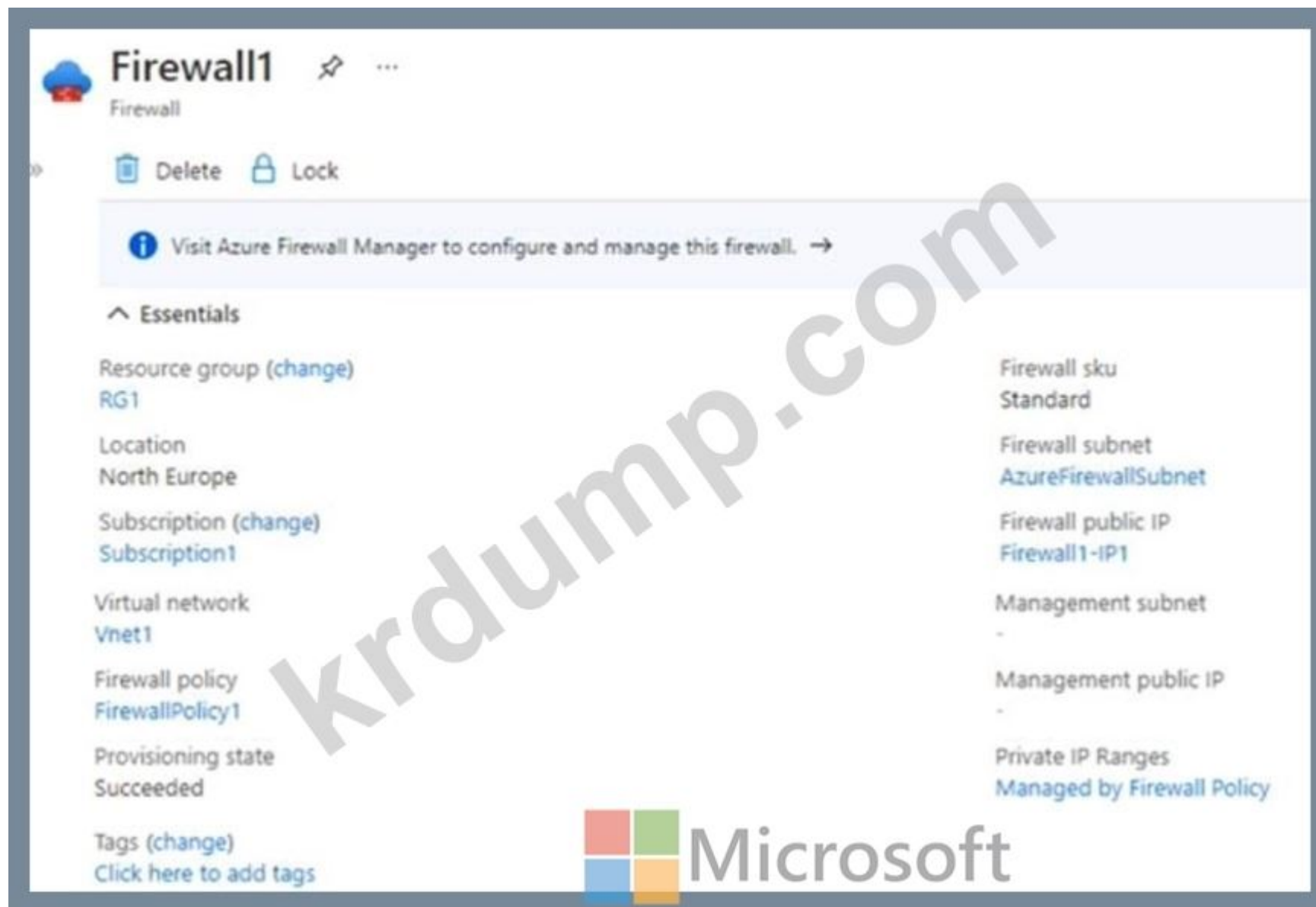
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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 is a FirewallPolicy resource.

* Vnet1 is a Vnet resource.

* Vnet1 is a Vnet resource.

Subnet1 is a Subnet resource, Subnet2 is a Subnet resource, Subnet3 is a Subnet resource (NSG) is a NetworkSecurityGroup resource. Subnet1 is associated with FirewallPolicy1. Subnet2 is associated with FirewallPolicy1. Subnet3 is associated with FirewallPolicy1. Subnet1 is associated with FirewallPolicy1. Subnet2 is associated with FirewallPolicy1. Subnet3 is associated with FirewallPolicy1.

Answer Area

Statements

A routing table must be associated with Subnet1 and Subnet2 to ensure that all internet traffic for VM1 and VM2 is sent via Firewall1.

The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.

Firewall1 can be configured to limit access to websites by categories.

Yes

No

☐
☐
☐
☐
☐
☐

Answer:

Answer Area

Statements



A routing table must be associated with Subnet1 and Subnet2 to ensure that all internet traffic for VM1 and VM2 is sent via Firewall1.

The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.

Firewall1 can be configured to limit access to websites by categories.

Yes

No

☐☐☐☐☐☐

NEW QUESTION: 48

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

- A. Azure □□□
- B. IP □□ □□
- C. □□ □□□
- D. Azure □□□ □□□

Answer: (SHOW ANSWER)

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor>

NEW QUESTION: 49

□□□ □□□ □□ □□□□□ □□□ □□□ □□□□ □□□□. □□ □□ Azure □□□ □□□ □□□ □□□□□. □ □□□ □□ □□ □□□□ Azure □□□□ □□□□ □□□□. □□ 1Gbps □ □□□□□ ExpressRoute □ □□□□ □□□. ExpressRoute Unlimited □□□ □□□□ □□□□ □□□. □□□□ □□□ □□□□□ □□□. □□ □□□ ExpressRoute □□□ □□□□ □□□?

- A. ExpressRoute □□
- B. □□□□□□□ □□□□
- C. ExpressRoute □□□□
- D. ExpressRoute □□

Answer: A (LEAVE A REPLY)

Reference:

<https://azure.microsoft.com/en-us/pricing/details/expressroute/>

NEW QUESTION: 50

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

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

You have an Azure Front Door instance. The instance has two listeners. The first listener is named "As1" and is configured to route traffic to the web app URLs listed in the table below. The second listener is named "As2" and is configured to route traffic to the web app URLs listed in the table below. You need to ensure that traffic to the "As1" listener is routed to the web app URLs listed in the table below. What should you do?

Answer Area

Listeners: 1

Routing rules: 1

Answer:

1, 2

NEW QUESTION: 51

You have an Azure Front Door instance. The instance has two listeners. The first listener is named "As1" and is configured to route traffic to the web app URLs listed in the table below. The second listener is named "As2" and is configured to route traffic to the web app URLs listed in the table below. You need to ensure that traffic to the "As1" listener is routed to the web app URLs listed in the table below. What should you do?

FD1
✦ ☆ ...

Front Door and CDN profiles

✕
Purge cache
⌚ Origin response timeout
🗑️ Delete
🔄 Refresh

^ Essentials
JSON View

Resource group (move)

:

BG6

Status

:

Active

Location

:

Global

Subscription (move)

:

Azure Pass - Sponsorship

Subscription ID

:

9651bd2a-3894-4fd9-9dbf-915f7d861d3e

Name

:

FD1

Pricing Tier

:

Azure Front Door Standard

Front Door ID

:

a4019e23-cd4e-4440-8792-4f9bc3a4c070

Origin response timeout

:

60 Seconds

Tags (edit)

:

Click here to add tags

Properties

Monitoring

Recommendations

Endpoints

Endpoint hostname

Endpoint1-fwgyhnhbdtqc2es.z01.azurefd.net

✔ Provision succeeded

✔ Enabled

Custom domains

Security policy

Routes

Route name

default-route

✔ Provision succeeded

✔ Enabled

Origin groups

Origin group name

default-origin-group

✔ Provision succeeded

FD1 is connected to Azure Private Link.

What is the status of the connection?

A. The connection is in the 'Establishing' state.

B. The connection is in the 'Established' state.

C. The connection is in the 'Failed' state.

D. The connection is in the 'Disconnected' state.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 52

Vnet2 and Vnet3 are connected via a virtual hub. What is the status of the connection?

What is the status of the connection?

A. Connected

B. BGP peering is established

- C. Vnet1 ☐ GatewaySubnet ☐ ☐ ☐ ☐ ☐ ☐
- D. Vnet2 ☐ Vnet3 ☐ GatewaySubnet ☐ ☐ ☐ ☐ ☐ ☐

Answer: B ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 53

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

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:

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:

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.	☐	☒

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: 54

Vnet1 is a virtual network in Azure. Vnet1 is connected to the Internet. Vnet1 is connected to the Internet.

App1 is an Azure App Service. App1 is connected to the Internet.

App1 is connected to Vnet1. App1 is connected to Vnet1. App1 is connected to Vnet1.

App1 is connected to Vnet1. App1 is connected to Vnet1.

A. App1 is connected to Vnet1.

B. App1 is connected to Vnet1.

C. NAT is connected to Vnet1.

D. App1 is connected to Vnet1.

Answer: D (LEAVE A REPLY)

Virtual network integration depends on a dedicated subnet.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual-network-integration> For outgoing traffic from Web App to vnet, it will go through Internet, so the cost not the minimum.

The connection between the Private Endpoint and the Web App uses a secure Private Link. Private Endpoint is only used for incoming flows to your Web App. Outgoing flows will not use this Private Endpoint, but you can inject outgoing flows to your network in a different subnet through the VNet integration feature.

<https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint#conceptual-overview>

NEW QUESTION: 55

Vnet1 is a virtual network in Azure. Vnet1 is connected to the Internet.

500 is a virtual network in Azure. 500 is connected to the Internet.

NSG1 is a network security group in Azure. NSG1 is connected to the Internet.

Vnet1 is a virtual network in Azure. Vnet1 is connected to the Internet.

NS61 is an IP address 131.107.1.15 that is used to connect to the Internet. It is a public IP address. What is the purpose of this IP address?

* It is used to connect to the Internet.

* It is used to connect to the Internet.

What is the purpose of this IP address?

A. It is used to connect to the Internet.

B. It is used to connect to the Internet.

C. It is used to connect to the Internet.

D. It is used to connect to the Internet.

Answer: (SHOW ANSWER)

NEW QUESTION: 56

DNSR1 is a DNS server that is used to resolve domain names to IP addresses.

azure.proseware.com is a domain name that is used to connect to the Internet. It is a public IP address. What is the purpose of this IP address?

It is used to connect to the Internet.

It is used to connect to the Internet.

Answer Area

azure.proseware.com:	168.63.129.16 168.63.129.16 192.168.0.100 The first IP address of the inbound endpoint subnet of PRDNS1 The first IP address of the outbound endpoint subnet of PRDNS1
corp.proseware.com:	192.168.0.100 168.63.129.16 192.168.0.100 The first IP address of the inbound endpoint subnet of PRDNS1 The first IP address of the outbound endpoint subnet of PRDNS1

Answer:

Answer Area

azure.proseware.com:	168.63.129.16 168.63.129.16 192.168.0.100 The first IP address of the inbound endpoint subnet of PRDNS1 The first IP address of the outbound endpoint subnet of PRDNS1
corp.proseware.com:	192.168.0.100 168.63.129.16 192.168.0.100 The first IP address of the inbound endpoint subnet of PRDNS1 The first IP address of the outbound endpoint subnet of PRDNS1

Explanation:

Answer Area

azure.proseware.com:	168.63.129.16
corp.proseware.com:	192.168.0.100

Microsoft

NEW QUESTION: 57

Sub1 Azure, Tenant1 Microsoft Entra. Sub1 VNetGW1 Azure VPN.

Tenant1 ☐ Azure VPN ☐☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

□□ □(P2S) VPN □□□ □□ Microsoft Entra □□□ □□□□□ VNetGW1□ □□□□ □□□. □□□□ □□□□ Azure VPN □□□□□□ □□□□ P2S VPN □□□ □□□ □ □□□ □□ □□□.

VNetGW1 □ Point-to-Site □□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□?

□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer:

Answer Area

 Microsoft

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>

Explanation:

Answer Area

Microsoft

Tenant:

Issuer:

NEW QUESTION: 58

NSG1□□□ □□□□ □□ □□□ □□□□.

NSG1 □ □ □ □ □ □ □ □ (NSG) □ □ □ □ □ □ □ □ . □ □ □ □ □ □ □ □ □ □ □ □ .

□□ □□ □□□ □□□□ □□□?

A. ☐☐☐☐ Block blobs Azure Storage ☐☐

B. ☐☐ ☐☐ v2 Azure Storage ☐☐

* Search for "Private DNS zones" in the search bar and select it.

- * Click on "Create".
- * Enter the DNS zone name as contoso.azure.
- * Select the appropriate subscription and resource group.
- * Click on "Review + create" and then "Create".

Step 2: Link VNET1 and VNET2 to the DNS Zone

- * Go to the newly created DNS zone (contoso.azure).
- * Select "Virtual network links" from the left-hand menu.
- * Click on "Add".
- * Enter a name for the link (e.g., VNET1-link).
- * Select the subscription and virtual network (VNET1).
- * Enable auto-registration to ensure that VMs are automatically registered in the DNS zone.
- * Click on "OK".
- * Repeat the process for VNET2.

Step 3: Configure DNS Settings for VNET1 and VNET2

- * Navigate to VNET1 in the Azure Portal.
- * Select "DNS servers" under the "Settings" section.
- * Ensure that the DNS server is set to "Default (Azure-provided)".
- * Repeat the process for VNET2.

Step 4: Verify Name Resolution

- * Deploy a virtual machine in VNET1 and another in VNET2.
- * Connect to the virtual machines using Remote Desktop Protocol (RDP) or Secure Shell (SSH).
- * Test name resolution by pinging the VM in VNET2 from the VM in VNET1 using its hostname (e.g., ping <VM-name>.contoso.azure).

Explanation:

- * Private DNS Zone: This allows you to manage and resolve domain names in a private network without exposing them to the public internet.
- * Virtual Network Links: Linking VNET1 and VNET2 to the DNS zone ensures that VMs in these networks can register their DNS records automatically.
- * Auto-registration: This feature automatically registers the DNS records of VMs in the linked virtual networks, simplifying management.
- * DNS Settings: Using Azure-provided DNS ensures that the VMs can resolve each other's names without additional configuration.

By following these steps, you ensure that virtual machines on VNET1 and VNET2 are included automatically in the DNS zone contoso.azure and can resolve each other's names seamlessly.

NEW QUESTION: 61

□□□□□ □□□□□ 50□ □□□□. □ □□□□□□ Windows Server□ □□□□ □□□ □□□□.

VNet1□□□□ □□ □□□□□ □□□ Azure □□□□ □□□□. VNet1□□ DB1□□□□ □□□□□□ □□□ □□□□.

□-□□□□ □□□ □□□□□ Azure □□□□ □□□□ □□□□ DB1□ □□□□ App1□□□□ □□ □□□ □□□□□.

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

□□: □□ □□□ 1□□□□□.

Answer Area

Microsoft

For inbound connections to the subscription:

- Azure Application Gateway
- An Azure external load balancer
- Azure NAT Gateway
- Azure VPN Gateway

For connections between the on-premises servers and VNet1:

- Point-to-site (P2S) VPN
- Point-to-site (P2S) VPN
- Site-to-Site (S2S) VPN

Answer:

Answer Area

Microsoft

For inbound connections to the subscription:

- Azure Application Gateway
- An Azure external load balancer
- Azure NAT Gateway
- Azure VPN Gateway

For connections between the on-premises servers and VNet1:

- Point-to-site (P2S) VPN
- Point-to-site (P2S) VPN
- Site-to-Site (S2S) VPN

Explanation:

Answer Area

Microsoft

For inbound connections to the subscription: Azure VPN Gateway

For connections between the on-premises servers and VNet1: Point-to-site (P2S) VPN

AZ-700-KR 📄📄📄📄📄📄 DumpTop 📄📄📄📄 AZ-700-KR 📄! DumpTop 📄📄 **AZ-700-KR** 📄📄📄📄📄, DumpTop AZ-700-KR 📄📄📄📄📄
📄📄📄📄📄📄. 📄📄📄📄📄📄 DumpTop AZ-700-KR 📄📄📄📄📄. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (**330** Q&As Dumps, **30%OFF**
Special Discount: KrDump)

NEW QUESTION: 62

VNet1□□□ □□ □□□□□ □□□ Azure □□□ □□□□. VNet1□□ Pool1□□□ Azure Virtual Desktop □□□ □□ □□□□ □□□□. Pool1□□ □□□ □□ □□□□ □□ Azure Firewall□ TLS □□□ □□□□ □□□.

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

□□: □□ □□□ 1□□□□□.

- A.** Azure □ □□□
B. □□ □□□□□
C. Azure NAT □□□□□
D. □□□□ ID
E. Azure □□ DNS □□
F. Microsoft Enter □□□□□□ □

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 63

□□□ □□□ Azure □□ □□□□ VPN □□□ □□ BGP□ □□□□□ □□□.

□□ □ □□ Azure □□□□ □□□□ □□□? □□□ □□□□ □□□ □□□□□. (□ □□ □□) □□: □□ □□□ 1□□□□.

- A.** □□ □□□□ □□□□□
- B.** Azure □□□□□□ □□□□□□
- C.** Azure □□□
- D.** □□ □□□□ □□□□□□
- E.** Azure □□

Answer: A,D (LEAVE A REPLY)

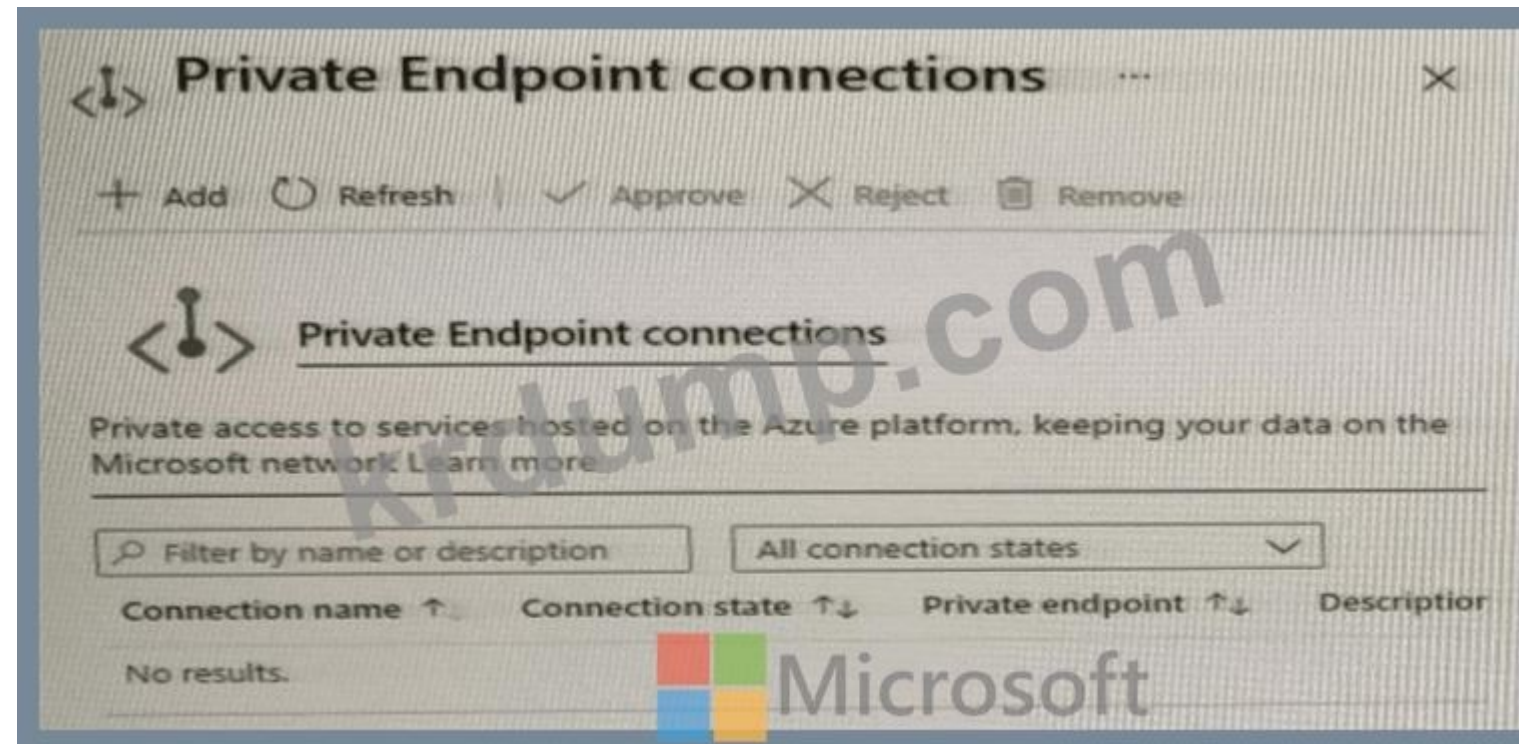
Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/bgp-howto>

NEW QUESTION: 64

App Service ☐☐☐ ☐☐☐ Azure App Service ☐☐ ☐☐☐☐.

as12 is a private IP address in Subnet2.



Subnet2 can contain only App Service apps in the ASP1 App Service plan.
As12 will use an IP address from Subnet2 for network communications.
Computers in Vnet1 will connect to a private IP address when they connect to as12.

Answer Area

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

Answer:

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

Explanation:

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

Reference:

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

NEW QUESTION: 65

contoso.onmicrosoft.com is an Azure Active Directory (Azure AD) tenant. The tenant contains the following resources:

- App1 is an Azure App Service
- contoso.com is an Azure DNS zone
- private.contoso.com is an Azure Private DNS zone
- Vnet1 is a virtual network

App1 is configured to use the private.contoso.com DNS zone for DNS resolution.

Azure DNS is configured to use the private.contoso.com DNS zone for DNS resolution.

What is the correct DNS configuration for App1?

- A. app1.private.contoso.com
- B. app1.contoso.com
- C. app1.privatelink.azurewebsites.net
- D. app1.contoso.onmicrosoft.com

Answer: C (LEAVE A REPLY)

NEW QUESTION: 66

Scenario: A company has a virtual network (Vnet1) that contains a subnet (Subnet1). The company wants to connect Subnet1 to a remote network (Vnet2) using a VPN connection. The company has a P2S (Point-to-Site) IKEv2 VPN connection that is configured to connect to Vnet1. The company also has a Client1 that is running Windows 10 and is configured to connect to Vnet1. The company wants to ensure that Client1 can connect to Vnet2 through the VPN connection.

What should the company do to ensure that Client1 can connect to Vnet2 through the VPN connection?

Vnet1 and Vnet2 are in the same Azure region and subscription.

P2S (Point-to-Site) IKEv2 VPN is configured to connect to Vnet1. Client1 is running Windows 10 and is configured to connect to Vnet1.

Vnet1 and Vnet2 are in the same Azure region and subscription. Vnet1 is connected to Vnet2 through a VPN connection.

Vnet2 is configured to use the private IP address space.

Client1 is configured to connect to Vnet2 through the VPN connection.

Client1 is configured to connect to Vnet2 through the VPN connection.

What should the company do to ensure that Client1 can connect to Vnet2 through the VPN connection?

What should the company do to ensure that Client1 can connect to Vnet2 through the VPN connection?

- A. Add a route to Vnet2 from Vnet1.
- B. Add a route to Vnet2 from Client1.

Answer: B (LEAVE A REPLY)

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

Reference:

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

NEW QUESTION: 67

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

Blob □□□□ □□□□ storageaccount1□□□ Azure Storage □□□ □□□□.

BLOB □□□□ □□ □□□□ □□□□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

* □□ □□□□□ □□□□ □□ □□□□□□ □□ storageaccount1□ □□□□ □ □□□ □□□□□.

* storageaccount1□ □□ □□□□ □□□□ □□□ □□□□□.

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

Actions

Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16

Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine

Configure a private endpoint on storageaccount1 and disable public access to the account

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

Deploy a virtual machine to a subnet in Vnet1

Answer Area



Microsoft

Answer:

ACTIONS

Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16

Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine

Configure a private endpoint on storageaccount1 and disable public access to the account

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

Deploy a virtual machine to a subnet in Vnet1

Answer Area

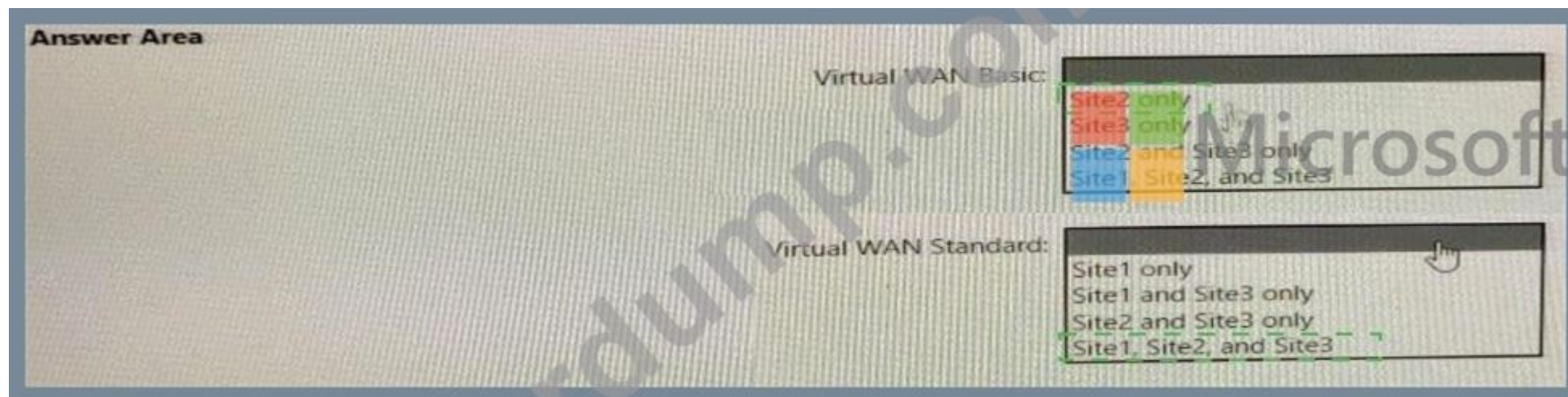
Configure a private endpoint on storageaccount1 and disable public access to the account

Deploy a virtual machine to a subnet in Vnet1

Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16

Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine

Explanation:



Explanation:

Virtual WAN Basic:

	▼
Site2 only	
Site3 only	
Site2 and Site3 only	
Site1, Site2, and Site3	



Virtual WAN Standard:

	▼
Site1 only	
Site1 and Site3 only	
Site2 and Site3 only	
Site1, Site2, and Site3	

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

NEW QUESTION: 69

Contoso Ltd. has an Active Directory (AD DS) domain named contoso.com.

The domain is configured with a single domain controller (CA) named dc1.com.

Azure AppGw1 is deployed to the Azure cloud.

AppGw1 is configured with the following settings:

* HTTP 1.1 protocol.

* SSL offload is enabled.

contoso.com. AppGwy1. .

?

Actions	Answer Area
From AppGwy1, create a routing rule.	
From AppGwy1, create a frontend IP configuration.	
From AppGwy1, create an SSL profile.	
From an on-premises computer, upload a certificate to AppGwy1.	
From AppGwy1, add an HTTP listener and associate the listener to the SSL profile.	

Answer:

Actions	Answer Area
From AppGwy1, create a routing rule.	From AppGwy1, create a frontend IP configuration.
From AppGwy1, create a frontend IP configuration.	From AppGwy1, create an SSL profile.
From AppGwy1, create an SSL profile.	From an on-premises computer, upload a certificate to AppGwy1.
From an on-premises computer, upload a certificate to AppGwy1.	From AppGwy1, add an HTTP listener and associate the listener to the SSL profile.
From AppGwy1, add an HTTP listener and associate the listener to the SSL profile.	

Explanation:

Actions	Answer Area
From AppGwy1, create a routing rule.	1 From AppGwy1, create a frontend IP configuration.
	2 From AppGwy1, create an SSL profile.
	3 From an on-premises computer, upload a certificate to AppGwy1.
	4 From AppGwy1, add an HTTP listener and associate the listener to the SSL profile.

NEW QUESTION: 70

5

VNET1.

Answer:

See the Explanation below for step by step instructions.

Explanation:

To archive all the metrics of VNET1 to an existing storage account, you can use Azure Monitor's diagnostic settings. Here's how you can do it:

Step-by-Step Solution

Step 1: Navigate to VNET1 in the Azure Portal

* Open the Azure Portal .

* Search for "Virtual networks" and select VNET1 from the list.

Step 2: Configure Diagnostic Settings

* In the VNET1 blade , select "Diagnostic settings" under the "Monitoring" section.

* Click on "Add diagnostic setting" .

Step 3: Set Up the Diagnostic Setting

* Enter a name for the diagnostic setting (e.g., VNET1-Metrics-Archive).

* Select the metrics you want to archive. You can choose from various metrics like TotalBytesReceived, TotalBytesSent, etc.

* Under "Destination details" , select "Archive to a storage account" .

* Choose the existing storage account where you want to archive the metrics.

* Configure the retention period if needed.

Step 4: Save the Configuration

* Review your settings to ensure everything is correct.

* Click on "Save" to apply the diagnostic setting.

Explanation:

* Diagnostic Settings : These allow you to collect and route metrics and logs from your Azure resources to various destinations, including storage accounts, Log Analytics workspaces, and Event Hubs.

* Metrics : Metrics provide numerical data about the performance and health of your resources.

Archiving these metrics helps in long-term analysis and compliance.

* Storage Account : Using an existing storage account ensures that the metrics are stored securely and can be accessed for future analysis.

By following these steps, you can ensure that all the metrics of VNET1 are archived to your existing storage account, enabling you to monitor and analyze the performance and health of your virtual network over time.

NEW QUESTION: 71

□□ □□□ Azure □□ □□□□□ □□ □□□□.

Name	Resource group	Location
Vnet1	RG1	East US
Vnet2	RG1	UK West
Vnet3	RG1	East US
Vnet4	RG1	UK West

□□ □□□ Azure □□□□ □□ □□□□.

Name	Type	Virtual network	Resource group	Location
VM1	Virtual machine	Vnet1	RG1	East US
VM2	Virtual machine	Vnet2	RG2	UK West
VM3	Virtual machine	Vnet3	RG3	East US
App1	App Service	Vnet1	RG4	East US
st1	Storage account	Not applicable	RG5	UK West

Azure Network Watcher□ □□ □□□□ □□□□ □□□ □ □□ □□□ □□□□ □□□.

□□□ □ □□ □□ □□□□ □□□□ □□□?

A. 4


```
{
  "timestamp": "2021-06-02T18:13:45+00:00",
  "resourceId": "/SUBSCRIPTIONS/6efbb4a5-d91a-4e4a-b6bf-5bdd6efea73c/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_HEADERS:User-Agent\\\\\\\"' required. ",
      "data": "",
      "file": "rules\\REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "appl.contoso.com",
    "transactionId": "d654811d0hgq3ea198165bq7428d74h6",
    "policyId": "default",
    "policyScope": "Global",
    "policyScopeName": "Global"
  }
}
```

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

□□ □□: □□□ □□ □□□ □□ □□□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 74

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 is a global load balancer that routes traffic to the nearest Azure region.

* <https://contoso.azurefd.net/uk> URL routes traffic to App1uk in the UK West region.

* <https://contoso.azurefd.net/us> URL routes traffic to App1us in the East US region.

* <https://contoso.azurefd.net/images> URL routes traffic to the storage account that contains the images for the website.

Contoso wants to ensure that traffic to the website is routed to the nearest Azure region. The website should be able to serve content from the nearest storage account.

What should you configure in the Azure Front Door routing rules?

Answer: 1, 2, 3, 4.

Number

1 2

3 4

Answer Area

Backend pools:

Routing rules:

Microsoft

Answer:

Number

1 2

3 4

Answer Area

Backend pools: 1 2

Routing rules: 2

Microsoft

Explanation:



NEW QUESTION: 75

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

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

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

Hub1□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □□□.

□□ □□: Azure NAT Gateway□ □□□□□.

□□□ □□ □□□ □□□□□?

- A. □
- B. □□□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 76

Azure Front Door □□□□ □□□(AFD1)□ Azure WAF(□ □□□□□□ □□□) □□(WAF1)□ □□□ Azure □□□ □□□□. AFD1□ WAF1□ □□□□ □□□□.

AFD1□ □□□□ □□□ □□ □□ □□□ □□□□ □□□.

□□ □□: AFD1□ □□ □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

- A. □□□
- B. □

Answer: B ([LEAVE A REPLY](#))

AZ-700-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ AZ-700-KR □□! DumpTop □ □□ **AZ-700-KR** □□ □□□ □□□□□□, DumpTop AZ-700-KR □□ □□□ □□□□□□ □□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ □□□ □□□□□. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (330 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)

NEW QUESTION: 77

You have a virtual network named Vnet1 in an Azure subscription. The virtual network has the following configuration:

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

Azure FirewallSubnet is connected to the Internet.

Subnet2 is connected to the Internet.

Subnet2 is connected to the Internet.

https://*.contoso.com.

What should you do?

- A. Create a new virtual network.
- B. Create a new network security group (NSG) and attach it to Subnet2.
- C. Create a new virtual network and connect it to the Internet.
- D. Create a new virtual network and connect it to the Internet.

Answer: (SHOW ANSWER)

NEW QUESTION: 78

You have a virtual network named Vnet1 in an Azure subscription. The virtual network has the following configuration:

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 is connected to the Internet.

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

What should you do?

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 is connected to the Internet.

* 0.0.0.0/0

* 10.0.0.0/16

What should you do?

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

Answer:

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

NEW QUESTION: 79

Which of the following is a valid IP address for a virtual machine?

A. 10.0.0.1/24

B. 10.0.0.1

C. 10.0.0.1/24

D. 10.0.0.1/24

E. 10.0.0.1/24

F. 10.0.0.1/24

G. 10.0.0.1/24

H. 10.0.0.1/24

I. 10.0.0.1/24

J. 10.0.0.1/24

K. 10.0.0.1/24

ExpressRoute is a dedicated network connection between Microsoft Azure and on-premises networks. Which of the following is a valid IP address for a virtual machine?

* 10.0.0.1/24

* 10.0.0.1/24

* 10.0.0.1/24

Which of the following is a valid IP address for a virtual machine?

A. 10.0.0.1/24

B. 10.0.0.1/24

C. 10.0.0.1/24

D. 40.0.0.1/24

Answer: (SHOW ANSWER)

NEW QUESTION: 80

□□□□□ □□ □□□ □□□□ □□□.1. □□□□ PaaS □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□.

□□□□ □□□ □□□□ □□□□?

- A. □□□ □□□□□
- B. Azure □□
- C. □□ □□□□□
- D. Azure □□□ □□□

Answer: A ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

NEW QUESTION: 81

□□□□□ □□□□□ □□□□.

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

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

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

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

□□: □□ □□□ 1□□□□.

Answer Area

Microsoft

Connection to Vnet1:

Private peering

Microsoft peering

Private peering

Public peering

Virtual network peering

Microsoft

Connection to SQL1:

Microsoft peering

Microsoft peering

Private peering

Public peering

Virtual network peering

Answer:

Answer Area



Connection to Vnet1: Private peering

Connection to SQL1: Microsoft peering

Explanation:

Answer Area



Connection to Vnet1: Private peering

Connection to SQL1: Microsoft peering

NEW QUESTION: 82

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 Area



Statements	Yes	No
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

Microsoft

Statements

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.

Yes

No

☐

☐

☐

☒

☒

☒

Topic 2, Litware. Inc Case Study 1

Overview

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

Existing Environment:

Hybrid Environment

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

All the offices connect to a virtual network named Vnet1 by using a Site-to-Site VPN connection.

Azure Environment

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

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

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

Requirements:

Business Requirements

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

Virtual Networking Requirements

Litware identifies the following virtual networking requirements:

* Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

- * Ensure that the records in the cloud.litwareinc.com zone can be resolved from the on-premises locations.
- * Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.
- * Minimize the size of the subnets allocated to platform-managed services.
- * Allow traffic from VMSSet1 to VMSSet2 on the TCP port 443 only.

Hybrid Networking Requirements

Litware identifies the following hybrid networking requirements:

- * Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely.
- Connections must be authenticated by Azure AD.
- * Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.
 - * The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.
 - * Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements

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

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

NEW QUESTION: 83

_____ 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____.

Answer Area

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:

Answer Area

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.	☐	☒

Explanation:

Answer Area

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.	☐	☒

NEW QUESTION: 84

Which of the following statements are true? (Select all that apply.)

Azure Bastion can be used to connect to virtual machines in a virtual network.

Azure Bastion can be used to connect to virtual machines in a virtual network. It can also be used to connect to virtual machines in a virtual network. It can also be used to connect to virtual machines in a virtual network.

Answer: All of the above.

Answer Area

Microsoft

Subnet mask:

- /24
- /26
- /28
- /30

Name:

- AzureBastionSubnet
- Azure Bastion Subnet
- Bastion_Subnet
- BastionSubnet

Answer:
Answer Area

Subnet mask:

- /24
- /26
- /28
- /30

Name:

- AzureBastionSubnet
- Azure Bastion Subnet
- Bastion_Subnet
- BastionSubnet

Microsoft

Explanation:

Answer Area

Subnet mask: /26

Name: AzureBastionSubnet

Microsoft

NEW QUESTION: 85

□ □ 1

subnet1-2 IP 10.1.2.4 .

```
subnet1-1 192.168.10.0/24 IP 192.168.10.1 subnet2 192.168.10.2
```

Answer:

See the Explanation below for step by step instructions.

* To deploy a firewall to subnet1-2, you need to create a network virtual appliance (NVA) in the same virtual network as subnet1-2. An NVA is a virtual machine that performs network functions, such as firewall, routing, or load balancing 1 .

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

2.

* To assign the IP address of 10.1.2.4 to the NVA, you need to create a static private IP address for the network interface of the virtual machine. You can do this in the IP configurations settings of the network interface 3 .

* To ensure that traffic from subnet1-1 to the IP address range of 192.168.10.0/24 is routed through the NVA, you need to create a user-defined route (UDR) table and associate it with subnet1-1. A UDR table allows you to override the default routing behavior of Azure and specify custom routes for your subnets 4 .

* To create a UDR table, you need to go to the Route tables service in the Azure portal and select + Create. You can give a name and a resource group for the route table 5 .

* To create a custom route, you need to select Routes in the route table and select + Add. You can enter the following information for the route 5 :

* Destination: 192.168.10.0/24

* Next hop type: Virtual appliance

* Next hop address: 10.1.2.4

* To associate the route table with subnet1-1, you need to select Subnets in the route table and select + Associate. You can select the virtual network and subnet that you want to associate with the route table 5 .

NEW QUESTION: 86

□□ □□ □□□ □□□□ □□□ 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 .comoso.com ☐ URL ☐ ☐ ☐ ☐ App1 ☐ ☐ ☐ ☐ ☐.

FW1 IDPS HP1 Server1

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

□□: □□ □□□ 1□□□□.

A. FW1□ □□□ □□ □□□□□ □□□□□.

B. □□ □□□□ KV1□ □□□□□.

C. FW1□ □□ □□ □□□□□□ □□□□□□.

D. HP1□ □□□□□□ □□□ □□□□□.

E. FW1 ☐ ☐ TLS ☐ ☐ ☐ ☐ ☐ ☐.

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 87

□□ □□ □□ □□ □□□□ □□□□.

Name	Type	Description
Group1	Microsoft Entra group	None
Group2	Microsoft Entra group	None
VPNGW1	Azure VPN Gateway	Supports Point-to-Site (P2S) VPN connections
VPNGW2	Azure VPN Gateway	Supports Point-to-Site (P2S) VPN connections

Microsoft Entra □□ □□□□ Azure VPN □□□□□□□□ □□□□□□□□ □□□□□□.

P2S VPN □□□□ Microsoft Entra □□□□ □□□□□□ □□□□. □□□□ □□ □□ □□□□ □□□□ □□□□.

* Group1□ □□□ VPNGW1□ VPN □□□□ □□□□ □□□□ □□□□.

* Group2□ □□□ VPNGW2□ VPN □□□□ □□□□ □□□□ □□□□.

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

Actions

- From the Microsoft Entra admin center, register two apps named App1 and App2. Assign Group1 to App1 and assign Group2 to App2.
- From the Microsoft Entra admin center, add a scope to App1 and App2.
- From the Microsoft Entra admin center, add a client app to App1 and App2.
- From the Azure portal, configure the Point-to-site configuration settings for VPNGW1 and VPNGW2.

Answer Area

Answer:

Actions

- From the Microsoft Entra admin center, register two apps named App1 and App2. Assign Group1 to App1 and assign Group2 to App2.
- From the Microsoft Entra admin center, add a scope to App1 and App2.
- From the Microsoft Entra admin center, add a client app to App1 and App2.
- From the Azure portal, configure the Point-to-site configuration settings for VPNGW1 and VPNGW2.

Answer Area

- From the Microsoft Entra admin center, register two apps named App1 and App2. Assign Group1 to App1 and assign Group2 to App2.
- From the Microsoft Entra admin center, add a scope to App1 and App2.
- From the Microsoft Entra admin center, add a client app to App1 and App2.
- From the Azure portal, configure the Point-to-site configuration settings for VPNGW1 and VPNGW2.

Explanation:

- | | |
|---|--|
| 3 | From the Microsoft Entra admin center, create a service principal for the application and App2 |
| 4 | From the Azure portal, configure the settings for VPNGW1 and VNet1 |

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 90

OpenVPN is a third-party VPN solution. Which Active Directory authentication protocol is supported by OpenVPN?

- A. RADIUS
- B. RADIUS
- C. Azure AD
- D. Azure Active Directory(Azure AD)

Answer: B (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 91

Azure App Service is a cloud-based platform for building and hosting web applications. Which Azure service is used to connect App Service to a private network?

PLS1 is a private endpoint for a service. Which Azure service is used to connect PLS1 to a private network?

App1 is a private endpoint for a service. Which Azure service is used to connect App1 to a private network?

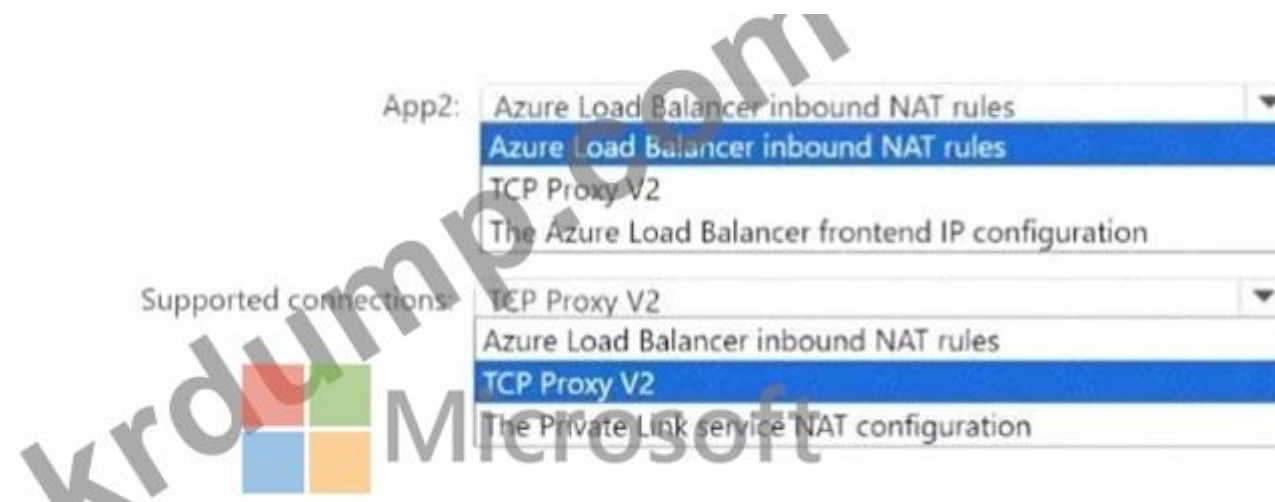
* App1 is a private endpoint for a service. Which Azure service is used to connect App1 to a private network?

* App1 is a private endpoint for a service. Which Azure service is used to connect App1 to a private network?

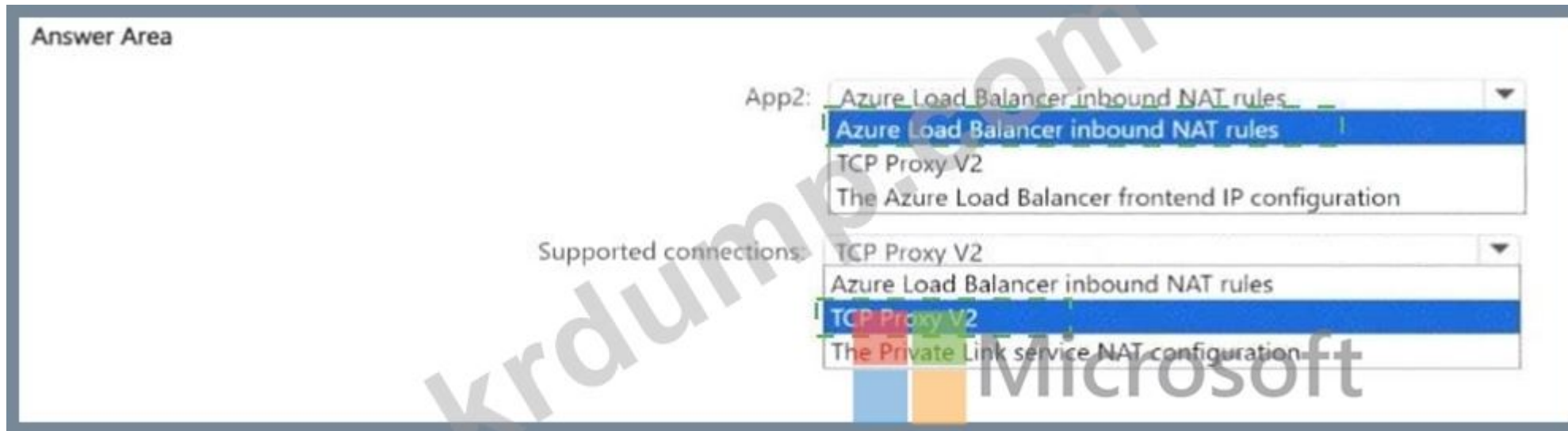
App2 is a private endpoint for a service. Which Azure service is used to connect App2 to a private network?

App2 is a private endpoint for a service. Which Azure service is used to connect App2 to a private network?

Answer Area



Answer:



Explanation:



AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-700-KR ☐☐! DumpTop ☐ ☐☐ **AZ-700-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐ ☐☐ ☐☐☐ ☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐ DumpTop AZ-700-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (330 Q&As Dumps, **30%OFF**

Special Discount: **KrDump**)

NEW QUESTION: 92

☐☐☐ ☐☐☐☐ 192.168.0.0/20☐ IP ☐☐ ☐☐☐ ☐☐☐☐ Vnet1☐☐☐ Azure ☐☐ ☐☐☐☐☐ ☐☐☐☐.
 Vnet1☐☐ 192.168.0.0/24☐ IP ☐☐ ☐☐☐ ☐☐☐☐ Subnet1☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.
 CIDR ☐☐☐ /48☐ ☐☐☐☐ Vnet1☐ ☐☐ IPv6 ☐☐ ☐☐☐ ☐☐☐☐☐.
 Subnet1☐ ☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐ IPv6 ☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐. ☐☐☐☐ ☐☐ IPv4 ☐☐☐ ☐☐ ☐☐☐☐☐☐ ☐☐☐.
 ☐☐☐☐ ☐☐ ☐☐☐? ☐☐☐☐☐☐ ☐☐ ☐☐☐☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐.
 ☐☐: ☐☐ ☐☐☐ 1☐☐☐☐☐.

Create an IPv6 subnet that uses a CIDR suffix of:

	▼
/20	
/24	
/48	
/64	

For each virtual machine, create an additional:

	▼
IP configuration	
NIC	
Public IPv6 address	

Answer:

Create an IPv6 subnet that uses a CIDR suffix of:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">/20</td></tr><tr><td colspan="2">/24</td></tr><tr><td colspan="2">/48</td></tr><tr><td colspan="2">/64</td></tr></table>		▼	/20		/24		/48		/64	
	▼										
/20											
/24											
/48											
/64											
For each virtual machine, create an additional:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td>IP configuration</td><td></td></tr><tr><td>NIC</td><td></td></tr><tr><td>Public IPv6 address</td><td></td></tr></table>		▼	IP configuration		NIC		Public IPv6 address			
	▼										
IP configuration											
NIC											
Public IPv6 address											

Explanation:

Create an IPv6 subnet that uses a CIDR suffix of:

	▼
/20	
/24	
/48	
/64	

For each virtual machine, create an additional:

	▼
IP configuration	
NIC	
Public IPv6 address	

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-overview>

<https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-add-to-existing-vnet-powershell>

1) Correct: /64

Explanation: 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.

Source: <https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview>

2) Correct: Public IPv6 Address

Explanation: Add IPv6 configuration to NIC. "Configure all of the VM NICs with an IPv6 address using Add-AzNetworkInterfaceIpConfig" Source: <https://docs.microsoft.com/en-us/azure/load-balancer/ipv6-add-to-existing-vnet-powershell>

NEW QUESTION: 93

VMSSet1[] VMSSet2[] [] [] [] [] . [] [] [] [] [] [] [] [] .
[] [] [] [] [] NSG [] [] NSG [] [] [] [] ? [] [] [] [] [] [] [] [] .
[] : [] [] [] 1[] [] [] .

Minimum number of custom NSG rules:

1
2
3
4
5

Minimum number of NSG assignments:

1
2
3
4
5

lte □□□ □□□ □□□□.

Answer:

Minimum number of custom NSG rules:

1
2
3
4
5

Minimum number of NSG assignments:

1
2
3
4
5

Explanation:

Minimum number of custom NSG rules:

1

2

3

4

5

Minimum number of NSG assignments:

1

2

3

4

5



Box 2: One NSG

The minimum requirement is one NSG. You could attach the NSG to VMSSet1 and restrict outbound traffic, or you could attach the NSG to VMSSet2 and restrict inbound traffic. Either way you would need two custom NSG rules.

Box 1: Two custom rules

With the NSG attached to VMSSet2, you would need to create a custom rule blocking all traffic from VMSSet1. Then you would need to create another custom rule with a higher priority than the first rule that allows traffic on port 443.

The default rules in the NSG will allow all other traffic to VMSSet2.

NEW QUESTION: 94

AGW1 is an Azure Application Gateway. Rule1 is a custom rule.

1. http://www.contoso.com is blocked. Pool1 is a VMSSet. Azure is a VMSSet.

VMSS2 is a VMSSet. Azure is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

AGW1 is a custom rule. http://www.adatum.com is a VMSSet. http://www.contoso.com is a VMSSet. Pool1 is a VMSSet.

Answer: A,D,E (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/configuration-overview>

NEW QUESTION: 95

□□□ □□□ □□□ 40□□ □□□ □□ □□□□. Azure □□□□ □□□ □□ □□ □□□□□ □□□□ □□□□.

* □□ □□ Azure □□□ □ □□□□

* □□□ Azure □□□ 3□ □□□□

Azure Virtual WAN□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

* □□□ □ □□□□ ExpressRoute □□□ □□ □□ □□□ □□□□ □□□ □ VPN□ □□□ □□□.

* □□□ □ □□□□ ExpressRoute □□□ □□□ □□□ □□□□ □□□ □ VPN□ □□□ □□□.

* □□ □□□ □□ □□ □□□□ □□ □□□ □□□ □□□□□ □□□.

* □□□ □□□□□ □□□.

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

Answer Area

Virtual WAN:

Virtual WAN hub:

Virtual network gateway:

Microsoft

Answer:

Answer Area

Virtual WAN:

Virtual WAN hub:

Virtual network gateway:

Microsoft

Explanation:



NEW QUESTION: 96

□□□□2□ □□ □□□□ □□□□ □□□. □□□□ PaaS □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□. □□ □□ □□□ □□□□ □□□?

- A. □□ □□□□□
- B. Azure □□□
- C. □□□ □□□□□
- D. Azure □□

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 97

□□ □□□□ □□□ Azure □□□ □□□□.

* Vnet1□□□□ □□ □□□□

* subnet1 □ AzureFirewallSubnet□□□ □ □□ □□□

* FW1□□□ □□□ □□ Azure □□□

* Subnet1□ □□□ RT1□□□□ □□ □□□

* RT1□ FW1□ 0.0.0.0/0□ □□ □□□

Windows Server□ □□□□ 10□□ □□□ Subnet1□ □□□ □, □□ □□□ □□□ □□□□□ □□ □□ □□□□□□.

□□ □□□ □□□□ □ □□□ □□□□ □□□.

□□□ □□ □□□?

- A. □□□□□□ □□ □□□ □□□ □□□□ 1688□□ □□□□□ □□□□ □□□□□.
- B. □□□□□ NAT □□□ □□ Azure Standard Load Balancer□ □□□□□.
- C. fW1□□ □□ 1688□ □□ DNAT □□□ □□□□□.
- D. Azure Key Management Service(KMS)□ □□ RI1□ □□□ □□□ □□□□□.

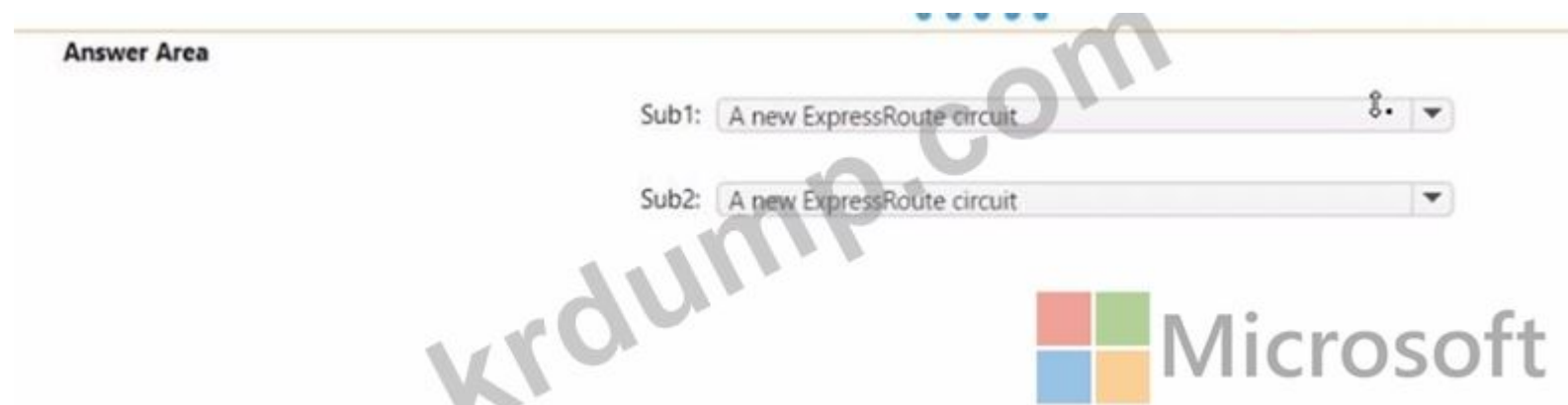
Answer: D ([LEAVE A REPLY](#))

Reference:

<https://ryanmangansitblog.com/2020/05/11/firewall-considerations-windows-virtual-desktop-wvd/>

NEW QUESTION: 98

□□ □□□ Azure □□□□ □□ □□□□.



NEW QUESTION: 99

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

Name	IP address	Hosted application protocol
VM1	10.1.1.11	HTTPS (TCP port 443)
VM2	10.1.1.21	SMTP (TCP port 25)
VM3	10.1.1.31	SFTP (TCP port 22)

□□ □□ □□□ VNet1□ □□□□□.

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

- A. □□ □□ □□□
- B. Azure □□□□□□ □□□□□
- C. NAT □□□□□
- D. □□ □□ □□□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 100

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

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

Policy1□□ □□□ □□ □□□ □□□□.

- * □□□: Microsoft.Storage
- * □□□ □□□: storage1
- Subnet1□ □□□ □□□ □□□□.
- * □□: □□□1
- * □□□ □□ □□: 10.0.0.0/24
- * NAT □□□□□: □□
- * □□□□ □□ □□: □□
- * □□□ □□□: □□

* 0000 000000
 o 000: 00 000
 * 000 00
 o 0000 000 00: 00
 00 0 000 00, 000 0000 '0'0 0000, 000 000 '0000'0 000000.
 00: 00 000 10000.

Answer Area

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

Answer:

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

Explanation:

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

NEW QUESTION: 101

VNet1000 00 000000 0000 Azure 0000 00000.
 000000 000000 0000 0(S2S) VPN 0000 00000 VNet10 000000.

VPN 1000 1000 1000 Azure Network Watcher 1000 1000 1000 1000.

1000 1000 1000 1000 Network Watcher 1000 1000 1000, 1000 1000 1000 1000 1000 1000? 1000 1000 1000 1000 1000 1000.

1000: 1000 1000 1000.

Answer Area

Microsoft

Feature:

- Connection monitor
- Connection troubleshoot
- VPN troubleshoot
- IP flow verify

Data source:

- Azure Monitor Agent
- Network Watcher Agent
- Virtual network flow logs

Answer:

1000 1000

Microsoft

Feature:

- Connection monitor
- Connection troubleshoot
- VPN troubleshoot
- IP flow verify

Data source:

- Azure Monitor Agent
- Network Watcher Agent
- Virtual network flow logs

Explanation:

Answer Area

Feature: VPN troubleshoot

Data source: Network Watcher Agent

 Microsoft

NEW QUESTION: 102

Vnet1□□□ □□□□ □□□□□ □□□ Azure □□□ □□ SQL1□□□ Azure SQL □□□□□□□ □□ □□□□□□ Vnet1□ □□□□.

fabrikam□□□ □□□ □□□ □□, Vnet1□□□ □□ □□□□□ VM1□□□ □□ □□□ □□□ Azure □□□ □□□□. VM1□ Vnet2□ □□□□ □□□□. Azure □□ □□ □□□□ □□□□ VM1 □ SQL 1□ □□ □□□ □□□ □□□□ □□□.

[illegible]

Resources

A NAT gateway

A peering link

A private endpoint

A service endpoint

An Azure application gateway

An Azure load balancer

Answer Area

Vnet1:

Vnet2:

Answer:

Resources

A NAT gateway

A peering link

A private endpoint

A service endpoint

An Azure application gateway

An Azure load balancer

Answer Area

Vnet1:

A private endpoint

Vnet2:

A peering link

Explanation:

Resources

A NAT gateway

A peering link

A private endpoint

A service endpoint

An Azure application gateway

An Azure load balancer

Answer Area

Vnet1:

Vnet2:

NEW QUESTION: 103

You have two virtual machines, VM1 and VM2, in a virtual network. VM1 has a network interface card (NIC) connected to a virtual switch (vSwitch) that is connected to a virtual network (VNet). VM2 has a NIC connected to a vSwitch that is connected to a different VNet. You want to establish a Remote Desktop session from VM1 to VM2.

Answer Area

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

Answer:

Answer Area

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

Explanation:

No

subnet1(WM1->NSG1 outbound->NSG10 outbound)->subnet2(NSG1 inbound->NSG11 inbound->VM2) Yes NSG10 blocks ICMP from VNet4 (source 10.10.0.0/16) but it is not blocked from VM2's subnet (VNet1 /Subnet2).

No

NSG11 blocks RDP (port TCP 3389) destined for "VirtualNetwork". VirtualNetwork is a service tag and means the address space of the virtual network (VNet1) which in this case is 10.1.0.0/16. Therefore, RDP traffic from subnet2 to anywhere else in VNet1 is blocked.

NEW QUESTION: 104

Four Azure VPN gateways, GW1, are connected to four local routers, RTR1, RTR2, RTR3, and RTR4, via four connections, Connection1, Connection2, Connection3, and Connection4. The connections are shown in the table below.

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

Branch1 is connected to GW1 via Connection1. Branch2 is connected to GW1 via Connection2. Branch3 is connected to GW1 via Connection3. Branch4 is connected to GW1 via Connection4. Branch1 is connected to GW1 via Connection1. Branch2 is connected to GW1 via Connection2. Branch3 is connected to GW1 via Connection3. Branch4 is connected to GW1 via Connection4.

* Branch1 is connected to GW1 via Connection1.

* Branch2 is connected to GW1 via Connection2.

Branch1 is connected to GW1 via Connection1.

A. Branch1 is connected to GW1 via Connection1.

B. Branch2 is connected to GW1 via Connection2.

C. Branch3 is connected to GW1 via Connection3.

D. Branch4 is connected to GW1 via Connection4.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 105

Four Azure Virtual Networks, VNet1, VNet2, VNet3, and VNet4, are shown in the table below.

Name	Type	Description
Vnet1	Virtual network	None
Subnet1	subnet	Hosted in Vnet1
Subnet2	subnet	Hosted in Vnet1
GatewaySubnet	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

Gateway 1 is connected to VNet1 via Connection1. Gateway 2 is connected to VNet2 via Connection2. Gateway 3 is connected to VNet3 via Connection3. Gateway 4 is connected to VNet4 via Connection4.

* VM1 is connected to VNet1 via Connection1.

* VM2 can ping IP address 10.0.0.100 successfully.

* Can ping 10.0.0.100 from VM1.

Gateway1 is Vnet1's default gateway.

Vnet1 can ping 10.0.0.100 successfully?

A. 5

B. 2

C. 3

D. 4

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 106

7

VNET2 can connect VNET1 and VNET3 without using gateways or the internet. VNET1 and VNET3 cannot connect VNET2 without using gateways or the internet.

Answer:

See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that hosts on VNET2 can access hosts on both VNET1 and VNET3, but hosts on VNET1 and VNET3 cannot communicate through VNET2:

* To connect different virtual networks in Azure, you need to use virtual network peering. Virtual network peering allows you to create low-latency, high-bandwidth connections between virtual networks without using gateways or the internet 1 .

* To create a virtual network peering, you need to go to the Azure portal and select your virtual network. Then select Peerings under Settings and select + Add 2 .

* On the Add peering page, enter or select the following information:

* Name: Type a unique name for the peering from the source virtual network to the destination virtual network.

* Virtual network deployment model: Select Resource manager.

* Subscription: Select the subscription that contains the destination virtual network.

* Virtual network: Select the destination virtual network from the list or enter its resource ID.

* Name of the peering from [destination virtual network] to [source virtual network] : Type a unique name for the peering from the destination virtual network to the source virtual network.

* Configure virtual network access settings: Select Enabled to allow resources in both virtual networks to communicate with each other.

* Allow forwarded traffic: Select Disabled to prevent traffic that originates from outside either of the peered virtual networks from being forwarded through either of them.

* Allow gateway transit: Select Disabled to prevent either of the peered virtual networks from using a gateway in the other virtual network.

* Use remote gateways: Select Disabled to prevent either of the peered virtual networks from using a gateway in the other virtual network as a transit point to another network.

* Select Add to create the peering 2 .

* Repeat the previous steps to create peerings between VNET2 and VNET1, and between VNET2 and VNET3. This will allow hosts on VNET2 to access hosts on both VNET1 and VNET3.

* To prevent hosts on VNET1 and VNET3 from communicating through VNET2, you need to use network security groups (NSGs) to filter traffic between subnets. NSGs are rules that allow or deny inbound or outbound traffic based on source or destination IP address, port, or protocol 3 .

* To create an NSG, you need to go to the Azure portal and select Create a resource. Search for network security group and select Network security group. Then select Create 4 .

* On the Create a network security group page, enter or select the following information:

* Subscription: Select your subscription name.

* Resource group: Select your resource group name.

* Name: Type a unique name for your NSG.

* Region: Select the same region as your virtual networks.

* Select Review + create and then select Create to create your NSG 4 .

* To add rules to your NSG, you need to go to the Network security groups service in the Azure portal and select your NSG. Then select Inbound security rules or Outbound security rules under Settings and select + Add .

* On the Add inbound security rule page or Add outbound security rule page, enter or select the following information:

* Source or Destination: Select CIDR block.

* Source CIDR blocks or Destination CIDR blocks: Enter the IP address range of the source or destination subnet that you want to filter. For example, 10.0.1.0/24 for VNET1 subnet 1, 10.0.2.0/24 for VNET2 subnet 1, and 10.0.3.0/24 for VNET3 subnet 1.

* Protocol: Select Any to apply the rule to any protocol.

* Action: Select Deny to block traffic from or to the source or destination subnet.

* Priority: Enter a number between 100 and 4096 that indicates the order of evaluation for this rule.

Lower numbers have higher priority than higher numbers.

* Na me: Type a unique name for your rule.

* Select Add to create your rule 4 .

* Repeat the previous steps to create inbound and outbound rules for your NSG that deny traffic between VNET1 and VNET3 subnets. For example, you can create an inbound rule that denies traffic from

10.0.1.0/24 (VNET1 subnet 1) to 10.0.3.0/24 (VNET3 subnet 1), and an outbound rule that denies traffic from 10.0.3.0/24 (VNET3 subnet 1) to 10.0.1.0/24 (VNET1 subnet 1).

* To associate your NSG with a subnet, you need to go to the Virtual networks service in the Azure portal and select your virtual network. Then select Subnets under Settings and select the subnet that you want to associate with your NSG 5 .

* On the Edit subnet page, under Network security group, select your NSG from the drop-down list. Then select Save 5 .

* Repeat the previous steps to associate your NSG with the subnets in VNET1 and VNET3 that you want to isolate from each other.

AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-700-KR ☐☐! DumpTop ☐ ☐☐ **AZ-700-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐
☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop AZ-700-KR ☐☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (**330 Q&As Dumps**, **30%OFF**)

Special Discount: KrDump)

NEW QUESTION: 107

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

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

□□ Front Door SKU□ □□□□ □□□, □□□ □□□□ □□ □□□□ □□□□□ □ □□□ □□□□ □□□ □□□□ □□□. □□□□ □□□ □□□□□ □□□.

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

□□: □□ □□□ 1□□□□.

Answer Area

SKU: Premium
Classic
Premium
Standard

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

Microsoft

Answer:

Answer Area

SKU: Premium
Classic
Premium
Standard

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

Microsoft

Explanation:

Answer Area

SKU: Premium

Use: Azure Private Link

Microsoft

NEW QUESTION: 108

□□ □□□□□ Azure □□□□ □ □ □□□□.



Firewall1

Firewall

 Delete  Lock

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

^ Essentials

Resource group (change)
RG1

Location
North Europe

Subscription (change)
Subscription1

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

Virtual network
Vnet1

Firewall policy
FirewallPolicy1

Provisioning state
Succeeded

Tags (change)
Click here to add tags

Firewall sku
Standard

Firewall subnet
AzureFirewallSubnet

Firewall public IP
Firewall-IP1

Firewall private IP
10.100.253.4

Management subnet

Management public IP

Private IP Ranges
Managed by Firewall Policy

 Microsoft

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

□□: □□ □□□ 1□□□□.

On Firewall1, forced tunneling [answer choice]

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



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

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

Answer:

	On Firewall1, forced tunneling [answer choice]	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">is enabled already</td></tr><tr><td colspan="2">cannot be enabled</td></tr><tr><td colspan="2">is disabled but can be enabled</td></tr></table>		▼	is enabled already		cannot be enabled		is disabled but can be enabled	
	▼									
is enabled already										
cannot be enabled										
is disabled but can be enabled										
On Firewall1, management by Azure Firewall Manager [answer choice]		<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">is enabled already</td></tr><tr><td colspan="2">cannot be enabled</td></tr><tr><td colspan="2">is disabled but can be enabled</td></tr></table>		▼	is enabled already		cannot be enabled		is disabled but can be enabled	
	▼									
is enabled already										
cannot be enabled										
is disabled but can be enabled										

Explanation:

On Firewall1, forced tunneling [answer choice]

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

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



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

Box 1:

If forced tunneling was enabled, the Firewall Subnet would be named AzureFirewallManagementSubnet.

Forced tunneling can only be enabled during the creation of the firewall. It cannot be enabled after the firewall has been deployed.

Box 2:

The "Visit Azure Firewall Manager to configure and manage this firewall" link in the exhibit shows that the firewall is managed by Azure Firewall Manager.

NEW QUESTION: 109

3 Azure Virtual Networks (Vnet1, Vnet2, and Vnet3) are connected to a single Azure Firewall instance.

Vnet1 has 12 subnets, Vnet2 has 4 subnets, and Vnet3 has 4 subnets. Vnet1 has App1 and App2. Vnet2 has App3 and App4. Vnet3 has App5 and App6.

Azure Virtual Network NAT is configured for App1 and App2. App3 and App4 are connected to the Internet via the Internet Gateway.

App5 and App6 are connected to the Internet via the Internet Gateway. App5 and App6 are also connected to the Internet via the Internet Gateway.

* App1 and App2 are connected to the Internet via the Internet Gateway.

* App3 and App4 are connected to the Internet via the Internet Gateway.

App5 and App6 are connected to the Internet via the Internet Gateway.

App7: App8 and App9.

Answer Area



Minimum number of subnets:

1
2
6
12

Minimum number of Virtual Network NAT instances:

1
2
6
12

Answer:

Answer Area

Minimum number of subnets:

Minimum number of Virtual Network NAT instances:

Microsoft

Explanation:

Minimum number of subnets:

Minimum number of Virtual Network NAT instances:

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview>

NEW QUESTION: 110

WebApp1 is an Azure App Service application. FDProfile1 is an Azure Front Door profile. FDProfile1 routes traffic to WebApp1.

<https://www.contoso.com/users/1234567890> WebApp1 returns 404.

FDProfile1 is configured with the following settings:

- A. ☐ ☐ ☐ ☐
- B. ☐ ☐
- C. ☐ ☐
- D. ☐ ☐ ☐

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 111

Sub1 and Sub2 are Azure virtual networks. Sub1 contains VM1. Sub2 contains VM2.

Azure Private Link is configured between Sub2 and VM1.

VM1 is configured with the following settings:

Sub1 is configured with the following settings:

- A. Azure DNS
- B. Azure Private Link

- C. ☐ ☐ ☐ ☐ ☐ ☐
- D. ☐ ☐ ☐ ☐ ☐ ☐

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 112

☐ ☐ ☐ 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. Endpoint3 ☐
- B. Endpoint2 ☐ Endpoint3 ☐
- C. Endpoint1 ☐
- D. Endpoint1, Endpoint2, Endpoint3 ☐ Endpoint4
- E. Endpoint1 ☐ Endpoint4 ☐

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 113

☐ ☐ ☐ ☐ VPN ☐ ☐ ☐ ☐.

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ Azure ☐ ☐ ☐.

☐ ☐ ☐ ☐ ☐ ☐ ☐ VPN ☐ ☐ ☐ ☐.

PowerShell ☐ ☐ ☐ ☐ ☐? ☐ ☐ ☐ ☐ ☐ ☐.

☐: ☐ ☐ 1 ☐ ☐.

- B. 100000 000 00
- C. 00 00 000 0000 000 00 00
- D. 0000 00 00

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 115

Azure 000 0000.

Azure Firewall Premium 0 0000, 00 Premium 000 000000, 0000 0 0000000 000 00 000 000000.
0000 00 000 000 00 000000?

- A. 000
- B. 00 000000
- C. 0000
- D. 00 0000

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 116

VM1 0 VM4 0 00 00 0000 ping 0 000000 000 0 00000? 000000 00 00000 000 000 000000.
00: 00 000 100000.

VM1:

	▼
VM2 only	
VM2 and VM4 only	
VM2, VM3, and VM4 only	
VM2, VM3, VM4, and VM5	

VM4:

	▼
VM3 only	
VM1 and VM3 only	
VM1, VM2, and VM3 only	
VM1, VM2, VM3, and VM5	

Answer:

VM1:

▼
VM2 only
VM2 and VM4 only
VM2, VM3, and VM4 only
VM2, VM3, VM4, and VM5

Microsoft

VM4:

▼
VM3 only
VM1 and VM3 only
VM1, VM2, and VM3 only
VM1, VM2, VM3, and VM5

Explanation:

VM1:

▼
VM2 only
VM2 and VM4 only
VM2, VM3, and VM4 only
VM2, VM3, VM4, and VM5

Microsoft

VM4:

▼
VM3 only
VM1 and VM3 only
VM1, VM2, and VM3 only
VM1, VM2, VM3, and VM5

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: 117

GW1 is an Azure VPN gateway. GW1 is a P2S VPN gateway.

GW1 is configured for SSTP and OpenVPN (SSL) tunnel types.

P2S VPN is configured for Microsoft Entra authentication.

What is the correct configuration for the point-to-site configuration of GW1?

Options: A. Microsoft Entra authentication and OpenVPN (SSL) tunnel type. B. Microsoft Entra authentication and SSTP tunnel type. C. Microsoft Entra authentication and IKEv2 and SSTP tunnel type. D. Microsoft Entra authentication and OpenVPN (SSL) tunnel type.

Correct Answer: C

Answer Area

- Register the Microsoft.HybridNetwork resource provider.
- For the point-to-site configuration of GW1, set Authentication type to **Microsoft Entra** and set Tunnel type to **OpenVPN (SSL)**.
- Grant the Azure VPN application admin consent to the Microsoft Entra tenant.
- For the point-to-site configuration of GW1, set Authentication type to **Microsoft Entra** and set Tunnel type to **IKEv2 and SSTP (SSL)**.
- Download the Azure VPN Client profile configuration package and distribute the package to the users.



Answer:

Actions

- Register the Microsoft.HybridNetwork resource provider.
- For the point-to-site configuration of GW1, set Authentication type to **Microsoft Entra** and set Tunnel type to **OpenVPN (SSL)**.
- Grant the Azure VPN application admin consent to the Microsoft Entra tenant.
- For the point-to-site configuration of GW1, set Authentication type to **Microsoft Entra** and set Tunnel type to **IKEv2 and SSTP (SSL)**.
- Download the Azure VPN Client profile configuration package and distribute the package to the users.

Answer Area

- Grant the Azure VPN application admin consent to the Microsoft Entra tenant.
- For the point-to-site configuration of GW1, set Authentication type to **Microsoft Entra** and set Tunnel type to **IKEv2 and SSTP (SSL)**.
- Download the Azure VPN Client profile configuration package and distribute the package to the users.

Explanation:

Actions	Answer Area
⋮ Register the Microsoft.HybridNetwork resource provider. ⋮ For the point-to-site configuration of GW1, set Authentication type to Microsoft Entra and set Tunnel type to OpenVPN (SSL).	1 ⋮ Grant the Azure VPN application admin consent to the Microsoft Entra tenant. 2 ⋮ For the point-to-site configuration of GW1, set Authentication type to Microsoft Entra and set Tunnel type to IKEv2 and SSTP (SSL). 3 ⋮ Download the Azure VPN Client profile configuration package and distribute the package to the users.

NEW QUESTION: 118

Azure ☐☐ ☐☐☐☐☐ ☐☐☐ ☐☐☐☐.

□ □ □ □ □ □ □ □ □ □ □ .

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

□□: □□ 1□□ 1□□□□.

- A.** VPN □□□□□
- B.** Azure □□
- C.** Azure Active Directory □□□ □□□(Azure AD DS)
- D.** Azure □□□□□□ □□□□□ v2
- E.** Azure □□ □□

Answer: A,B,D (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 119

□□ □□□ □□□□□ □□□□□ □□ □□□□.

Name	ASN	IP address space	Connection type	Description
Branch1	64551	10.50.0.0/24,10.61.0.0/16	VPN	Is an on-premises datacenter
Branch2	64551	10.50.0.0/16,10.61.0.0/16	VPN and ExpressRoute	AS Path has a prefix of 64551,64551,64551
Branch3	64551	10.50.20.0/24,10.61.0.0/16	ExpressRoute	None

VWAN1 Azure WAN VNet1 Azure . VWAN1 VNet1 . VWAN1

```

□ □□□ □□ □□□ AS Path□□□.

```

VNet1 10.61.1.5 10.61.1.5 10.61.1.5 10.61.1.5

□□ □□□ □□□ □□□?

- A.** Branch1 ☐ ☐ ☐ VPN ☐ ☐
- B.** Branch3 ☐ ☐ ☐ ExpressRoute ☐ ☐
- C.** Branch2 ☐ ☐ ☐ VPN ☐ ☐

D. Branch2 ☐ ☐ ExpressRoute ☐ ☐

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 120

You are configuring a new Azure Load Balancer.

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

You want to configure the Load Balancer with the following settings:

* Name: LB1

* Location: West US

* SKU: Standard

* IP Address: IP3

Which IP address should you select for the Load Balancer?

A. IP1 or IP3

B. IP3

C. IP3 or IP5

D. IP2

E. IP1, IP2, IP3, IP4 or IP5

F. IP1, IP3, IP4 or IP5

Answer: C ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address> This is because "Load balancer and the public IP address SKU must match when you use them with public IP addresses" <https://docs.microsoft.com/en-us/azure/load-balancer/skus> Standard SKU Load Balancer routes traffic within and across regions, and to Availability Zones for high resiliency.

NEW QUESTION: 121

You are configuring a new Azure Load Balancer.

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

□□□□ 1□ □□□ 1□ □□□□ □□. □□□□ VM1□ □□ □□ □□□□ □□. □□ □□ □□ □□□ □□□ □□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□ □□□□ □□□□.

Actions

Change the PIP1 SKU to **Standard**.

Start VM1.

Shut down VM1.

Disassociate PIP1 from NIC1.

Change Assignment to Dynamic for PIP1.

Associate PIP1 to NIC1.

Answer Area

Answer:

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview>

NEW QUESTION: 123

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

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

□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

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

□□ □□□ □□ LB1□□□ □□ □□□□ □□□□□.

* SKU: □□

* □□: □□

* □□□: Subnet12

* □□ □□□□ VNet1

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

Microsoft

NEW QUESTION: 124

APPGW1-NSG1 is a network security group. Which Azure Front Door routing rule configuration should you use to route traffic to the application gateway?

- A. AzureFrontDoor.Rule1
- B. AzureFrontDoor.FirstParty
- C. AzureFrontDoor.Rule1Rule1
- D. AzureFrontDoor.Infra

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 125

You have an Azure subscription. You need to create a policy that can be linked to the planned application gateway and block connections from IP addresses in the 131.107.150.0/24 range. Which Azure CLI command should you use to create the policy?

Answer:

See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for creating a policy that can be linked to the planned application gateway and block connections from IP addresses in the 131.107.150.0/24 range:

- * To create a policy, you need to go to the Azure portal and select Create a resource. Search for WAF , select Web Application Firewall , then select Create 1 .
- * On the 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
- * On the Custom rules tab, select Add a rule to create a custom rule that blocks connections from IP addresses in the 131.107.150.0/24 range 2 . Enter or select the following information for the custom rule:
 - * Rule name: Type a unique name for your custom rule
 - * Priority: Type a number that indicates the order of evaluation for this rule
 - * Rule type: Select Match rule
 - * Match variable: Select RemoteAddr

- * Operator: Select IPMatch
- * Match values: Type 131.107.150.0/24
- * Action: Select Block
- * On the Review + create tab, review your settings and select Create to create your WAF policy 1 .
- * To link your policy to the planned application gateway, you need to go to the Application Gateway service in the Azure port al and select your application gateway 3 .
- * On the Web appl ication firewall tab, select your WAF poli cy from the drop-down list a nd select Save

NEW QUESTION: 126

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

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

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

P2S(Point-to-Site) IKEv2 VPN□ □□□□ Vnet1□ □□□□ Client1□□□□ Windows 10 □□□□ □□□□.

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

Vnet2□ □□ □□□□□□□ □□□ □ □□□□□.

Client1□ Vnet2□ □□□ □ □□□ □□ □□ □□□□□□.

Client1□ Vnet2□ □□□ □ □□□ □□□□□ □□□.

□□ □□: VPN □□□□□□ □□□ □□□□□□□ □□ □□□□□□.

□□□□ □□□ □□□□□□?

- A. □
- B. □□□

Answer: A (LEAVE A REPLY)

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

Reference:

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

NEW QUESTION: 127

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

FWP1□ □□ □□ □□□ □□ □□□□ □□□ □□□□□□.

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

□□: □□ □□□ 1□□□□□.

Priorities:

100

200

300

Answer Area

RC1:

RC2:

RC3:

Answer:

Priorities:

100

200

300

Answer Area

RC1: 300

RC2: 200

RC3: 100

Explanation:

Priorities:

100

200

300

Answer Area

RC1: 300

RC2: 200

RC3: 100

NEW QUESTION: 128

www.contoso.com FQDN. The company has two Azure App Service environments. The first environment is named AS1 and the second environment is named AS2. The first environment is located in the East US region and the second environment is located in the West US region.

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

Azure Traffic Manager is configured to route traffic to the AS1 environment. The traffic manager profile is named TMprofile1.

The traffic manager profile is configured to route traffic to the AS1 environment. The traffic manager profile is configured to route traffic to the AS1 environment.

What is the correct DNS record configuration for the traffic manager profile?

A. www.contoso.com 131 107 100 1 131 107 200 1 CNAME

B. www.contoso.com TMprofile1.azurefd.net CNAME

C. www.contoso.com TMprofile1.trafficmanager.net CNAME

D. as1.contoso.com as2.contoso.com TXT

Answer: C ([LEAVE A REPLY](#))

Reference:

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

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

NEW QUESTION: 129

□□ □□ □□□ □□□□ □□□ 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□ □□□□ □□□□□.

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

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

□□: □□□ □□ □□□□ 1□□ □□□ □□□□.

Answer Area

DNS record type:

TXT

A

CNAME

SRV

TXT

Store the certificate in:

KeyVault2

FD1

KeyVault1

KeyVault2

Answer:

Answer Area

2, 4

NEW QUESTION: 132

Which Azure service can be used to protect your applications from DDoS attacks?

Microsoft Defender for Cloud is a cloud-native security solution that provides comprehensive protection for your Azure resources.

* NS-2. Which Azure service can be used to protect your applications from DDoS attacks?

* NS-8. Which Azure service can be used to protect your applications from DDoS attacks?

* NS-9. Which Azure service can be used to protect your applications from DDoS attacks?

Which Azure service can be used to protect your applications from DDoS attacks?

Which Azure service can be used to protect your applications from DDoS attacks?

Which Azure service can be used to protect your applications from DDoS attacks?

Answer Area

NS-2:

NS-8:

NS-9:

Answer:

NEW QUESTION: 134

Hub1 is a virtual hub in an Azure Virtual WAN. VNet1 is connected to Hub1 by using a connection named Conn1.

VNet2 is connected 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.

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 Peer1.

VNet1 is connected to VNet3 by using a virtual network peering named Peer2.

VWAN1 is a virtual WAN in an Azure Virtual WAN. VNet1 is connected to VWAN1 by using a connection named Conn1.

What is the default route table for VNet1?

Answer Area

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

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

Answer:

Answer Area

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

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

Explanation:

Answer Area

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

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

NEW QUESTION: 135

FrontDoor1 is an Azure Front Door. VNet1 is connected to FrontDoor1 by using a connection named Conn1.

Azure VNet1 is connected to Azure VNet2 by using a virtual network peering named Peer1.

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

Answer:

Explanation:

NEW QUESTION: 136

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



All services / Route tables / RouteTable1

Route table

Move Delete Refresh Give feedback

Essentials JSON View

Resource group (change)
RG1

Associations
1 subnet associations

Location
North Europe

Subscription (change)
Visual Studio Premium with MSDN

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

Tags (change)
Click here to add tags

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 Area

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

Answer:

Answer Area

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



Explanation:

Answer Area

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

AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-700-KR ☐☐! DumpTop ☐ ☐☐ **AZ-700-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐. ☐☐☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop AZ-700-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (330 Q&As Dumps, **30%OFF**)
Special Discount: **KrDump**)

NEW QUESTION: 137

[illegible]

- A.** Vnet2 ☐ Vnet3 ☐ GatewaySubnet ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
- B.** Vnet1 ☐ GatewaySubnet ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
- C.** BGP ☐ ☐ ☐ ☐
- D.** ☐ ☐ ☐ ☐

Answer: ([SHOW ANSWER](#))

VNet 1 will get the default from BGP and propagate it to VNET 2 and 3

NEW QUESTION: 138

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

* AzureFirewall□□□

* 00000000

* 000 1

* 0002

* 0003

Subnet2 Microsoft.Web/serverfarms 0000 00 0000 000000. 00 0000 00 00 00 00 0000 0000 0000.

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

Azure WAF(0 000000 000)0 000 AG1000 Azure 0000000 0000000 0000 000. AG10 VMSS10 0000 0 000000.

AG10 00 0000 0000 000?

A. GatewaySubnet

B. Subrwt2

C. Subnet 1

D. AzureFjrewall Subnet

E. Subnet3

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 139

030 00000 DNS 0000 00000.

Azure00 DNS 000 00000 000.

00 0 00 000 0000 0000 000? 0000 00 0000 00 000 00 0000 00 000 0000 0000.

Actions

Answer Area



- Modify the SOA records for the domain.
- Identify the IP addresses of the name servers.
- Create a public DNS zone.
- Identify the FQDNs of the name servers.
- Modify the NS records for the domain.

Answer:

Actions

- Modify the SOA records for the domain.
- Identify the IP addresses of the name servers.
- Create a public DNS zone.
- Identify the FQDNs of the name servers.
- Modify the NS records for the domain.

Answer Area

- Create a public DNS zone.
- Identify the FQDNs of the name servers.
- Modify the NS records for the domain.

Explanation:

Actions

- Modify the SOA records for the domain.
- Identify the IP addresses of the name servers.

Answer Area

- Create a public DNS zone.
- Identify the FQDNs of the name servers.
- Modify the NS records for the domain.

NEW QUESTION: 140

□□□□ □ □□□ □□□□ 10□□ □□□□. □ □□□□□ □□ □□ Azure □□□ □□□□□ □□ □□□□□ □□ □□□□ □ □□□□.

□□ □□ □□□□ App1□□□□ □□□□□□□□ □□□ □□□□. 10□□□□ App1□ □□□□□ □□□ □□□□ □□ □□□ □ □□ □□□□□□ □□□□□□.

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

DNS □□□ □□□ □□□□□ Traffic Manager □□□□ □□□□ □□□.

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

□□: □□ □□□ 1□□□□□.

Answer Area

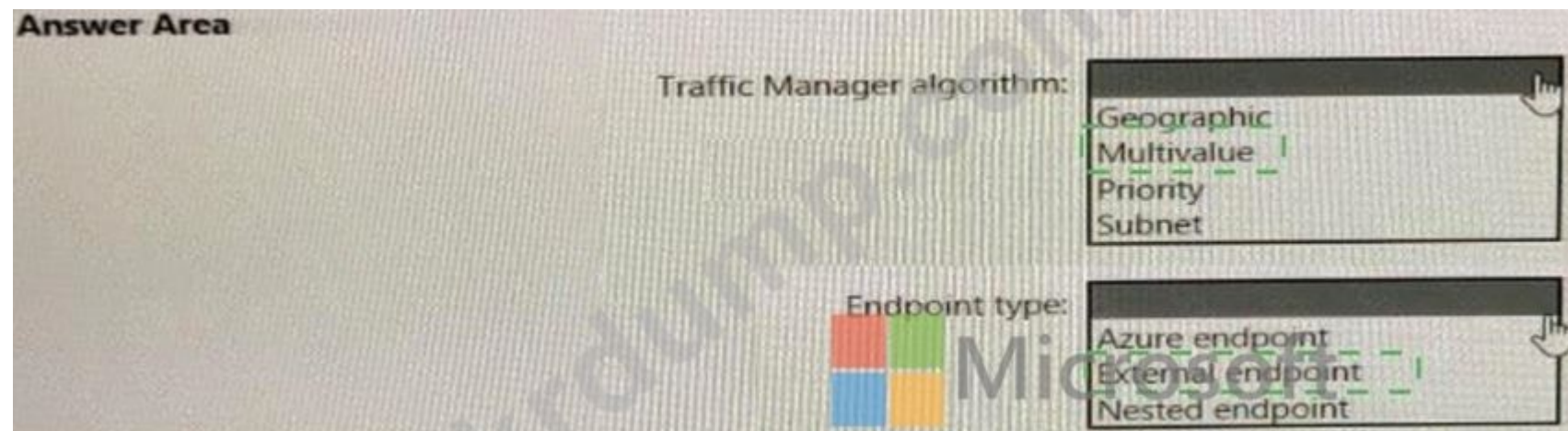
Traffic Manager algorithm:

- Geographic
- Multivalue
- Priority
- Subnet

Endpoint type:

- Azure endpoint
- External endpoint
- Nested endpoint

Answer:



Explanation:

Traffic Manager algorithm:

	▼
Geographic	
Multivalue	
Priority	
Subnet	

Endpoint type:

	▼
Azure endpoint	
External endpoint	
Nested endpoint	

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods>

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types>

NEW QUESTION: 141

1000 00 0000 0000 Azure 00 000000 000000 0000. 0 00000 IPv6 000 000000. 0 00000 00 20000 00 0000 00 0000 00000000. 00 00000 0000 0000 0000 0000 000000 0000. 0000 00000 0000?

A. /24

B. /120

C. /64

D. /48

Answer: A (LEAVE A REPLY)

NEW QUESTION: 142

You are configuring an Azure environment.

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 and VM2 are both virtual machines. storage1 is a storage account.

* VM1 and VM2 are both virtual machines.

* storage1 is a storage account.

What is the correct configuration?

A. storage1 is linked to Subnet1.

B. storage1 is linked to VM1.

C. storage1 is linked to VM2.

D. storage1 is linked to VNet1 (NSG).

Answer: A (LEAVE A REPLY)

NEW QUESTION: 143

You are configuring an Azure Traffic Manager profile.

TM1 is a Traffic Manager profile. TM2 is a Traffic Manager profile. TM3 is a Traffic Manager profile.

Name	Location
App1	North Europe
App2	East US
App3	Central US
TM2	West Europe
TM3	West US

TM2 MinChildEndpoint = 2.

Name	Location	Weight
App4	West Europe	99
App5	West Europe	1

TM3 is a Traffic Manager profile.

Name	Location
App6	West US
App2	East US

App2, App4, App6 □□□□□□ □□□□ □□□ □□□□□□□□.

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

□□: □□□ □□ □□□□ 1□□ □□□ □□□□.

Traffic from West Europe:

▼

App1

App2

App4

App5

Microsoft

Traffic from West US:

▼

App1

App2

App3

App6

Answer:

Traffic from West Europe:

▼

App1

App2

App4

App5

Microsoft

Traffic from West US:

▼

App1

App2

App3

App6

Explanation:



Traffic from West US:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles> Traffic from West Europe:

This goes back to the origin TM1 that uses performance traffic-routing method, which means the closest location is App1 and naturally be the next best performance instance.

Traffic from West US:

This goes back to the original TM1 that uses performance traffic-routing method, from TM1, the other 2 US locations would be App2 and App3. But App2 we know it 's already degraded (unavailable), hence the only option would be App3.

Answer = App3

NEW QUESTION: 144

Hub1 Spoke1 □□ □□□□ □□□□ □□□□.

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

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

☐ ☐☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐ ☐ ☐☐ ☐☐☐☐.

□□: □□ □□□ 1□□□□.

Values	Answer Area
-AllowForwardedTraffic	\$hub = Get-AZVirtualNetwork -ResourceGroup "RG1" -Name "Hub1"
-AllowGatewayTransit	\$spoke = Get-AZVirtualNetwork -ResourceGroup "RG2" -Name "Spoke1"
-UseRemoteGateways	Add-AZVirtualNetworkPeering -Name "Hub1-Spoke1" -VirtualNetwork \$hub
	-RemoteVirtualNetworkId \$spoke.id Value
	Add-AZVirtualNetworkPeering -Name "Spoke1-Hub1" -VirtualNetwork \$spoke
	-RemoteVirtualNetworkId \$hub.id Value

Answer:

Values	Answer Area
-AllowForwardedTraffic	\$hub = Get-AZVirtualNetwork -ResourceGroup "RG1" -Name "Hub1"
-AllowGatewayTransit	\$spoke = Get-AZVirtualNetwork -ResourceGroup "RG2" -Name "Spoke1"
-UseRemoteGateways	Add-AZVirtualNetworkPeering -Name "Hub1-Spoke1" -VirtualNetwork \$hub
	-RemoteVirtualNetworkId \$spoke.id -AllowGatewayTransit
	Add-AZVirtualNetworkPeering -Name "Spoke1-Hub1" -VirtualNetwork \$spoke
	-RemoteVirtualNetworkId \$hub.id -UseRemoteGateways

Explanation:

\$hub = Get-AZVirtualNetwork -ResourceGroup "RG1" -Name "Hub1"
\$spoke = Get-AZVirtualNetwork -ResourceGroup "RG2" -Name "Spoke1"
Add-AZVirtualNetworkPeering -Name "Hub1-Spoke1" -VirtualNetwork \$hub
-RemoteVirtualNetworkId \$spoke.id -AllowGatewayTransit
Add-AZVirtualNetworkPeering -Name "Spoke1-Hub1" -VirtualNetwork \$spoke
-RemoteVirtualNetworkId \$hub.id -UseRemoteGateways

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#virtual-network-peering>

AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ AZ-700-KR ☐☐! DumpTop ☐ ☐☐ **AZ-700-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop AZ-700-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐☐☐. ☐☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop AZ-700-KR ☐☐☐☐☐☐☐☐. <https://www.dumptop.com/Microsoft/AZ-700-KR-dump.html> (330 Q&As Dumps, **30%OFF** Special Discount: **KrDump**)