Microsoft.Pre.AZ-700.by.VCEplus.57q - DEMO

Testlet 1

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

Overview

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

Existing Environment

Hybrid Environment

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

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

Azure Environment

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

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

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 can be resolved from the on-premises locations.
- Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.
- Minimize the size of the subnets allocated to platform-managed services.
- Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements

Litware identifies the following hybrid networking requirements:

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

PaaS Networking Requirements

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

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

QUESTION 1
HOTSPOT

You need to recommend a configuration for the ExpressRoute connection from the Boston datacenter. The solution must meet the hybrid networking requirements and business requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the ExpressRoute gateway type to:

- High Performance (ERGw2AZ)
- Standard Performance (ERGw1AZ)
- Ultra Performance (ERGw3AZ)

To minimize latency of traffic to Vnet2:

- Create a dedicated ExpressRoute circuit for Vnet2
- Connect Vnet2 directly to the ExpressRoute circuit
- Configure gateway transit for the peering between Vnet1 and Vnet2

Correct Answer:

Answer Area

Set the ExpressRoute gateway type to:

- High Performance (ERGw2AZ)
- Standard Performance (ERGw1AZ)
- Ultra Performance (ERGw3AZ)

To minimize latency of traffic to Vnet2:

- Create a dedicated ExpressRoute circuit for Vnet2
- Connect Vnet2 directly to the ExpressRoute circuit
- Configure gateway transit for the peering between Vnet1 and Vnet2

Section: [none]
Explanation
Explanation/Reference:

Testlet 2

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

Overview

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

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

Existing Environment

Azure Network Infrastructure

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

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

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

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

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

Azure Private DNS Zones

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

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

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

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

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

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

Requirements

Virtual Network Requirements

Contoso has the following virtual network requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
  - Two container groups that connect to Vnet6
  - Three virtual machines that connect to Vnet6
  - Allow VPN connections to be established to Vnet6
  - Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.
- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet. **Network**

Security Requirements

Contoso has the following network security requirements:

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

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

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

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

QUESTION 1 You need to configure GW1 to meet the network security requirements for the P2S VPN users.

Which Tunnel type should you select in the Point-to-site configuration settings of GW1?

A. IKEv2 and OpenVPN (SSL)
B. IKEv2
C. IKEv2 and SSTP (SSL)
D. OpenVPN (SSL)
E. SSTP (SSL)

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant **Question Set 3**

QUESTION 1 Your company has a single on-premises datacenter in New York. The East US Azure region has a peering location in New York.

The company only has Azure resources in the East US region.

You need to implement ExpressRoute to support up to 1 Gbps. You must use only ExpressRoute Unlimited data plans. The solution must minimize costs.

Which type of ExpressRoute circuits should you create?

A. ExpressRoute Local
B. ExpressRoute Direct
C. ExpressRoute PremiumD. ExpressRoute Standard

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference: https://azure.microsoft.com/en-us/pricing/details/expressroute/

QUESTION 2 You are planning an Azure Point-to-Site (P2S) VPN that will use OpenVPN.

Users will authenticate by an on-premises Active Directory domain.

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

A. an Azure key vault
B. a RADIUS server
C. a certification authority
D. Azure Active Directory (Azure AD) Application Proxy

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 3 You plan to configure BGP for a Site-to-Site VPN connection between a datacenter and Azure.

Which two Azure resources should you configure? Each correct answer presents a part of the solution. (Choose two.)

NOTE: Each correct selection is worth one point.

A. a virtual network gateway
B. Azure Application Gateway
C. Azure Firewall
D. a local network gateway
E. Azure Front Door

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/bgp-howto

QUESTION 4 You fail to establish a Site-to-Site VPN connection between your company's main office and an Azure virtual network.

You need to troubleshoot what prevents you from establishing the IPsec tunnel.

Which diagnostic log should you review?

A. IKEDiagnosticLog
B. RouteDiagnosticLog
C. GatewayDiagnosticLog
D. TunnelDiagnosticLog

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics

Testlet 1

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

Overview

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

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

Existing Environment

Azure Network Infrastructure

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

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

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

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

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

Azure Private DNS Zones

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

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

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

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

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

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

Requirements

Virtual Network Requirements

Contoso has the following virtual network requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
  - Two container groups that connect to Vnet6
  - Three virtual machines that connect to Vnet6
  - Allow VPN connections to be established to Vnet6
  - Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.
- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet. **Network**

Security Requirements

Contoso has the following network security requirements:

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

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

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

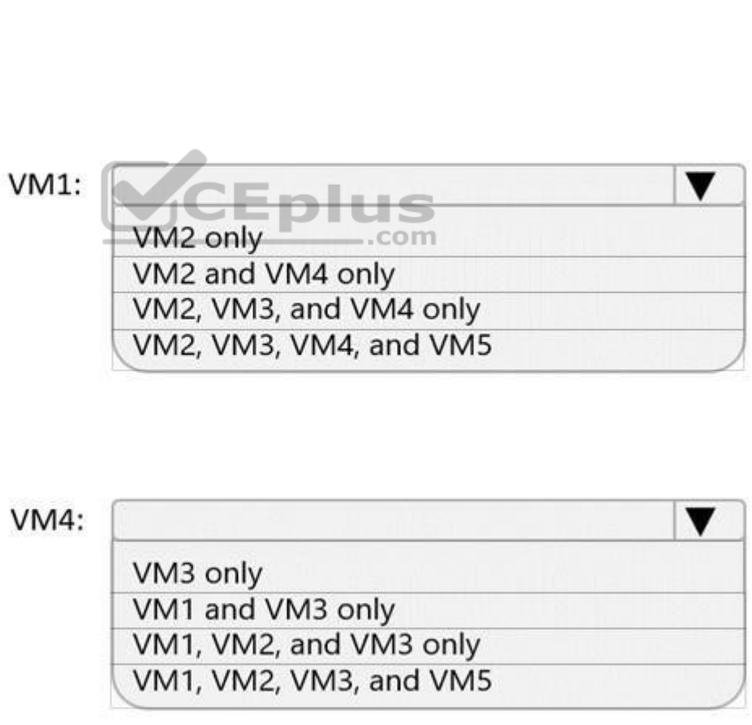
Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

QUESTION 1
HOTSPOT

Which virtual machines can VM1 and VM4 ping successfully? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area

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

Section: [none]
Explanation

Explanation/Reference:
Explanation:
Box 1: VM2, VM3 and VM4.
VM1 is in VNet1/Subnet1. VNet1 is peered with VNet2 and VNet3.
There are no NSGs blocking outbound ICMP from VNet1. There are no NSGs blocking inbound ICMP to VNet1/Subnet2, VNet2 or VNet3. Therefore, VM1 can ping VM2 in VNet1/Subnet2, VM3 in VNet2 and VM4 in VNet3.

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

QUESTION 2
What should you implement to meet the virtual network requirements for the virtual machines that connect to Vnet4 and Vnet5?

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

Correct Answer: E
Section: [none]
Explanation

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

Question Set 2

QUESTION 1
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have two Azure virtual networks named Vnet1 and Vnet2.

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

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

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You reset the gateway of Vnet1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

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

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

QUESTION 2
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have two Azure virtual networks named Vnet1 and Vnet2.

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

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

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You enable BGP on the gateway of Vnet1.

Does this meet the goal?

A. Yes
B. No

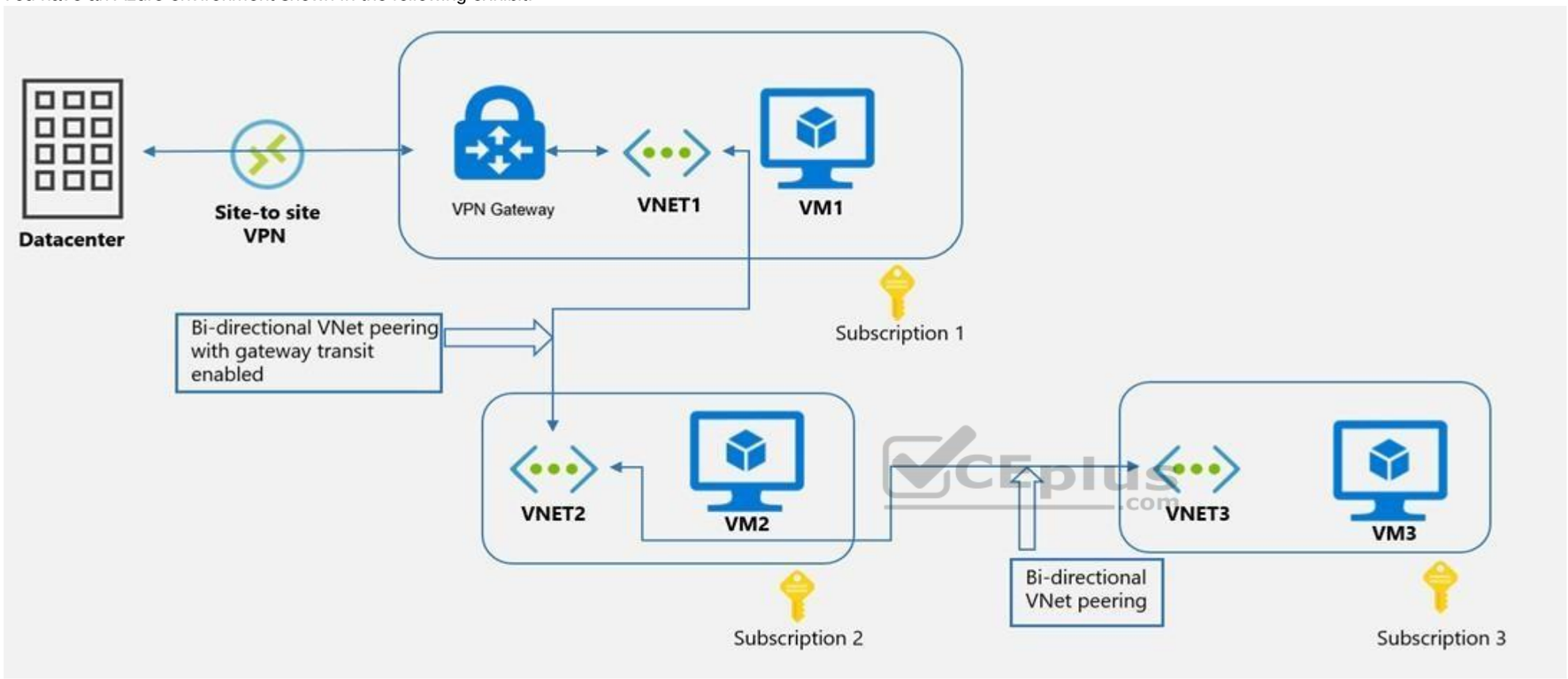
Correct Answer: B
Section: [none]
Explanation

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

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

QUESTION 3
HOTSPOT

You have an Azure environment shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

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

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

Correct Answer:

Answer Area

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

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

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

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

Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit?toc=/azure/virtual-network/toc.json

QUESTION 4 You plan to deploy Azure virtual network.

You need to design the subnets.

Which three types of resources require a dedicated subnet? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure Bastion
B. Azure Active Directory Domain Services
C. Azure Private Link
D. Azure Application Gateway v2
E. VPN gateway

Correct Answer: ADE
Section: [none]
Explanation

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

QUESTION 5
HOTSPOT

You have an Azure private DNS zone named contoso.com that is linked to the virtual networks shown in the following table.

Name	IP address
Vnet1	10.1.0.0/16
Vnet2	10.2.0.0/16

The links have auto registration enabled.

You create the virtual machines shown in the following table.

Name	IP address
VM1	10.1.10.10
VM2	10.2.10.10
VM3	10.2.10.11

You manually add the following entry to the contoso.com zone:

Name: VM1 IP address: 10.1.10.9

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: No
The manual DNS record will overwrite the auto-registered DNS record so VM1 will resolve to 10.1.10.9.

Box 2: No
The DNS record for VM1 is now a manually created record rather than an auto-registered record. Only auto-registered DNS records are deleted when a VM is deleted.

Box 3: No
This answer depends on how the IP address is changed. To change the IP address of a VM manually, you would need to select 'Static' as the IP address assignment. In this case, the DNS record will not be updated because only DHCP assigned IP addresses are auto-registered.

Reference: https://docs.microsoft.com/en-us/azure/dns/dns-faq-private

QUESTION 6
HOTSPOT

Your company has an Azure virtual network named Vnet1 that uses an IP address space of 192.168.0.0/20. Vnet1 contains a subnet named Subnet1 that uses an IP address space of 192.168.0.0/24.

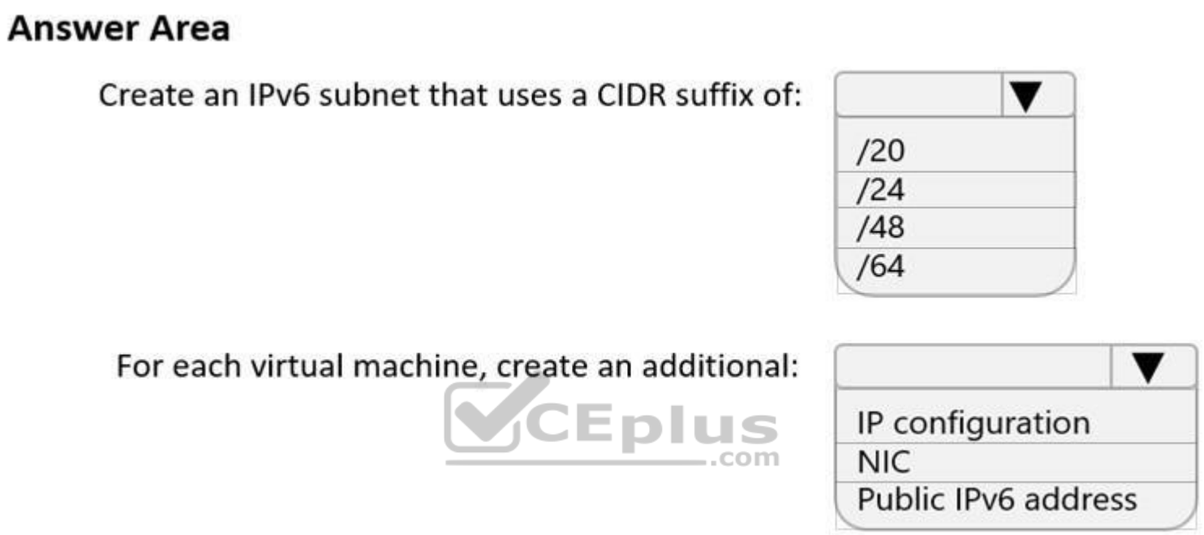
You create an IPv6 address range to Vnet1 by using a CIDR suffix of /48.

You need to enable the virtual machines on Subnet1 to communicate with each other by using IPv6 addresses assigned by the company. The solution must minimize the number of additional IPv4 addresses.

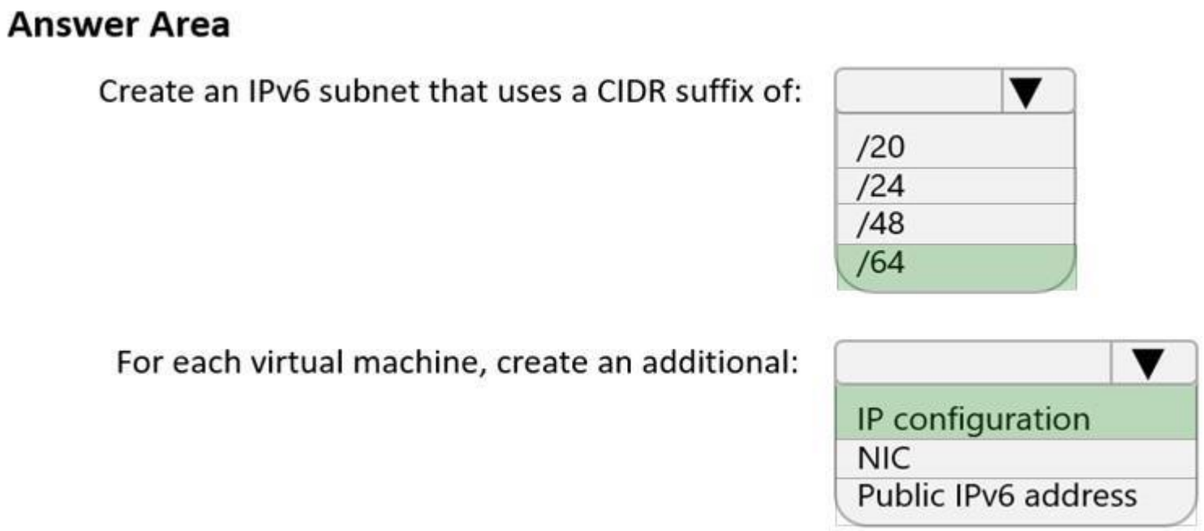
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Section: [none]
Explanation

Explanation/Reference:
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

QUESTION 7
HOTSPOT

You plan to deploy Azure Virtual WAN.

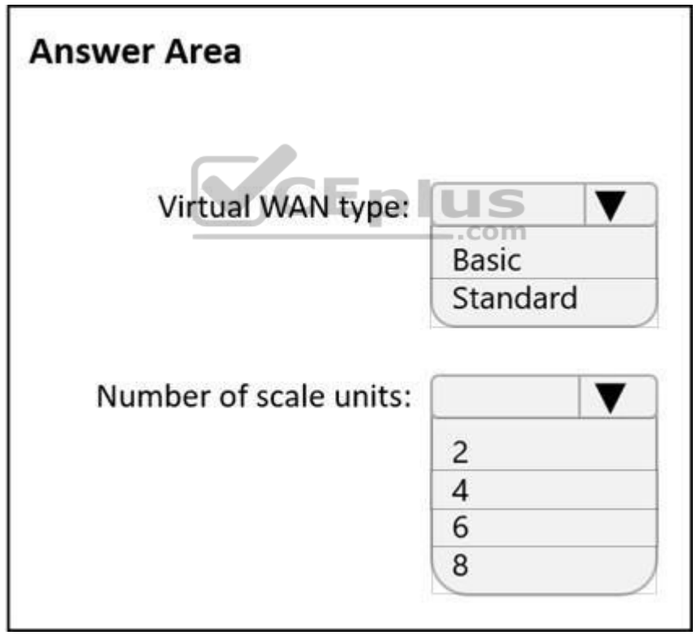
You need to deploy a virtual WAN hub that meets the following requirements:

Supports 10 sites that will connect to the virtual WAN hub by using a Site-to-Site VPN connection
Supports 8 Gbps of ExpressRoute traffic Minimizes
costs

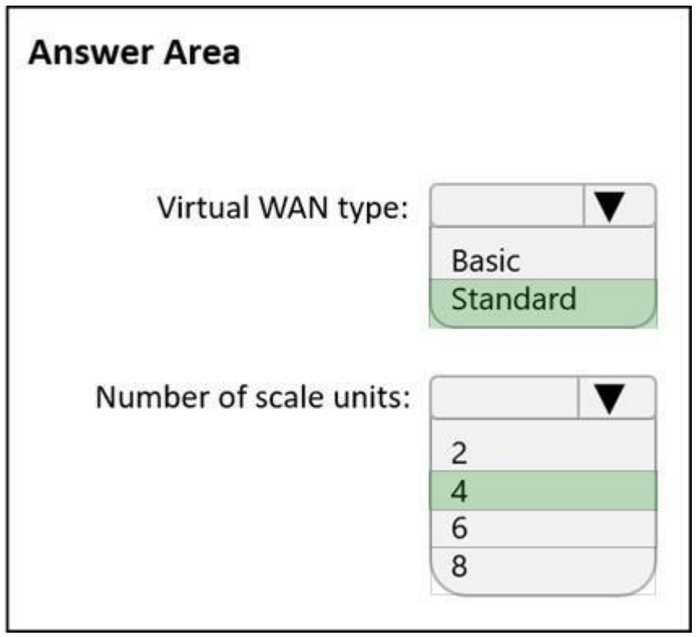
What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Section: [none]
Explanation

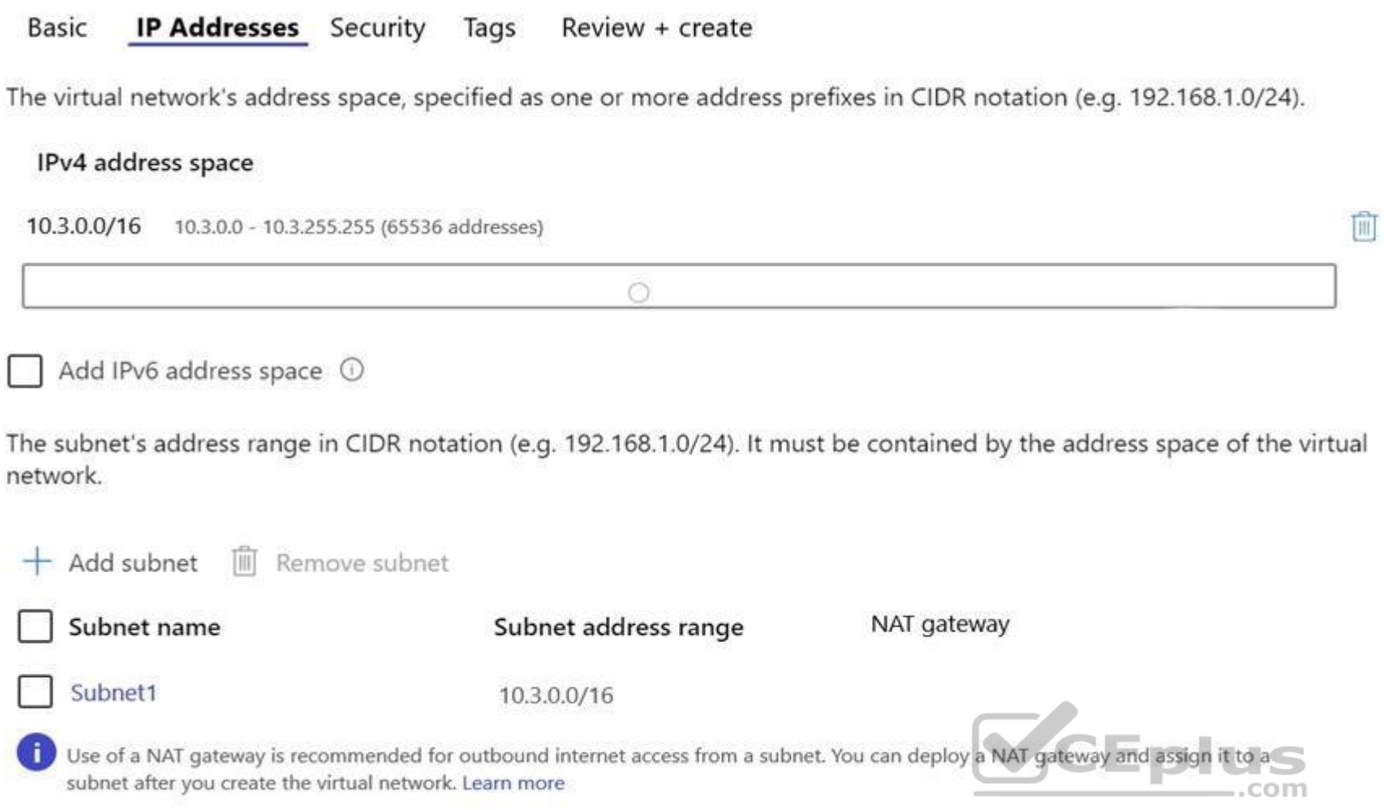
Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

QUESTION 8
DRAG DROP

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

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

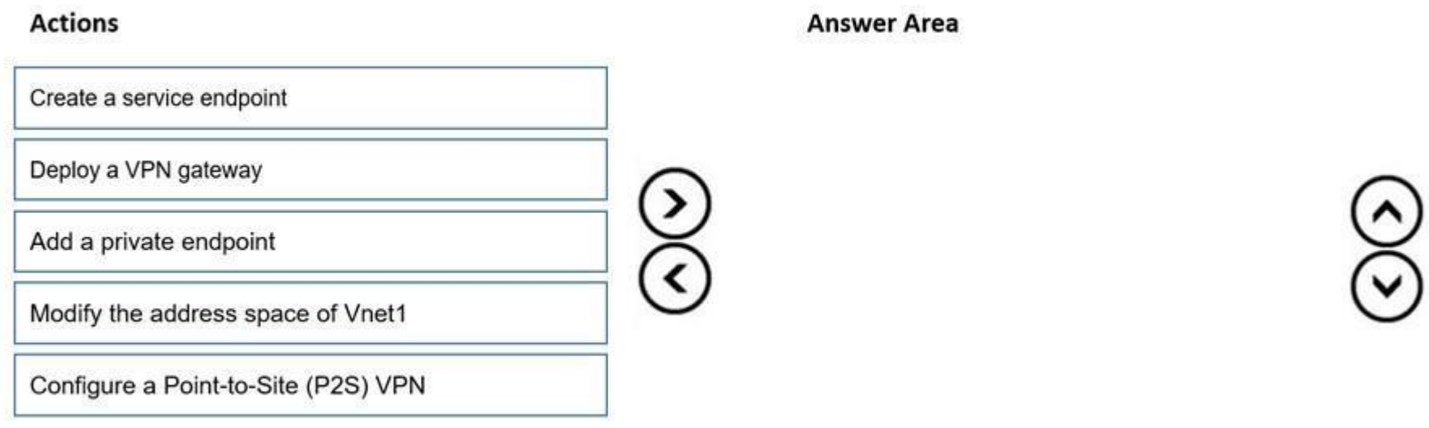
The IP Addresses settings for Vnet1 are configured as shown in the exhibit.



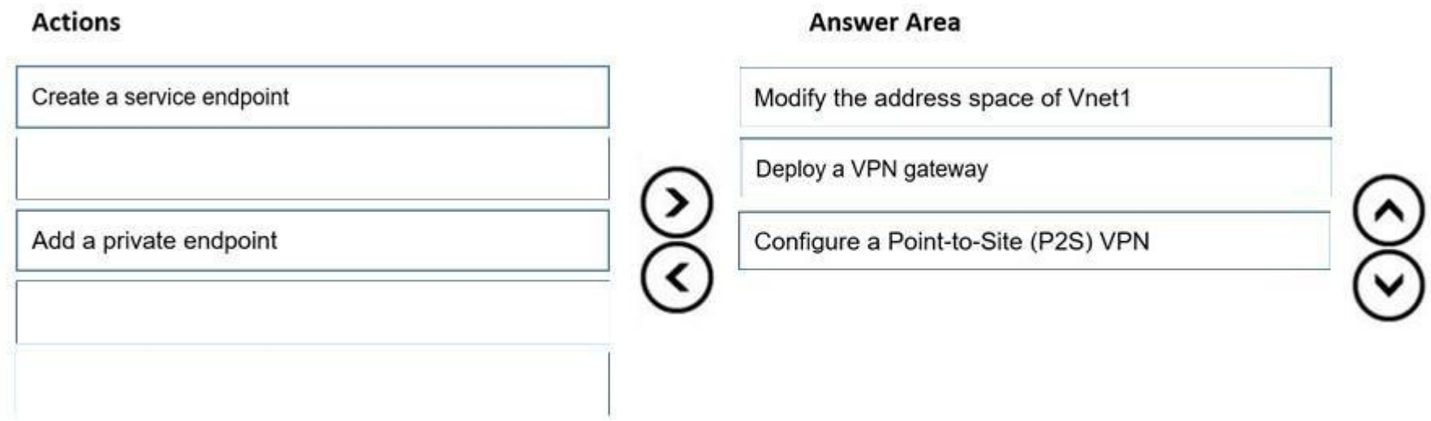
You need to ensure that you can integrate WebApp1 and Vnet1.

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

Select and Place:



Correct Answer:



Section: [none]
Explanation

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

QUESTION 9
DRAG DROP

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

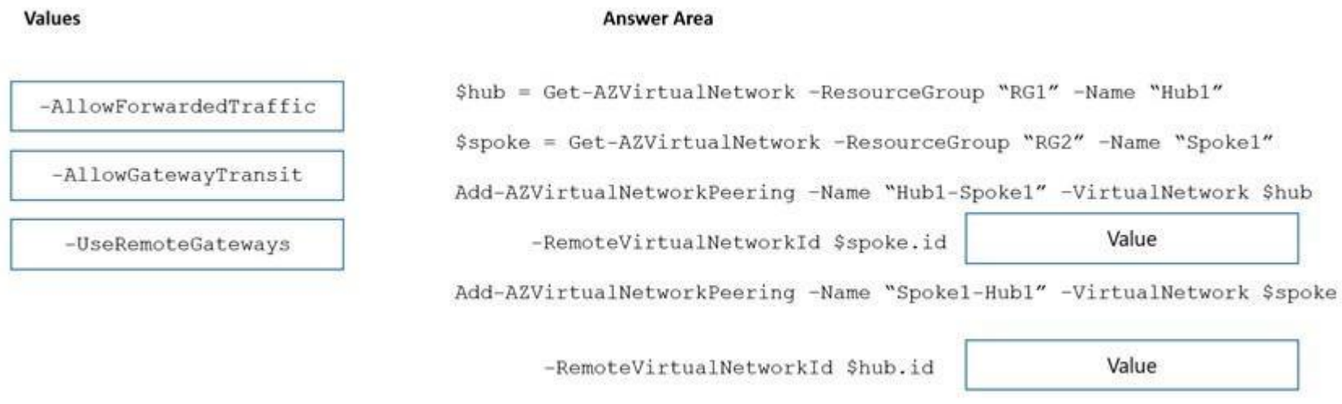
You are implementing peering between Hub1 and Spoke1.

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

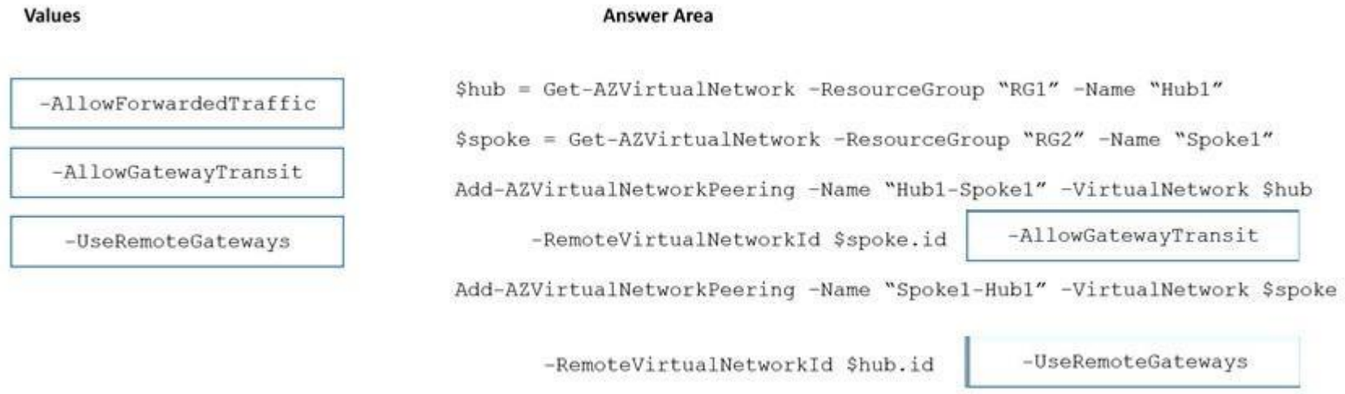
How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Section: [none]
Explanation

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

QUESTION 10
DRAG DROP

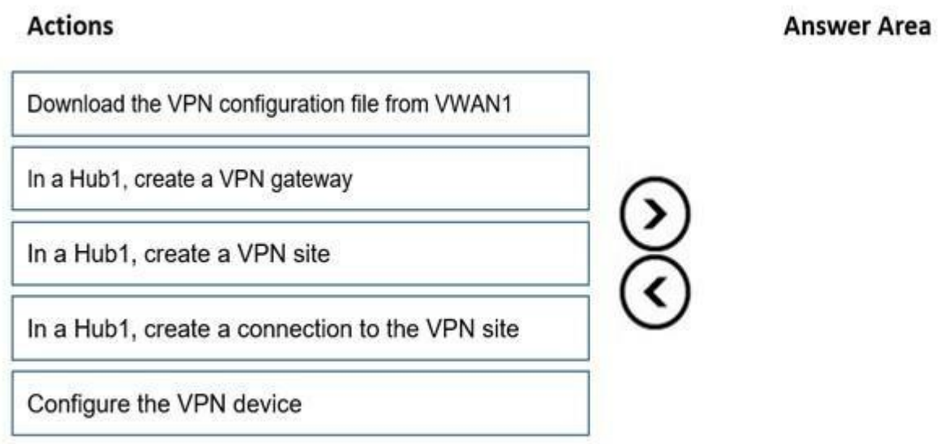
You have three on-premises sites. Each site has a third-party VPN device.

You have an Azure virtual WAN named VWAN1 that has a hub named Hub1. Hub1 connects two of the three on-premises sites by using a Site-to-Site VPN connection.

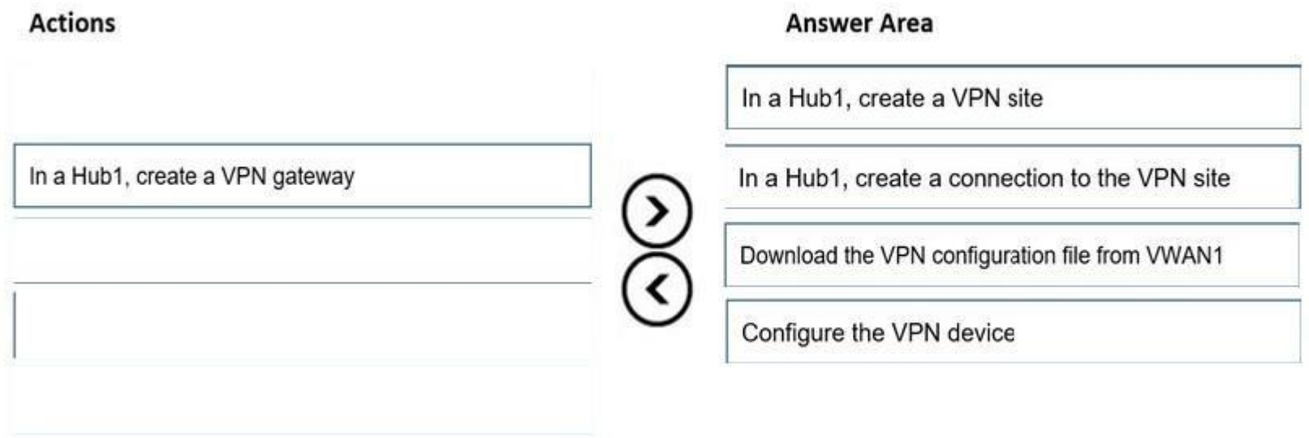
You need to connect the third site to the other two sites by using Hub1.

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

Select and Place:



Correct Answer:



Section: [none]
Explanation

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

QUESTION 11
HOTSPOT

You are planning an Azure solution that will contain the following types of resources in a single Azure region:

Virtual machine
Azure App Service
Virtual Network gateway
Azure SQL Managed Instance

App Service and SQL Managed Instance will be delegated to create resources in virtual networks.

You need to identify how many virtual networks and subnets are required for the solution. The solution must minimize costs to transfer data between virtual networks.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Virtual Networks:

1
2
3
4

Subnets:

1
2
3
4

Correct Answer:

Answer Area

Virtual Networks:

1
2
3
4

Subnets:

1
2
3
4

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network

QUESTION 12

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have two Azure virtual networks named Vnet1 and Vnet2.

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

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

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You download and reinstall the VPN client configuration.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

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

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

Testlet 1

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

Overview

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

Existing Environment

Hybrid Environment

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

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

Azure Environment

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

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

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 can be resolved from the on-premises locations.
- Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.
- Minimize the size of the subnets allocated to platform-managed services.
- Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements

Litware identifies the following hybrid networking requirements:

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

PaaS Networking Requirements

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

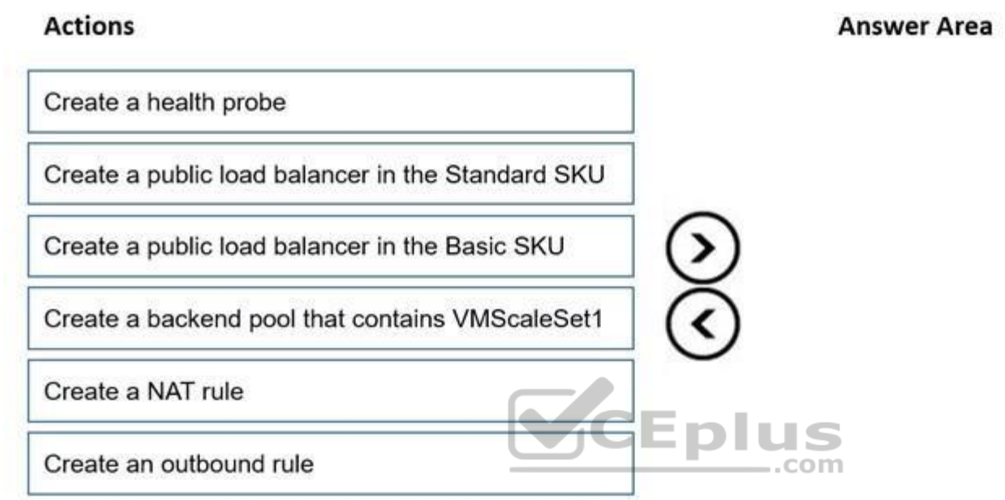
▪ The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1. ▪ The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

QUESTION 1
DRAG DROP

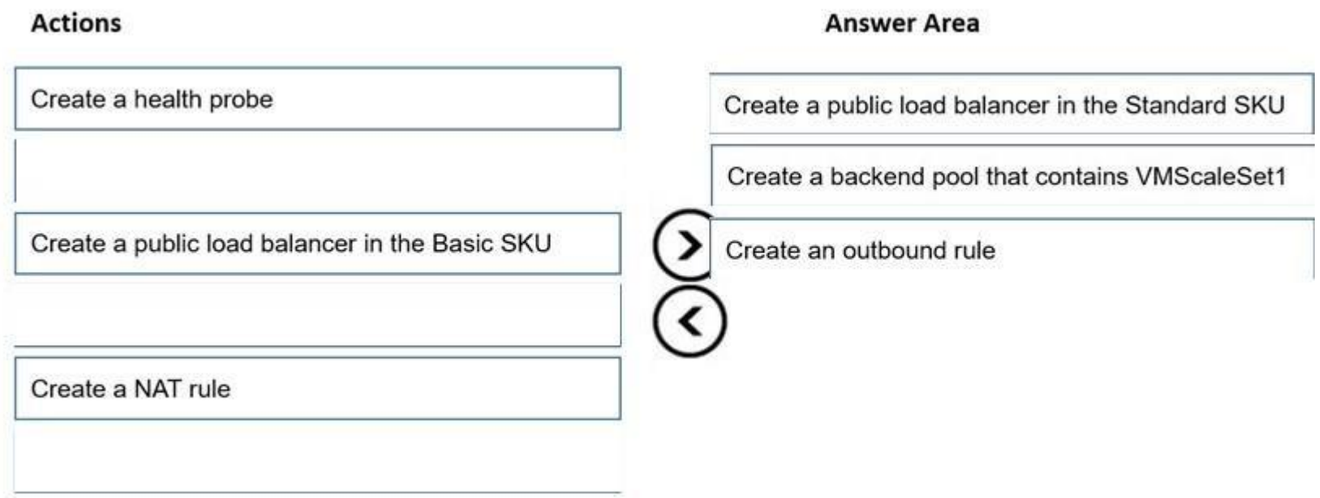
You need to implement outbound connectivity for VMScaleSet1. The solution must meet the virtual networking requirements and the business requirements.

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

Select and Place:



Correct Answer:



Section: [none]

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

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

What should you use to configure the default route?

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

Correct Answer: B
Section: [none]
Explanation

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

Testlet 2

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

Overview

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

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

Existing Environment

Azure Network Infrastructure

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

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

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

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

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

Azure Private DNS Zones

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

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

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

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

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

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

Requirements

Virtual Network Requirements

Contoso has the following virtual network requirements:

- Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
  - Two container groups that connect to Vnet6
  - Three virtual machines that connect to Vnet6
  - Allow VPN connections to be established to Vnet6
  - Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.
- The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.
- A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet. **Network**

Security Requirements

Contoso has the following network security requirements:

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

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

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

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

QUESTION 1
HOTSPOT

You are implementing the virtual network requirements for VM-Analyze.

What should you include in a custom route that is linked to Subnet2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Address prefix:
- 0.0.0.0/0
- 0.0.0.0/32
- 10.1.0.0/16
- 255.255.255.255/0
- 255.255.255.255/32

Next hop type:
- None
- Internet
- Virtual appliance
- Virtual network
- Virtual network gateway

Correct Answer:

Answer Area

Address prefix: ▼
- 0.0.0.0/0
- 0.0.0.0/32
- 10.1.0.0/16
- 255.255.255.255/0
- 255.255.255.255/32

Next hop type: ▼
- None
- Internet
- Virtual appliance
- Virtual network
- Virtual network gateway

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview
Question Set 3

QUESTION 1
HOTSPOT

You have an Azure subscription that contains the route tables and routes shown in the following table.

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

The subscription contains the subnets shown in the following table.

Name	Prefix	Route table	Virtual network
Subnet1	10.10.1.0/24	RT1	Vnet1
Subnet2	10.10.2.0/24	RT2	Vnet1
GatewaySubnet	10.10.3.0/24	**None**	Vnet1

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

Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

There is a Site-to-Site VPN connection to each local network gateway.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	◯	◯
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	◯	◯
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	◯	◯

Correct Answer:

Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	○	○
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	○	○

Section: [none]
Explanation

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

QUESTION 2
You have an Azure subscription that contains the public IP addresses shown in the following table.

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

You plan to deploy a NAT gateway named NAT1.

Which public IP addresses can be used as the public IP address for NAT1?

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

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:

Only static IPv4 addresses in the Standard SKU are supported. IPv6 doesn't support NAT.

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

QUESTION 3 You have an Azure application gateway named AGW1 that has a routing rule named Rule1. Rule 1 directs traffic for http://www.contoso.com to a backend pool named Pool1. Pool1 targets an Azure virtual machine scale set named VMSS1.

You deploy another virtual machine scale set named VMSS2.

You need to configure AGW1 to direct all traffic for http://www.adatum.com to VMSS2.
The solution must ensure that requests to http://www.contoso.com continue to be directed to Pool1.

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: ADE
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/application-gateway/configuration-overview

QUESTION 4
HOTSPOT

You have an Azure Traffic Manager parent profile named TM1. TM1 has two child profiles named TM2 and TM3.

TM1 uses the performance traffic-routing method and has the endpoints shown in the following table.

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

TM2 uses the weighted traffic-routing method with `MinChildEndpoint = 2` and has the endpoints shown in the following table.

Name	Location	Weight
App4	West Europe	99
App5	West Europe	1

TM3 uses priority traffic-routing method and has the endpoints shown in the following table.

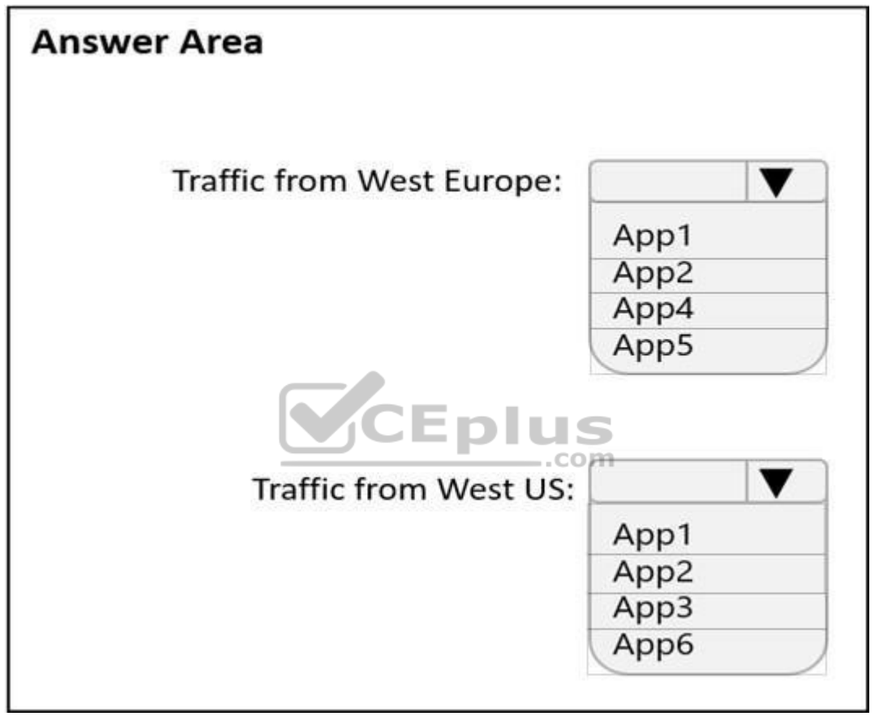
Name	Location
App6	West US
App2	East US

The App2, App4, and App6 endpoints have a degraded monitoring status.

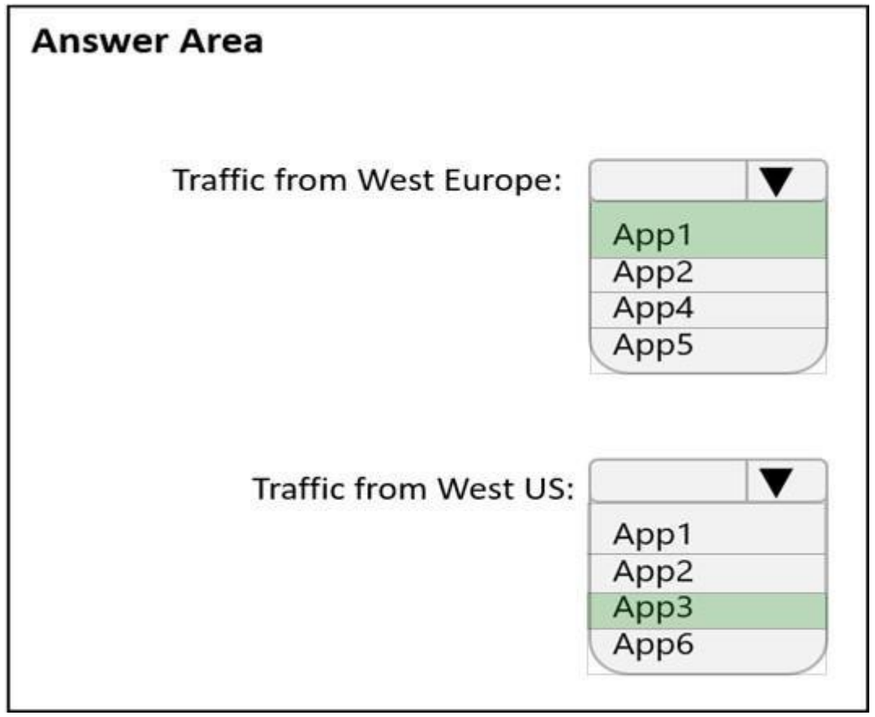
To which endpoint is traffic directed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Hot Area:



Correct Answer:



Section: [none]
Explanation
Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles

QUESTION 5
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

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

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

```
{
 "timeStamp": "2021-06-02T18:13:45+00:00",
 "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
 "operationName": "ApplicationGatewayFirewall",
 "category": "ApplicationGatewayFirewallLog",
 "properties": {
   "instanceId": "appgw_0",
   "clientIp": "137.135.10.24",
   "clientPort": "",
   "requestUri": "/login",
   "ruleSetType": "OWASP_CRS",
   "ruleSetVersion": "3.0.0",
   "ruleId": "920300",
   "message": "Request Missing an Accept Header",
   "action": "Matched",
   "site": "Global",
   "details": {
     "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
     "data": "",
     "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
     "line": "1247"
   },
   "hostname": "app1.contoso.com",
   "transactionId": "f7546159ylhjk7wall4568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


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

Solution: You add a rewrite rule for the host header.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 6
HOTSPOT

You have an Azure Front Door instance that provides access to a web app. The web app uses a hostname of www.contoso.com.

You have the routing rules shown in the following table.

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

Which rule will apply to each incoming request? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

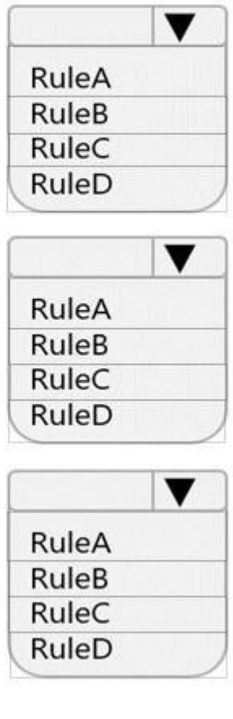
Hot Area:

Answer Area

www.contoso.com/abc/def

www.contoso.com/default.htm

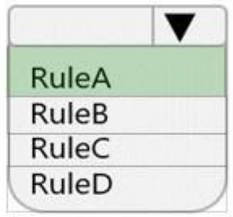
www.contoso.com/abc/def/default.htm



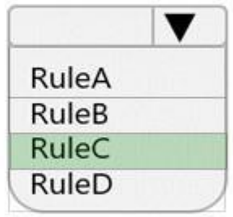
Correct Answer:

Answer Area

www.contoso.com/abc/def



www.contoso.com/default.htm



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

Section: [none]
Explanation

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

QUESTION 7
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

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

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

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


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

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

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 8 You have an Azure subscription that contains an Azure App Service app. The app uses a URL of https://www.contoso.com.

You need to use a custom domain on Azure Front Door for www.contoso.com. The custom domain must use a certificate from an allowed certification authority (CA).

What should you include in the solution?

A. an enterprise application in Azure Active Directory (Azure AD)
B. Active Directory Certificate Services (AD CS)
C. Azure Key Vault
D. Azure Application Gateway

Correct Answer: C
Section: [none]
Explanation

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

QUESTION 9 You have an Azure application gateway for a web app named App1. The application gateway allows end-to-end encryption.

You configure the listener for HTTPS by uploading an enterprise-signed certificate.

You need to ensure that the application gateway can provide end-to-end encryption for App1.

What should you do?

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

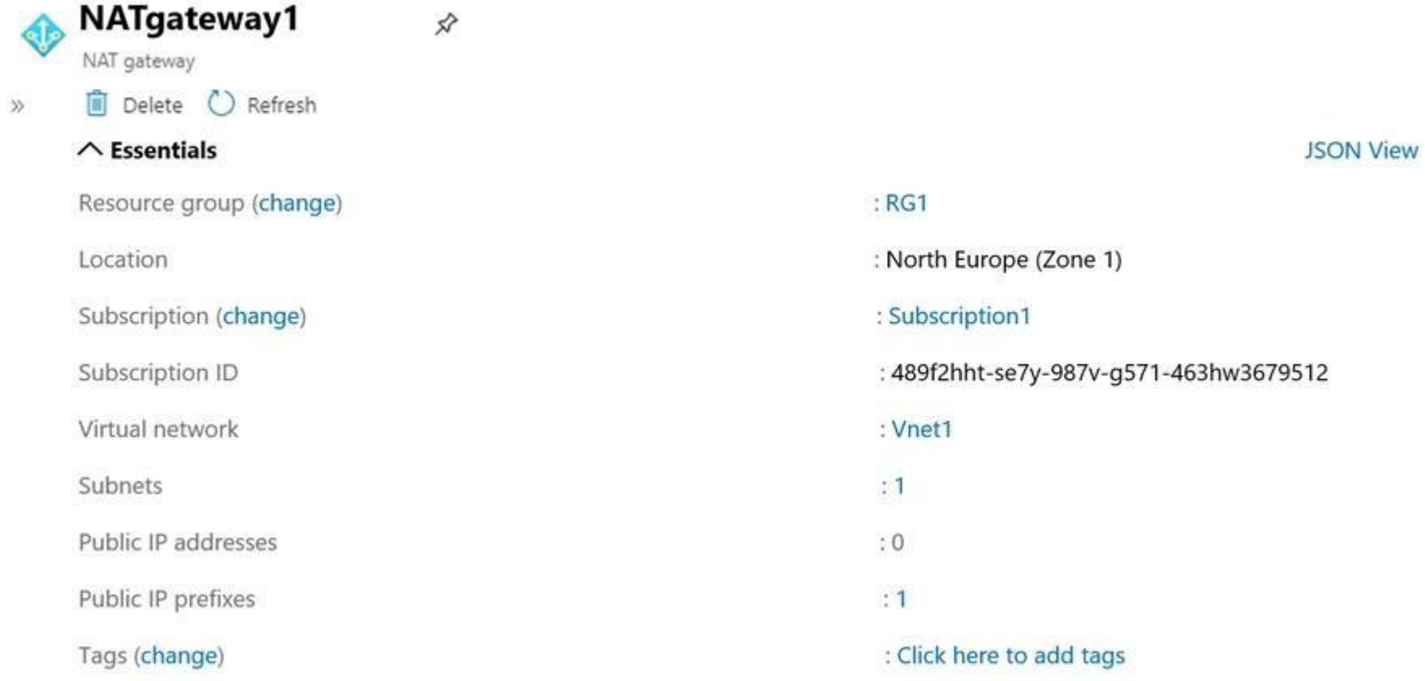
Correct Answer: D
Section: [none]
Explanation

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

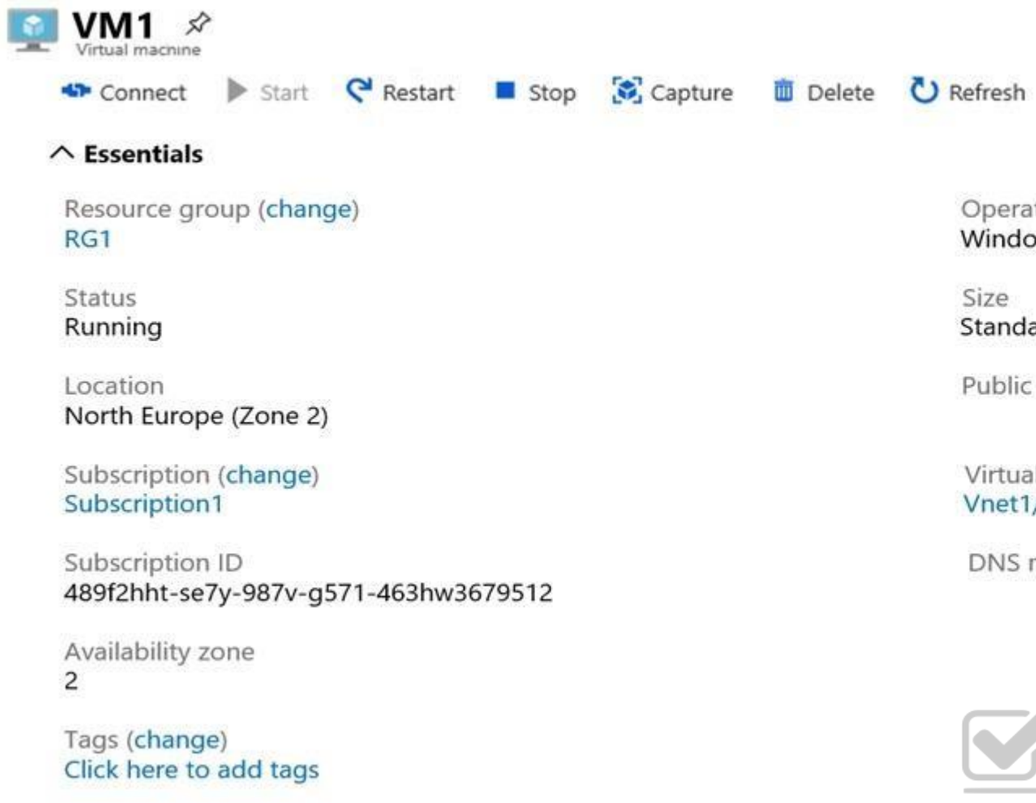
QUESTION 10
HOTSPOT

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

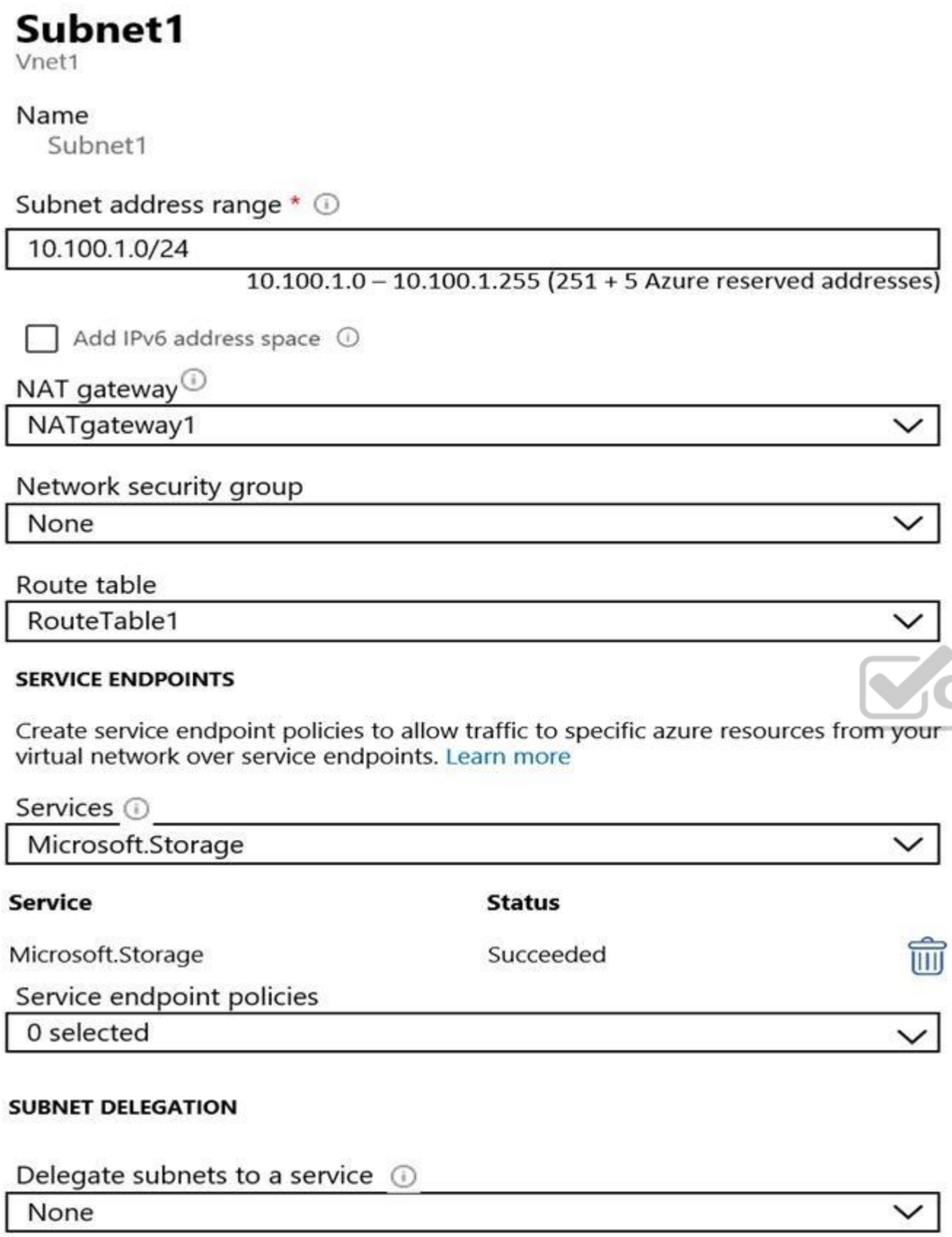
You have the NAT gateway shown in the NATgateway1 exhibit.



You have the virtual machine shown in the VM1 exhibit.



Subnet1 is configured as shown in the Subnet1 exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: No
VM1 is in Zone2 whereas the NAT Gateway is in Zone1. The VM would need to be in the same zone as the NAT Gateway to be able to use it. Therefore, VM1 cannot use the NAT gateway.

Box 2: Yes
NATgateway1 is configured in the settings for Subnet2.

Box 3: No
The NAT gateway does not have a single public IP address, it has an IP prefix which means more than one IP address. The VMs the use the NAT Gateway can use different public IP addresses contained within the IP prefix.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource

QUESTION 11
You have an Azure application gateway named AppGW1 that balances requests to a web app named App1.

You need to modify the server variables in the response header of App1.

What should you configure on AppGW1?

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

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 12 You have an Azure Virtual Desktop deployment that has 500 session hosts.

All outbound traffic to the internet uses a NAT gateway.

During peak business hours. some users report that they cannot access internet resources. In Azure Monitor, you discover many failed SNAT connections.

You need to increase the available SNAT connections.

What should you do?

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

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 13
You have an Azure subscription that contains the public IPv4 addresses shown in the following table.

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

You plan to create a load balancer named LB1 that will have the following settings:

Name: LB1
Location: West US
Type: Public
SKU: Standard

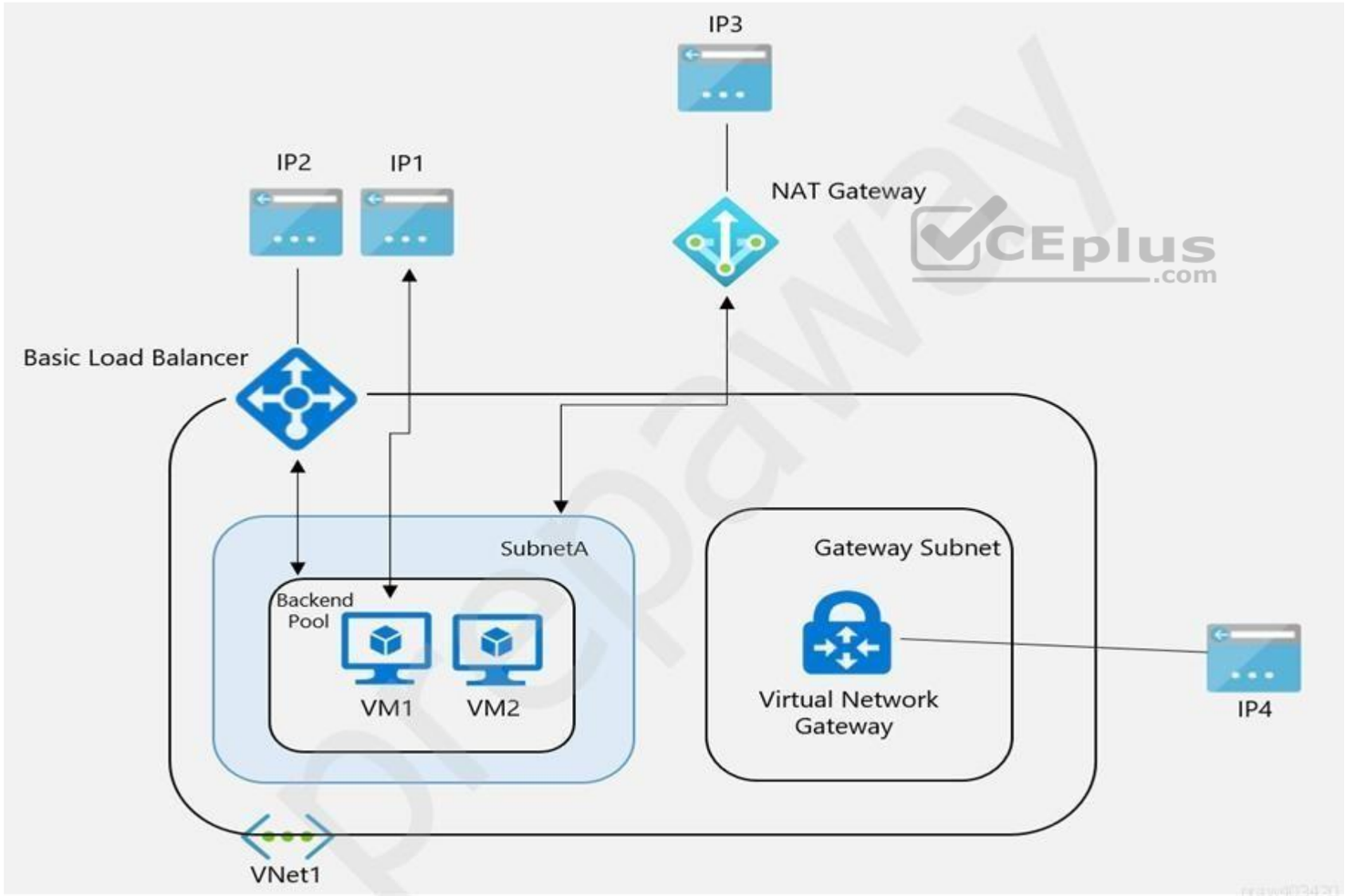
Which public IPv4 addresses can be used by LB1?

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

Correct Answer: F
Section: [none]
Explanation

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

QUESTION 14
You have the Azure environment shown in the exhibit.



VM1 is a virtual machine that has an instance-level public IP address (ILPIP).

Basic Load Balancer uses a public IP address. VM1 and VM2 are in the backend pool.

NAT Gateway uses a public IP address named IP3 that is associated to SubnetA.

VNet1 has a virtual network gateway that has a public IP address named IP4.

When initiating outbound traffic to the internet from VM1, which public address is used?

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

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 15
You are configuring two network virtual appliances (NVAs) in an Azure virtual network. The NVAs will be used to inspect all the traffic within the virtual network.

You need to provide high availability for the NVAs. The solution must minimize administrative effort.

What should you include in the solution?

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

Correct Answer: A
Section: [none]
Explanation

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

QUESTION 16 You have five virtual machines that run Windows Server. Each virtual machine hosts a different web app.

You plan to use an Azure application gateway to provide access to each web app by using a hostname of www.contoso.com and a different URL path for each web app, for example: https://www.contoso.com/app1.

You need to control the flow of traffic based on the URL path.

What should you configure?

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

Correct Answer: C
Section: [none]
Explanation
Explanation/Reference:
Reference:

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

QUESTION 17
You plan to publish a website that will use an FQDN of www.contoso.com. The website will be hosted by using the Azure App Service apps shown in the following table.

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

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

You need to ensure that Traffic Manager routes traffic for www.contoso.com.

Which DNS record should you create?

A. two A records that map www.contoso.com to 131.107.100.1 and 131.107.200.1
B. a CNAME record that maps www.contoso.com to TMprofile1.azurefd.net
C. a CNAME record that maps www.contoso.com to TMprofile1.trafficmanager.net
D. a TXT record that contains a string of as1.contoso.com and as2.contoso.com in the details

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/quickstart-create-traffic-manager-profile https://docs.microsoft.com/en-us/azure/app-service/configure-domain-traffic-manager

QUESTION 18
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

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

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

```
{
 "timeStamp": "2021-06-02T18:13:45+00:00",
 "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
 "operationName": "ApplicationGatewayFirewall",
 "category": "ApplicationGatewayFirewallLog",
 "properties": {
   "instanceId": "appgw_0",
   "clientIp": "137.135.10.24",
   "clientPort": "",
   "requestUri": "/login",
   "ruleSetType": "OWASP_CRS",
   "ruleSetVersion": "3.0.0",
   "ruleId": "920300",
   "message": "Request Missing an Accept Header",
   "action": "Matched",
   "site": "Global",
   "details": {
     "message": "Warning. Match of \\\"pm AppleWebKit Android\\\" against \\\"REQUEST_HEADER:User-Agent\\\" required. ",
     "data": "",
     "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
     "line": "1247"
   },
   "hostname": "app1.contoso.com",
   "transactionId": "f7546159y1hjk7wa114568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


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

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

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Testlet 1

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

Overview

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

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

Existing Environment

Azure Network Infrastructure

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

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

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

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

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

Azure Private DNS Zones

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

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

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

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

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

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

Requirements

Virtual Network Requirements

Contoso has the following virtual network requirements:

▪ Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
- Two container groups that connect to Vnet6
- Three virtual machines that connect to Vnet6
- Allow VPN connections to be established to Vnet6
- Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network.

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

Security Requirements

Contoso has the following network security requirements:

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

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

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

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

QUESTION 1
HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct 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	◯	◯

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: No
NSG10 which is attached to VM1's subnet blocks RDP (port TCP 3389) to 'Any' which means the port is blocked to all destinations.

Box 2: Yes
NSG10 blocks ICMP from VNet4 (source 10.10.0.0/16) but it is not blocked from VM2's subnet (VNet1/Subnet2).

Box 3: No
NSG11 blocks RDP (port TCP 3389) destined for 'VirtualNetwork'. VirtualNetwork is a service tag and means the address space of the virtual network (VNet1) which in this case is 10.1.0.0/16. Therefore, RDP traffic from subnet2 to anywhere else in VNet1 is blocked.

Testlet 2

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

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

Overview

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

Existing Environment

Hybrid Environment

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

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

Azure Environment

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

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

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 can be resolved from the on-premises locations.
- Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.
- Minimize the size of the subnets allocated to platform-managed services.
- Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements

Litware identifies the following hybrid networking requirements:

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

PaaS Networking Requirements

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

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

QUESTION 1
HOTSPOT

You need to restrict traffic from VMScaleSet1 to VMScaleSet2. The solution must meet the virtual networking requirements.

What is the minimum number of custom NSG rules and NSG assignments required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 2: One NSG

The minimum requirement is one NSG. You could attach the NSG to VMScaleSet1 and restrict outbound traffic, or you could attach the NSG to VMScaleSet2 and restrict inbound traffic. Either way you would need two custom NSG rules.

Box 1: Two custom rules
With the NSG attached to VMScaleSet2, you would need to create a custom rule blocking all traffic from VMScaleSet1. Then you would need to create another custom rule with a higher priority than the first rule that allows traffic on port 443.
The default rules in the NSG will allow all other traffic to VMScaleSet2.

Question Set 3

QUESTION 1
You have an Azure virtual network that contains the subnets shown in the following table.

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

You deploy an Azure firewall to AzureFirewallSubnet. You route all traffic from Subnet2 through the firewall.

You need to ensure that all the hosts on Subnet2 can access an external site located at https://*.contoso.com.

What should you do?

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

Correct Answer: D
Section: [none]
Explanation

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

QUESTION 2 You have an Azure Web Application Firewall (WAF) policy in prevention mode that is associated to an Azure Front Door instance.

You need to configure the policy to meet the following requirements:

Log all connections from Australia.
Deny all connections from New Zealand.
Deny all further connections from a network of 131.107.100.0/24 if there are more than 100 connections during one minute.

What is the minimum number of objects you should create?

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

Correct Answer: A
Section: [none]
Explanation

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

QUESTION 3 You have an Azure subscription that contains multiple virtual machines in the West US Azure region.

You need to use Traffic Analytics.

Which two resources should you create? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct answer selection is worth one point.

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

Correct Answer: BC
Section: [none]
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

QUESTION 4
HOTSPOT

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

Name	Connected to
VM1	Vnet1/Subnet1
VM2	Vnet1/Subnet2

Subnet1 and Subnet2 are associated to a network security group (NSG) named NSG1 that has the following outbound rule:

Priority: 100
Port: Any
Protocol: Any
Source: Any
Destination: Storage
Action: Deny

You create a private endpoint that has the following settings:

Name: Private1
Resource type: Microsoft.Storage/storageAccounts
Resource: storage1
Target sub-resource: blob
Virtual network: Vnet1 Subnet:
Subnet1

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1	◯	◯
From VM1, you can upload data to a blob storage container in storage1	◯	◯
From VM2, you can upload data to a blob storage container in storage1	◯	◯

Correct Answer:

Answer Area

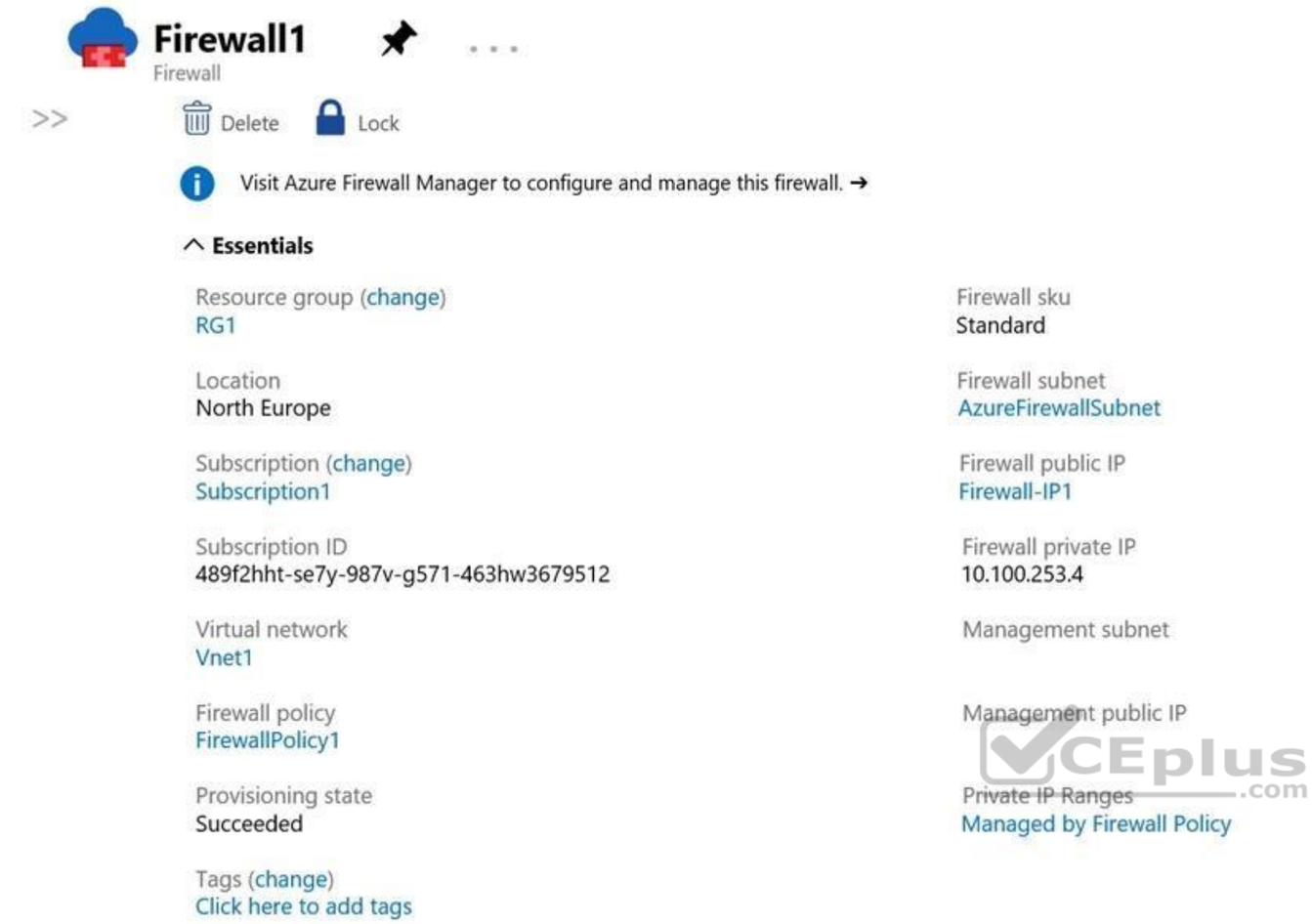
Statements	Yes	No
From VM2, you can create a container in storage1	◯	◯
From VM1, you can upload data to a blob storage container in storage1	◯	◯
From VM2, you can upload data to a blob storage container in storage1	◯	◯

Section: [none]
Explanation

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

QUESTION 5
HOTSPOT

You have an Azure firewall shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

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

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

Correct Answer:

Answer Area

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

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

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

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

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1:
If forced tunneling was enabled, the Firewall Subnet would be named AzureFirewallManagementSubnet. Forced tunneling can only be enabled during the creation of the firewall. It cannot be enabled after the firewall has been deployed.

Box 2:
The “Visit Azure Firewall Manager to configure and manage this firewall” link in the exhibit shows that the firewall is managed by Azure Firewall Manager.

QUESTION 6 You have a hybrid environment that uses ExpressRoute to connect an on-premises network and Azure.

You need to log the uptime and the latency of the connection periodically by using an Azure virtual machine and an on-premises virtual machine.

What should you use?

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

Correct Answer: C
Section: [none]
Explanation

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

QUESTION 7 You have an Azure subscription that contains the following resources:

A virtual network named Vnet1
Two subnets named subnet1 and AzureFirewallSubnet
A public Azure Firewall named FW1
A route table named RT1 that is associated to Subnet1 A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

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

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 8
HOTSPOT

You have an Azure application gateway named AppGW1 that provides access to the following hosts:

www.adatum.com

www.contoso.com
www.fabrikam.com

AppGW1 has the listeners shown in the following table.

Name	Frontend IP address	Type	Host name
Listen1	Public	Multi site	www.contoso.com
Listen2	Public	Multi site	www.fabrikam.com
Listen3	Public	Multi site	www.adatum.com

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

Name	Policy mode	Custom rule		
		Priority	Condition	Association
Policy1	Prevention	50	If IP address does contain 131.107.10.15 then deny traffic.	Application gateway: AppGW1
Policy2	Detection	10	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen1
Policy3	Prevention	70	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
From 131.107.10.15, you can access www.contoso.com	◯	◯
From 131.107.10.15, you can access www.fabrikam.com	◯	◯
From 131.107.10.15, you can access www.adatum.com	◯	◯

Correct Answer:

Answer Area

Statements	Yes	No
From 131.107.10.15, you can access www.contoso.com	◯	◯
From 131.107.10.15, you can access www.fabrikam.com	◯	◯
From 131.107.10.15, you can access www.adatum.com	◯	◯

Section: [none]
Explanation

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

QUESTION 9
You have an Azure virtual network that contains a subnet named Subnet1. Subnet1 is associated to a network security group (NSG) named NSG1. NSG1 blocks all outbound traffic that is not allowed explicitly.

Subnet1 contains virtual machines that must communicate with the Azure Cosmos DB service.

You need to create an outbound security rule in NSG1 to enable the virtual machines to connect to Azure Cosmos DB.

What should you include in the solution?

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

Correct Answer: A
Section: [none]
Explanation

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

Testlet 1

Case Study

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

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

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

Overview

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

Existing Environment

Hybrid Environment

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

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

Azure Environment

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

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

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 can be resolved from the on-premises locations.
- Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.
- Minimize the size of the subnets allocated to platform-managed services.
- Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements

Litware identifies the following hybrid networking requirements:

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

PaaS Networking Requirements

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

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

QUESTION 1
HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

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

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

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

Correct Answer:

Answer Area

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

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

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

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

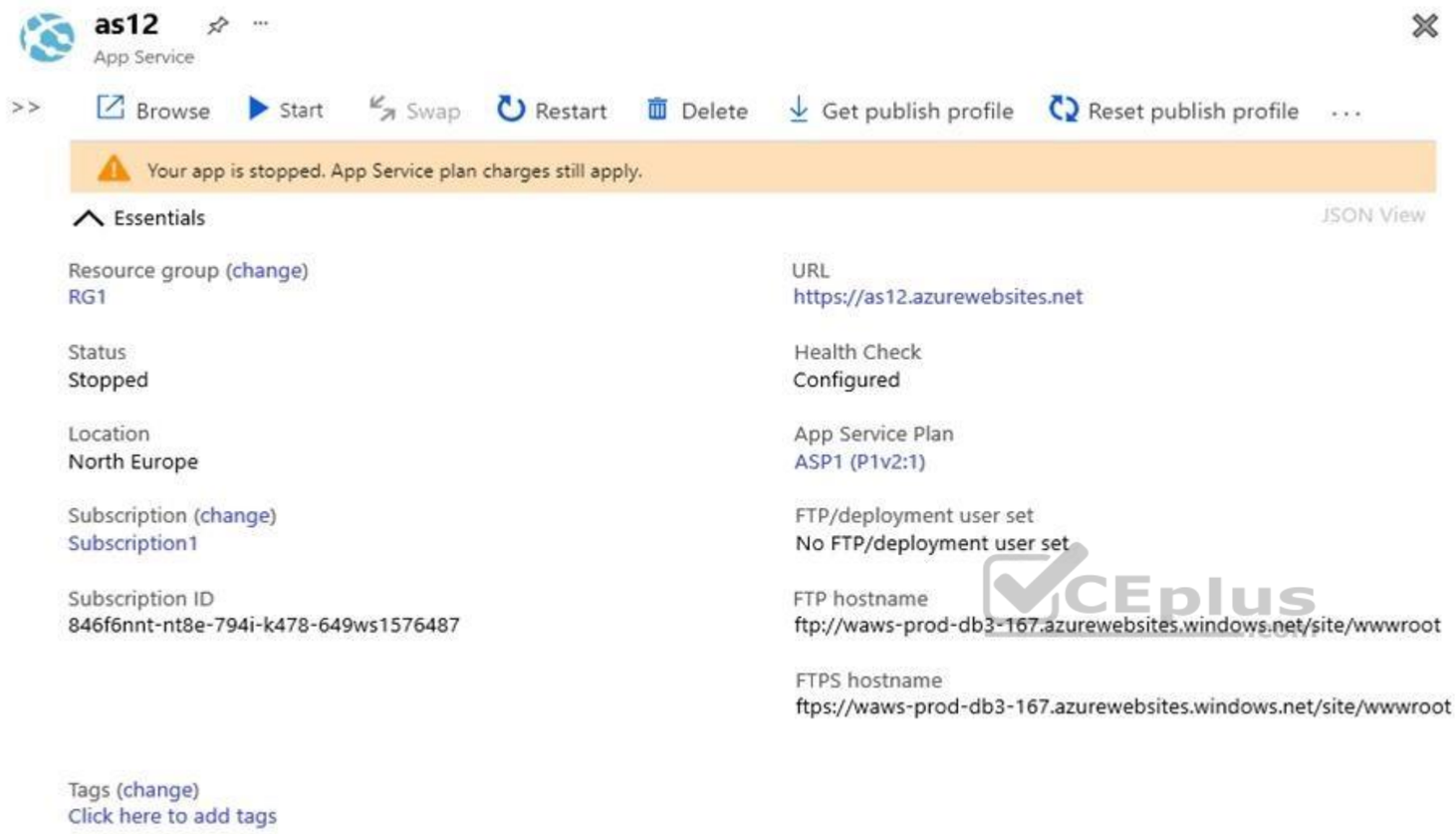
Section: [none]
Explanation

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

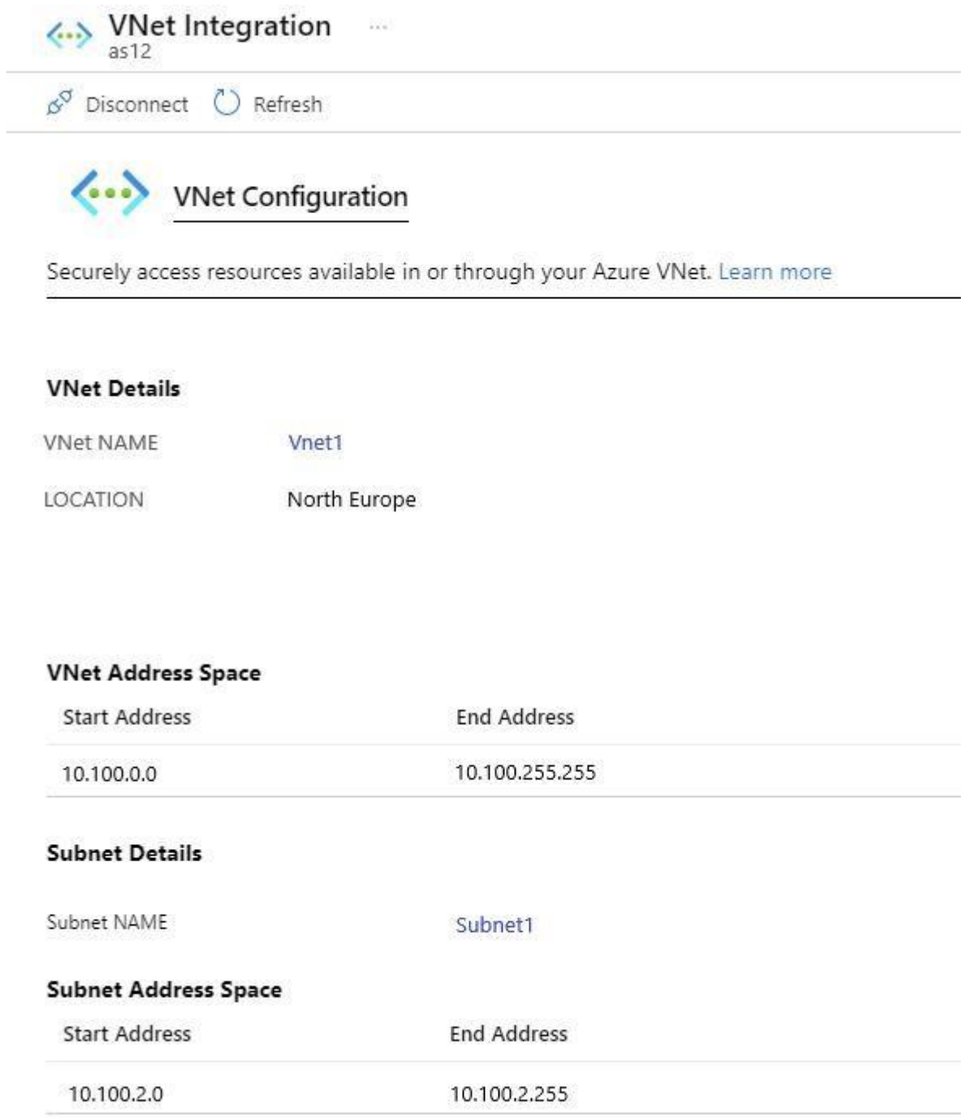
Question Set 2

QUESTION 1
HOTSPOT

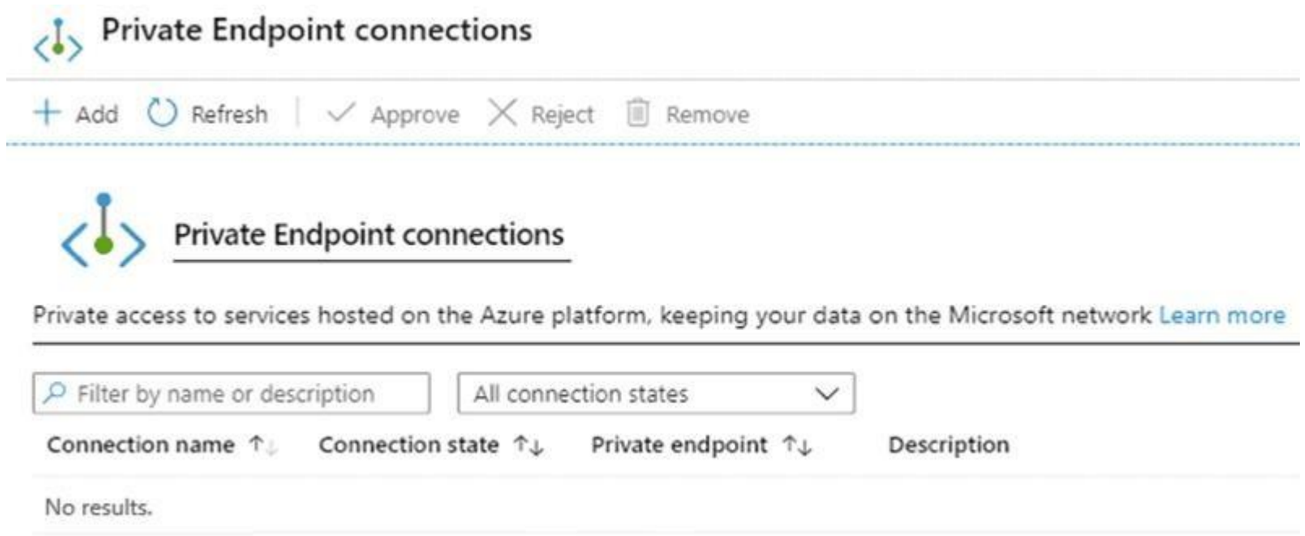
You have the Azure App Service app shown in the App Service exhibit.



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



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



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

Section: [none]
Explanation

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

QUESTION 2
DRAG DROP

You have an Azure virtual network named Vnet1 that connects to an on-premises network.

You have an Azure Storage account named storageaccount1 that contains blob storage.

You need to configure a private endpoint for the blob storage. The solution must meet the following requirements:

Ensure that all on-premises users can access storageaccount1 through the private endpoint. Prevent access to storageaccount1 from being interrupted.

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

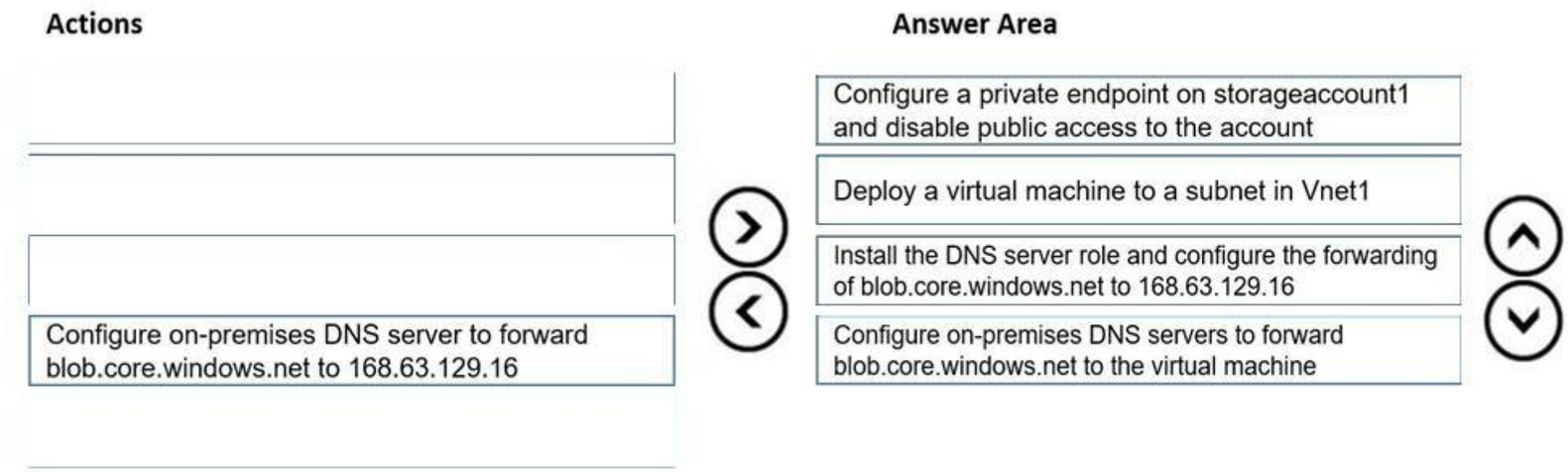
Select and Place:

Actions

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

Answer Area

Correct Answer:



Section: [none]
Explanation

Explanation/Reference:
Explanation:

168.63.129.16 is the IP address of Azure DNS which hosts Azure Private DNS zones. It is only accessible from within a VNet which is why we need to forward on-prem DNS requests to the VM running DNS in the VNet. The VM will then forward the request to Azure DNS for the IP of the storage account private endpoint.

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints

QUESTION 3
You have an Azure virtual network named Vnet1 that has one subnet. Vnet1 is in the West Europe Azure region.

You deploy an Azure App Service app named App1 to the West Europe region.

You need to provide App1 with access to the resources in Vnet1. The solution must minimize costs.

What should you do first?

A. Create a private link.
B. Create a new subnet.
C. Create a NAT gateway.
D. Create a gateway subnet and deploy a virtual network gateway.

Correct Answer: D
Section: [none]
Explanation

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

QUESTION 4
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The subscription contains the following resources:

An Azure App Service app named App1
An Azure DNS zone named contoso.com
An Azure private DNS zone named private.contoso.com A
virtual network named Vnet1

You create a private endpoint for App1. The record for the endpoint is registered automatically in Azure DNS.

You need to provide a developer with the name that is registered in Azure DNS for the private endpoint.

What should you provide?

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

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference: