

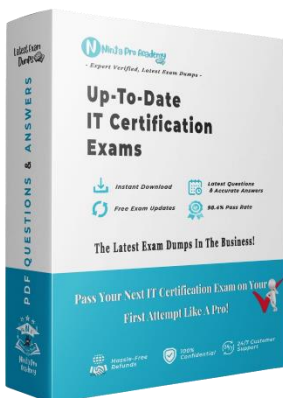


- Expert Verified, Latest Exam Dumps -

Microsoft

Latest AZ-700 Exam PDF Demo

Get Full AZ-700 Exam Questions & Answers



Vendor: Microsoft

Exam Code: AZ-700

Exam Name: Designing and Implementing Microsoft Azure Networking Solutions

Total Questions: 262 Q&A

Last Updated: 07-04-2024

<https://latestexamdumps.com/vendors/microsoft/microsoft-az-700-exam/>

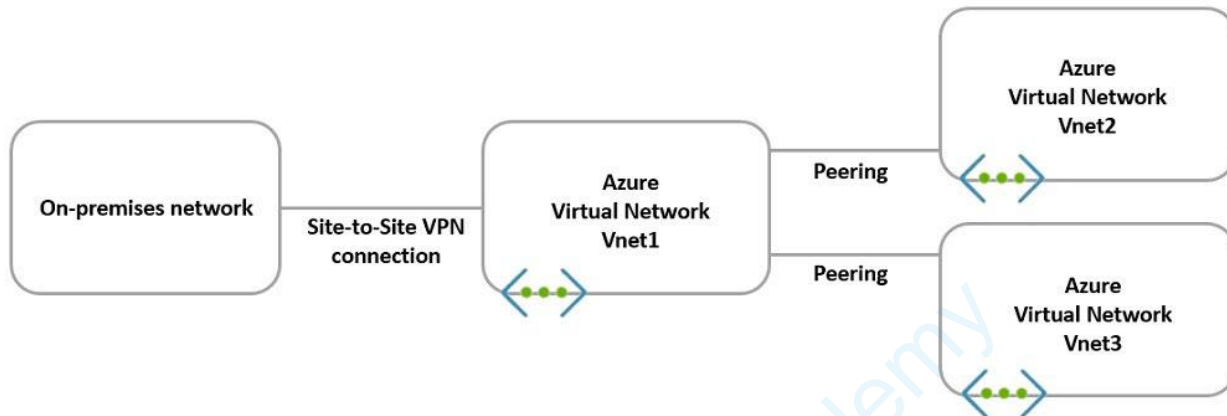


Our team regularly monitors exam updates from the vendor. At any time, you can access the member center to download the most recent updates. Our commitment is to continually enhance product quality and our level of service to ensure customer satisfaction. For any inquiries, please reach out to us at team@latestexamdumps.com and our expert team will provide support within 24 hours.

QUESTION 1

HOTSPOT -

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



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

Add peering ...

Vnet1

This virtual network

Peering link name *

Peering-Vnet1-Vnet2 ✓

Traffic to remote virtual network ⓘ

- ☒ Allow (default)
☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- ☒ Allow (default)
☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

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

Remote virtual network

Peering link name *

Peering-Vnet1-Vnet2 ✓

Virtual network deployment model ⓘ

- ☒ Resource manager
☐ Classic

☐ I know my resource ID ⓘ

Subscription* ⓘ

Subscription1 ✓

Virtual network

Vnet2 ✓

Traffic to remote virtual network ⓘ

- ☒ Allow (default)
☐ Block all traffic to the remote virtual network

Add

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

©NinjaProAcademy

Add peering ...

Vnet3

This virtual network

Peering link name *

Peering-Vnet1-Vnet3 ✓

Traffic to remote virtual network ⓘ

- ☒ Allow (default)
☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

- ☒ Allow (default)
☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

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

Remote virtual network

Peering link name *

Peering-Vnet1-Vnet3 ✓

Virtual network deployment model ⓘ

- ☒ Resource manager
☐ Classic

☐ I know my resource ID ⓘ

Subscription* ⓘ

Subscription1 ✓

Virtual network

Vnet1 ✓

Traffic to remote virtual network ⓘ

- ☒ Allow (default)
☐ Block all traffic to the remote virtual network

Traffic to remote virtual network

- ☒ Allow (default)
☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

- ☒ Allow (default)
☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server

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

Add

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

Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	<input type="radio"/>	<input type="radio"/>
The resources in Vnet2 can communicate with the resources in Vnet3.	<input type="radio"/>	<input type="radio"/>
The resources in Vnet2 can communicate with the resources in the on-premises network.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area:

Statements	Yes	No
The resources in Vnet2 can communicate with the resources in Vnet1.	<input checked="" type="radio"/>	<input type="radio"/>
The resources in Vnet2 can communicate with the resources in Vnet3.	<input type="radio"/>	<input checked="" type="radio"/>
The resources in Vnet2 can communicate with the resources in the on-premises network.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation/Reference:

Box 1: Yes -

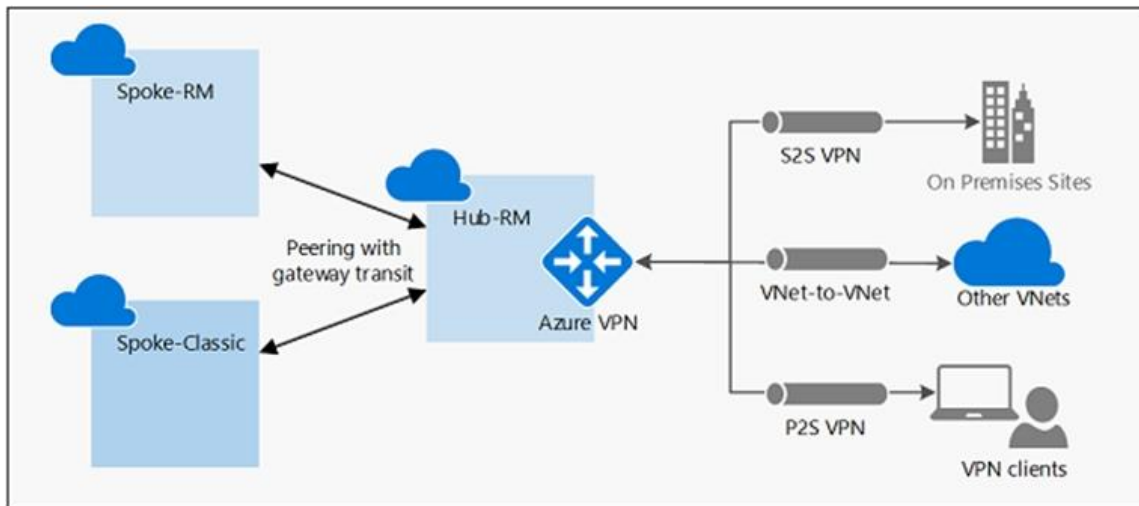
Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes.

Box 2: No -

No Virtual Gateway is used.

Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity.

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



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

Box 3: No -
No Virtual Gateway is used.

Reference:

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

QUESTION 2

You have an Azure virtual network named Vnet1 and an on-premises network. The on-premises network has policy-based VPN devices.

In Vnet1, you deploy a virtual network gateway named GW1 that uses a SKU of VpnGw1 and is route-based. You have a Site-to-Site VPN connection for GW1 as shown in the following exhibit.

 Save

 Discard

Use Azure Private IP Address ⓘ

Disabled Enabled

BGP ⓘ

Disabled Enabled

IPsec / IKE policy ⓘ

Default Custom

Use policy based traffic selector ⓘ

Enable Disable

DPD timeout in seconds * ⓘ

45

Connection Mode ⓘ

☒ Default ☐ InitiatorOnly ☐ ResponderOnly

IKE Protocol ⓘ
IKEv2

You need to ensure that the on-premises network can connect to the route-based GW1. What should you do before you create the connection?

- A. Set Connection Mode to ResponderOnly.
- B. Set BGP to Enabled.
- C. Set Use Azure Private IP Address to Enabled.
- D. Set IPsec / IKE policy to Custom.

Correct Answer: D

Explanation/Reference:

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

QUESTION 3

HOTSPOT

-

Your on-premises network contains a VPN device.

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

You need to create a Site-to-Site VPN connection that has a custom cryptographic policy.

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

NOTE: Each correct selection is worth one point.

Answer Area

```
...
$policy = New-AzIpssecPolicy
New-AzIpssecTrafficSelectorPolicy
New-AzServiceEndpointPolicy
New-AzVpnClientIpssecPolicy -IkeEncryption AES256 -IkeIntegrity SHA384 -DhGroup DHGroup24 -IpssecEncryption AES256
-IpssecIntegrity SHA256 -PfsGroup None -SALifeTimeSeconds 14400 -SADataSizeKilobytes 102400000
...
New-AzVirtualHub
New-AzVirtualNetworkGateway
New-AzVirtualNetworkGatewayConnection
New-AzVirtualNetworkGatewayNatRule -Name $Connection16 -ResourceGroupName $RG1 -VirtualNetworkGateway1 $vnet1gw
-LocalNetworkGateway2 $lng6 -Location $Location1 -ConnectionType IPsec -IpssecPolicies $policy -SharedKey 'AzureA1b2C3'
```

Answer:

Answer Area

```
...
$policy = New-AzIpssecPolicy
New-AzIpssecTrafficSelectorPolicy
New-AzServiceEndpointPolicy
New-AzVpnClientIpssecPolicy -IkeEncryption AES256 -IkeIntegrity SHA384 -DhGroup DHGroup24 -IpssecEncryption AES256
-IpssecIntegrity SHA256 -PfsGroup None -SALifeTimeSeconds 14400 -SADataSizeKilobytes 102400000
...
New-AzVirtualHub
New-AzVirtualNetworkGateway
New-AzVirtualNetworkGatewayConnection
New-AzVirtualNetworkGatewayNatRule -Name $Connection16 -ResourceGroupName $RG1 -VirtualNetworkGateway1 $vnet1gw
-LocalNetworkGateway2 $lng6 -Location $Location1 -ConnectionType IPsec -IpssecPolicies $policy -SharedKey 'AzureA1b2C3'
```

Explanation/Reference:

<https://learn.microsoft.com/en-us/powershell/module/az.network/new-azipsecpolicy?view=azps-9.2.0>

<https://learn.microsoft.com/en-us/powershell/module/az.network/new-azvirtualnetworkgatewayconnection?view=azps-9.2.0#example-1>

QUESTION 4

HOTSPOT

-

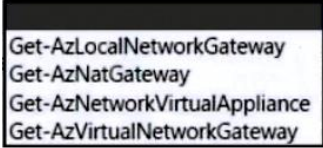
You have an Azure virtual network and an on-premises datacenter that connect by using a Site-to-Site VPN tunnel.

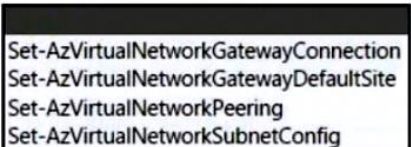
You need to ensure that all traffic from the virtual network to the internet is routed through the datacenter.

How should you complete the PowerShell script to configure forced tunneling? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


Answer Area

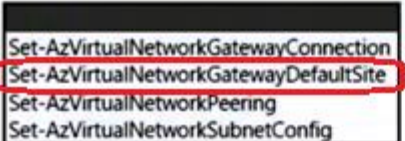
```
$force1 =  -Name "HQ" -ResourceGroupName "ForcedTunneling"

$force2 = Get-AzVirtualNetworkGateway -Name "Gateway1" -ResourceGroupName "ForcedTunneling"
 -GatewayDefaultSite $force1 -VirtualNetworkGateway $force2
```

Answer:

Answer Area

```
$force1 =  -Name "HQ" -ResourceGroupName "ForcedTunneling"

$force2 = Get-AzVirtualNetworkGateway -Name "Gateway1" -ResourceGroupName "ForcedTunneling"
 -GatewayDefaultSite $force1 -VirtualNetworkGateway $force2
```

Explanation/Reference:

<https://learn.microsoft.com/en-us/powershell/module/az.network/set-azvirtualnetworkgatewaydefaultsite?view=azps-9.2.0>

QUESTION 5

You have an Azure subscription that contains a virtual network.

You plan to deploy an Azure VPN gateway and 90 Site-to-Site VPN connections. The solution must meet the following requirements:

- Ensure that the Site-to-Site VPN connections remain available if an Azure datacenter fails.
- Minimize costs.

Which gateway SKU should you specify?

- A. VpnGw1AZ
- B. VpnGw2AZ
- C. VpnGw4AZ
- D. VpnGw5AZ

Correct Answer: C

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#benchmark>

QUESTION 6

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

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

To enter your password, place your cursor in the Enter password box and click on the password below.

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

Azure Password: xxxxxxxxxx

-

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

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You are preparing to connect your on-premises network to VNET4 by using a Site-to-Site VPN. The on-premises endpoint of the VPN will be created on a firewall named Firewall1.

The on-premises network has the following configuration:

- internal address range: 10.10.0.0/16
- Firewall1 internal IP address: 10.10.1.1
- Firewall public IP address: 131.107.50.60

BGP is NOT used.

You need to create the object that will provide the IP addressing configuration of the on-premises network to the Site-to-Site VPN. You do NOT need to create a virtual network gateway to complete this task.

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

Answer:

Create a site-to-site VPN connection in the Azure portal
We only create a local network gateway

The local network gateway is a specific object that represents your on-premises location (the site) for routing purposes. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you'll create a connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. If your on-premises network changes or you need to change the public IP address for the VPN device, you can easily update the values later.

Step 1: From the Azure portal, in Search resources, services, and docs (G+) type local network gateway. Locate local network gateway under Marketplace in the search results and select it. This opens the Create local network gateway page.

Step 2: On the Create local network gateway page, on the Basics tab, specify the values for your local network gateway.

* Select Endpoint type: IP address

* Endpoint: Enter 131.107.50.60 (The Firewall public IP address)

(IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device, select the IP address option and fill in the IP address as shown in the example. This is the public IP address of the VPN device that you want Azure VPN gateway to connect to. If you don't have the IP address right now, you can use the values shown in the example, but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure won't be able to connect.)

* Address Space: Enter 10.10.0.0/16 (The internal address range)

Select the endpoint type for the on-premises VPN device - IP address or FQDN (Fully Qualified Domain Name).

IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device.

[Home](#) >

Create local network gateway

Basics Advanced Review + create

A local network gateway is a specific object that represents an on-premises location (the site) for routing purposes. [Learn more.](#)

Project details

Subscription * Content Development
Resource group * TestRG1
[Create new](#)

Instance details

Region * East US
Name * Site1
Endpoint IP address FQDN
IP address * 4.3.2.1
Address space

10.0.0.0/24
20.0.0.0/24
[Add additional address range](#)

[Review + create](#)

[Previous](#)

[Next: Advanced >](#)

Step 3: On the Advanced tab, you can configure BGP settings if needed. Skip this.

Step 4: When you have finished specifying the values, select Review + create at the bottom of the page to validate the page.

Step 5: Select Create to create the local network gateway object.

Reference:

<https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal>

QUESTION 7

SIMULATION



Username and password

-

Use the following login credentials as needed:

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

To enter your password, place your cursor in the Enter password box and click on the password below.

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

Azure Password: xxxxxxxxxx

-

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

The following information is for technical support purposes only:

Lab Instance: 12345678

-

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

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

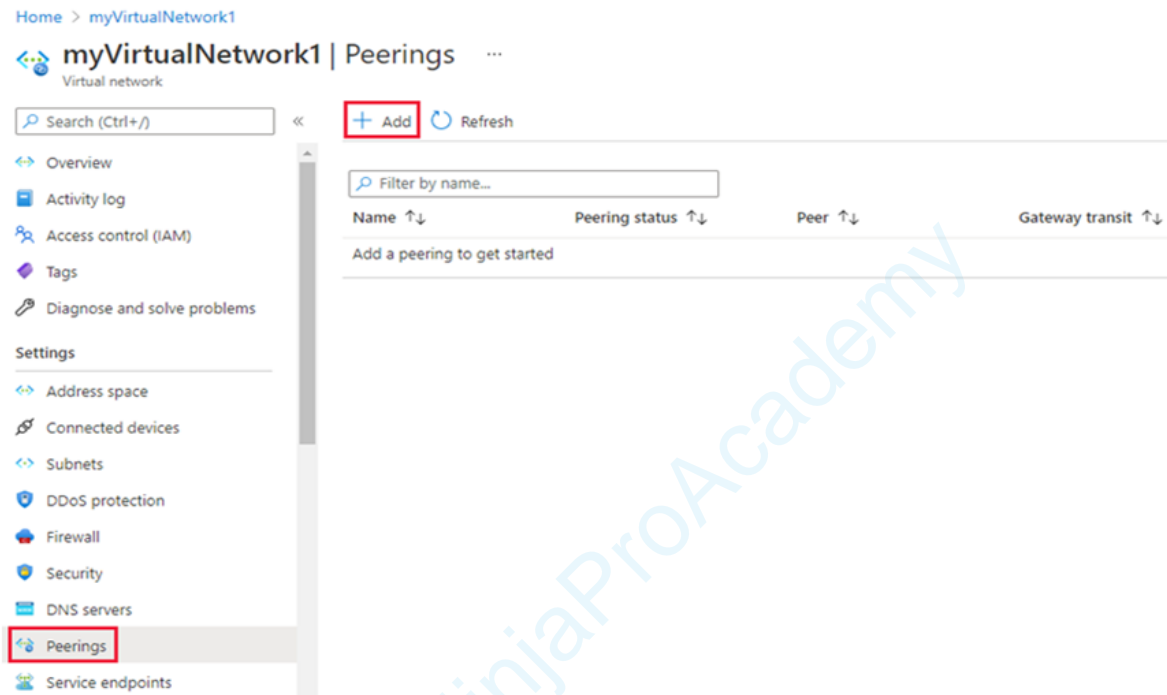
Answer:

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

Peer virtual networks

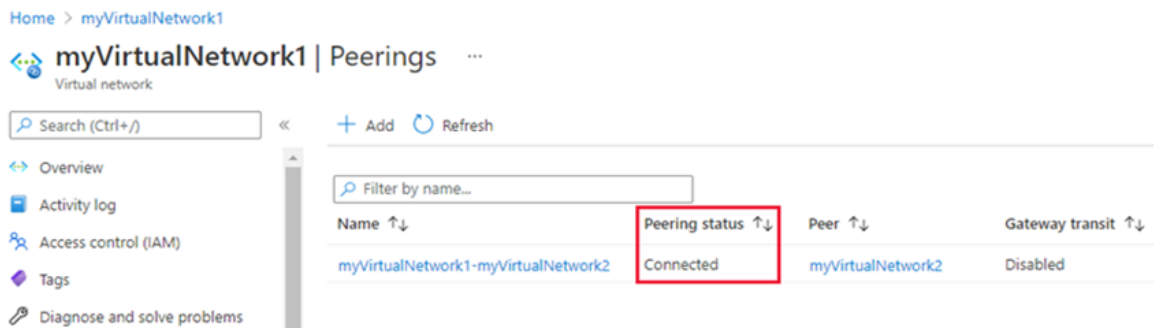
Step 1: In the search box at the top of the Azure portal, look for VNET2. When VNET2 appears in the search results, select it.

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



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

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



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

Reference:

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

QUESTION 8

HOTSPOT

-

You have an Azure subscription that contains a virtual network gateway named VNetGwy1. VNetGwy1 has a public IP address of 20.25.32.214.

You need to query the health probe of VNetGwy1.

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

NOTE: Each correct selection is worth one point.

Answer Area

://20.25.32.214: /healthprobe

http	80
https	443
snmp	8081

Answer:

Answer Area

://20.25.32.214: /healthprobe

http	80
https	443
snmp	8081

Explanation/Reference:

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

QUESTION 9

Case Study -

Overview -

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

Existing Environment -

Hybrid Environment -

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

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

Azure Environment -

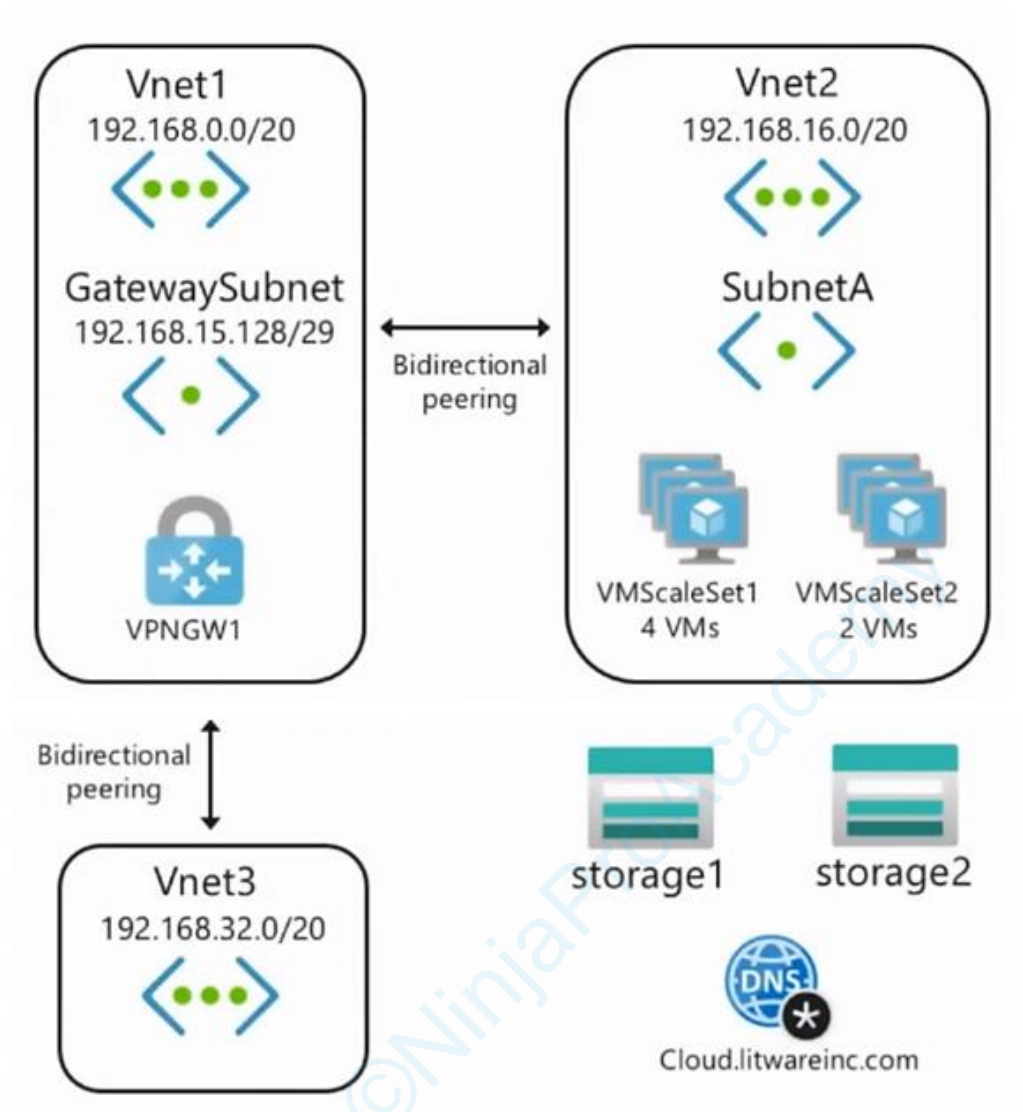
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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

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

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

Azure Network Diagram -



Requirements -

Business Requirements -

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

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

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

- Minimize the size of the subnets allocated to platform-managed services.
- Allow traffic from VMSSet1 to VMSSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

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

PaaS Networking Requirements -

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

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

You need to connect Vnet2 and Vnet3. The solution must meet the virtual networking requirements and the business requirements.

Which two actions should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. On the peering from Vnet1, select Allow for Traffic forwarded from remote virtual network.
- B. On the peerings from Vnet2 and Vnet3, select Allow for Traffic forwarded from remote virtual network.
- C. On the peering from Vnet1, select Use the remote virtual network's gateway or Route Server.
- D. On the peering from Vnet1, select Allow for Traffic to remote virtual network.
- E. On the peerings from Vnet2 and Vnet3, select Use the remote virtual network's gateway or Route Server.

Correct Answer: BE

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering?tabs=peering-portal#create-a-peering>
<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>

QUESTION 10

HOTSPOT

-

You have an Azure subscription.
 You have an Azure subscription.

You plan to use Azure Virtual WAN.

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

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

- Minimizes costs

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

NOTE: Each correct selection is worth one point.

Answer Area

For the S2S VPN gateway:

▼
2
4
8
16

For the ExpressRoute gateway:

▼
2
4
8
16

Answer:

Answer Area

For the S2S VPN gateway:

2
4
8
16

For the ExpressRoute gateway:

2
4
8
16

Explanation/Reference:

For S2S 1 scale unit = 500 Mbps

$4000/500 = 8$ scale units

<https://learn.microsoft.com/en-us/azure/virtual-wan/gateway-settings#s2s>

For ExpressRoute 1 scale unit = 2Gbps

$8/2 = 4$

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-expressroute-about#expressroute-performance>

QUESTION 11

DRAG DROP

-

You have an on-premises network.

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

You need to connect VNet1 to the on-premises network by using an ExpressRoute circuit.

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.

Actions

Configure Azure public peering.

Create a connection from VNet1 to the ExpressRoute circuit.

Create the ExpressRoute circuit.

Configure Azure private peering.

Send a service key to your connectivity provider.

Answer Area

1

2

3

4

Answer:**Answer Area**

1

Create the ExpressRoute circuit.

2

Send a service key to your connectivity provider.

3

Configure Azure private peering.

4

Create a connection from VNet1 to the ExpressRoute circuit.

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager#create-a-new-expressroute-circuit>

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-circuit-portal-resource-manager#send-the-service-key-to-your-connectivity-provider-for-provisioning>

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager#prerequisites>

QUESTION 12

You have three on-premises networks.

You have an Azure subscription that contains a Basic Azure virtual WAN. The virtual WAN contains a single virtual hub and a virtual network gateway that is limited to a throughput of 1 Gbps.

The on-premises networks connect to the virtual WAN by using Site-to-Site (S2S) VPN connections.

You need to increase the throughput of the virtual WAN to 3 Gbps. The solution must minimize administrative effort.

What should you do?

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

Correct Answer: D

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/virtual-wan/gateway-settings#s2s>

QUESTION 13

You have 10 on-premises networks that are connected by using a 3rd party Software Defined Wide Area Network (SD-WAN) solution. You have an Azure subscription that contains five virtual networks.

You plan to connect the Azure virtual networks and the on-premises networks by using an Azure Virtual WAN with a single virtual WAN hub.

You need to ensure that the Azure Virtual WAN can act as a node in the 3rd party SD-WAN solution.

What should you include in the solution?

- A. An Azure Virtual WAN ExpressRoute gateway
- B. A Network Virtual Appliance (NVA)
- C. A Site to site gateway (VPN gateway)
- D. A Point to site gateway (User VPN gateway)

Correct Answer: B

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/virtual-wan/sd-wan-connectivity-architecture#direct-nva>

QUESTION 14

HOTSPOT

-

You have the Azure resources shown in the following table.

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

You need to link VNet2 to Circuit1.

What should you create in each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sub1:

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

Sub2:

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

Answer:

Answer Area

Sub1: ▼

- A new ExpressRoute circuit
- An ExpressRoute circuit connection
- An ExpressRoute circuit connection authorization**

Sub2: ▼

- A new ExpressRoute circuit
- An ExpressRoute circuit connection**
- An ExpressRoute circuit connection authorization

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-classic#administration>

QUESTION 15

HOTSPOT

-

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

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

You establish BGP peering between NVA1 and Hub1.

You need to implement transit connectivity between VNet1 and VNet3 via Hub1 by using BGP peering. The solution must minimize costs.

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

NOTE: Each correct selection is worth one point.

Answer Area

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

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

On VNet3, implement:

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

Answer:

Answer Area

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

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

On VNet3, implement:

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

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/virtual-wan/scenario-bgp-peering-hub>

QUESTION 16

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

Explanation/Reference:

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

QUESTION 17

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 (Azure AD DS)
- C. Azure Private Link
- D. Azure Application Gateway v2
- E. VPN gateway

Correct Answer: ADE

Explanation/Reference:

<https://docs.microsoft.com/en-us/azure/bastion/bastion-overview#architecture>

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

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsub>

QUESTION 18

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:

Answer Area

Virtual WAN type:

	▼
Basic	
Standard	

Number of scale units:

	▼
2	
4	
6	
8	

Answer:

Answer Area

Virtual WAN type:

	▼
Basic	
Standard	

Number of scale units:

	▼
2	
4	
6	
8	

Explanation/Reference:

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

QUESTION 19**HOTSPOT -**

You have an Azure subscription.

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

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

You plan to deploy Azure Virtual WAN.

You are evaluating Virtual WAN Basic and Virtual WAN Standard.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Virtual WAN Basic:

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

Virtual WAN Standard:

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

Answer:

Answer Area

Virtual WAN Basic:

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

Virtual WAN Standard:

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

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about#basicstandard>

QUESTION 20

HOTSPOT -

You have an Azure subscription that contains two virtual networks named Vnet1 and Vnet2.

You register a public DNS zone named fabrikam.com. The zone is configured as shown in the Public DNS Zone exhibit.

Fabrikam.com
✕
...

DNS zone

+ Record set
 + Child zone
 → Move
 ✕ Delete zone
 ↺ Refresh

^ Essentials
 JSON View


Resource group (change) : rg1
 Subscription (change) : Subscription1
 Subscription ID : 169d1bba-ba4c-471c-b513-092eb7063265
 Name server 1 : ns1-06.azure-dns.com.
 Name server 2 : ns2-06.azure-dns.net.
 Name server 3 : ns3-06.azure-dns.org.
 Name server 4 : ns4-06.azure-dns.info.
 Tags (change) : [Click here to add tags](#)

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

🔍 Search record sets

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

You have a private DNS zone named fabrikam.com. The zone is configured as shown in the Private DNS Zone exhibit.


Fabrikam.com
Private DNS zone

[+ Record set](#)
[→ Move](#)
[Delete zone](#)
[Refresh](#)

Essentials
[JSON View](#)

Resource group ([change](#)) : rg1
Subscription ([change](#)) : Subscription1
Subscription ID : 169d1bba-ba4c-471c-b513-092eb7063265
Tags ([change](#)) : [Click here to add tags](#)

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

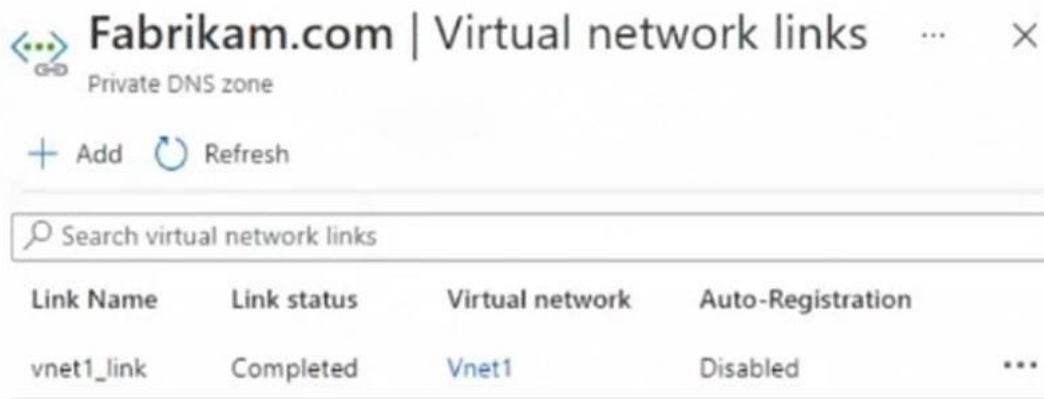
Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.co... Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False

Subscription ([change](#)) : Subscription1
Subscription ID : 169d1bba-ba4c-471c-b513-092eb7063265
Tags ([change](#)) : [Click here to add tags](#)

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

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.co... Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
appservice1	A	3600	131.107.100.10	False
server1	A	3600	131.107.100.1	False
server2	A	3600	131.107.100.2	False
server3	A	3600	131.107.100.3	False
www	CNAME	3600	appservice1.fabrikam.com	False

You have a virtual network link configured as shown in the Virtual Network Link exhibit.



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

Answer Area

Statements	Yes	No
Queries for www.fabrikam.com from the internet are resolved to 131.107.1.1.	<input type="radio"/>	<input type="radio"/>
Queries for server1.fabrikam.com can be resolved from the internet.	<input type="radio"/>	<input type="radio"/>
Queries for www.fabrikam.com from Vnet2 are resolved to 131. 107.100. 10.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Queries for www.fabrikam.com from the internet are resolved to 131.107.1.1.	<input checked="" type="radio"/>	<input type="radio"/>
Queries for server1.fabrikam.com can be resolved from the internet.	<input type="radio"/>	<input checked="" type="radio"/>
Queries for www.fabrikam.com from Vnet2 are resolved to 131. 107.100. 10.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation/Reference:

Box 1: Yes -

DNS queries from the internet use the public DNS zone. In the public DNS zone, www.fabrikam.com is a CNAME record that resolves to appservice1.fabrikam.com which resolves to 131.107.1.1.

Box 2: No -

DNS queries from the internet use the public DNS zone. There is no DNS record for server1.fabrikam.com in the public DNS zone.

Box 3: No -

The private DNS zone is linked to VNet1, not VNet2. Therefore, resources in VNet2 cannot query the private DNS zone.

QUESTION 21

You have an application named App1 that listens for incoming requests on a preconfigured group of 50 TCP ports and UDP ports.

You install App1 on 10 Azure virtual machines.

You need to implement load balancing for App1 across all the virtual machines. The solution must minimize the number of load balancing rules.

What should you include in the solution?

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

Correct Answer: C

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview>

QUESTION 22

HOTSPOT

-

You have two Azure App Service instances that host the web apps shown the following table.

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

You deploy an Azure 2 that has one public frontend IP address and two backend pools.

You need to publish all the web apps to the application gateway. Requests must be routed based on the HTTP host headers.

What is the minimum number of listeners and routing rules you should configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Listeners:

0
1
2
3
4

Routing rules:

0
1
2
3
4

Answer:

Answer Area

Listeners:

0
1
2
3
4

Routing rules:

0
1
2
3
4

Explanation/Reference:

<https://learn.microsoft.com/en-us/training/modules/configure-azure-application-gateway/3-determine-routing>

QUESTION 23

Your company has four branch offices and an Azure subscription. The subscription contains an Azure VPN gateway named GW1.

The branch offices are configured as shown in the following table.

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

The branch office routers provide internet connectivity and Site-to-Site VPN connections to GW1.

The users in Branch1 report that they can connect to internet resources, but cannot access Azure resources.

You need to ensure that the Branch1 users can connect to the Azure resources. The solution must meet the following requirements:

- Minimize downtime for all users.
- Minimize administrative effort.

What should you do first?

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

Correct Answer: C

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/vpn-gateway/reset-gateway>

QUESTION 24

DRAG DROP

-

You have an Azure subscription that contains a virtual network named Vnet1 and an Azure SQL database named SQL1. SQL1 has a private endpoint on Vnet1.

You have a partner company named Fabrikam, Inc. Fabrikam has an Azure subscription that contains a virtual network named Vnet2 and a virtual machine named VM1. VM1 is connected to Vnet2.

You need to provide VM1 with access to SQL1 by using an Azure Private Link service.

What should you implement on each virtual network? To answer, drag the appropriate resources to the correct virtual networks. Each resource may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Resources	Answer Area
A NAT gateway	
A peering link	Vnet1: <input type="text"/>
A private endpoint	Vnet2: <input type="text"/>
A service endpoint	
An Azure application gateway	
An Azure load balancer	

Answer:

Answer Area

Vnet1:

Vnet2:

Explanation/Reference:

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

QUESTION 25

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

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

You plan to deploy an Azure Virtual Network NAT gateway named Gateway1. The solution must meet the following requirements:

- VM1 will access the internet by using its public IP address.
- VM2 will access the internet by using its public IP address.
- Administrative effort must be minimized.

You need to ensure that you can deploy Gateway1 to Vnet1.

What is the minimum number of subnets required on Vnet1?

- A. 2
- B. 3
- C. 4

D. 5

Correct Answer: C

Explanation/Reference:

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

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#nat-gateway-and-basic-sku-resources>

QUESTION 26

HOTSPOT

-

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

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

You have a virtual machine named VM5 that has the following IP address configurations:

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

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

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

The virtual network links in the fabrikam.com DNS zone are configured as shown in the exhibit. (Click the Exhibit tab.)

fabrikam.com | Virtual network links

Private DNS zone

Search (Ctrl+/)

+ Add Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Virtual network links

Properties

Locks

Search virtual network links

Link Name	Link status	Virtual network	Auto-Registration
link1	Completed	vnet2	Enabled

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

Updating the IP address configurations of VM5 to use a DNS server address of 10.4.0.2 will enable the virtual machine to resolve app1.fabrikam.com.

☐☐

Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.

☐☐

Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.

☐☐

Answer:

Answer Area

Statements

Yes

No

Updating the IP address configurations of VM5 to use a DNS server address of 10.4.0.2 will enable the virtual machine to resolve app1.fabrikam.com.

☐☒

Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.

☒☐

Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.

☐☒

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/dns/dns-faq-private>

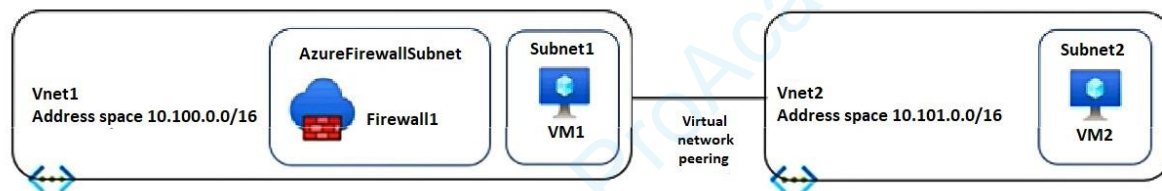
QUESTION 27**HOTSPOT**

-


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

Name	Type
Vnet1	Virtual network
Vnet2	Virtual network
Firewall1	Azure Firewall
Subnet1	Virtual subnet
Subnet2	Virtual subnet
VM1	Virtual machine
VM2	Virtual machine



The virtual network topology is shown in the following exhibit.




Firewall1 is configured as shown in following exhibit.


Firewall1
✎
...

Firewall

>>
 Delete
 Lock

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

^ Essentials

Resource group (change)
[RG1](#)

Location
North Europe

Subscription (change)
[Subscription1](#)

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

Virtual network
[Vnet1](#)

Firewall policy
[FirewallPolicy1](#)

Provisioning state
Succeeded

Tags (change)
[Click here to add tags](#)

Firewall sku
Standard

Firewall subnet
[AzureFirewallSubnet](#)

Firewall public IP
[Firewall1-IP1](#)

Firewall private IP
10.100.253.4

Management subnet
-

Management public IP
-

Private IP Ranges
Managed by Firewall Policy

FirewallPolicy1 contains the following rules:

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

No custom private endpoints, service endpoints, routing tables, or network security groups (NSGs) were created.

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

NOTE: Each correct selection is worth one point.

Answer Area	Statements	Yes	No
	A routing table must be associated with Subnet1 and Subnet2 to ensure that all internet traffic for VM1 and VM2 is sent via Firewall1.	<input type="radio"/>	<input type="radio"/>
	The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	<input type="radio"/>	<input type="radio"/>
	Firewall1 can be configured to limit access to websites by categories.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area	Statements	Yes	No
	A routing table must be associated with Subnet1 and Subnet2 to ensure that all internet traffic for VM1 and VM2 is sent via Firewall1.	<input checked="" type="radio"/>	<input type="radio"/>
	The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	<input type="radio"/>	<input checked="" type="radio"/>
	Firewall1 can be configured to limit access to websites by categories.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation/Reference:

Box 1: Yes.

- You need to add User Defined Route to the Firewall Appliance from the subnets.

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal>

Box 2: No.

- The firewall is not a VPN Gateway, and we do not have any connection with On-Premises.

<https://learn.microsoft.com/en-us/answers/questions/516530/how-to-set-up-a-multi-spoke-virtual-network-in-azu>

Box 3: Yes.

- Azure Firewall can filter by web categories.

<https://learn.microsoft.com/en-us/azure/firewall/web-categories>

QUESTION 28

HOTSPOT

-

You have an on-premises network.

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

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

You need to implement an ExpressRoute circuit to access the resources in the subscription. The solution must ensure that the on-premises network connects to the Azure resources by using the ExpressRoute circuit.

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

NOTE: Each correct selection is worth one point.

Answer Area

Connection to Vnet1:

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

Connection to SQL1:

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

Answer:

Answer Area

Connection to Vnet1:

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

Connection to SQL1:

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

Explanation/Reference:

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

QUESTION 29

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

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

You deploy Azure Firewall to Vnet3.

You need to ensure that the traffic from Subnet1-1 to Subnet2-1 passes through the firewall.

What should you configure?

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

Correct Answer: B

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route>

QUESTION 30

DRAG DROP

-

You have two on-premises datacenters.

You have an Azure subscription that contains four virtual networks named VNet1, VNet2, VNet3, and VNet4.

You create an Azure virtual WAN named VWAN1. VWAN1 contains a single virtual hub that is connected to both on-premises datacenters and all the virtual networks in a full mesh topology.

You create a route table named RT1.

You need to configure VWAN1 to meet the following requirements:

- Connectivity between VNet1 and VNet2 and both on-premises datacenters must be allowed.
- Connectivity between VNet3 and VNet4 and both on-premises datacenters must be allowed.
- VNet1 and VNet2 must be isolated from VNet3 and VNet4.

How should you configure routing for VNet1 and VNet2 and for both on-premises datacenters? To answer, drag the appropriate route tables and route table propagation to the correct requirements.

Each route table and route table propagation 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.

Route solutions

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

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

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

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

Answer Area

VNet1 and VNet2:

Route solution

On-premises datacenters:

Route solution

Answer:

Answer Area

VNet1 and VNet2:

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

On-premises datacenters:

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

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/virtual-wan/scenario-isolate-vnets>

QUESTION 31

DRAG DROP

-

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

Name	Type	Description
Gateway1	NAT gateway	Unconfigured
NIC1	Network interface	A network interface with a statically assigned public IP address named PIP1
PIP1	Public IP address	A Basic SKU public IP address
VNet1	Virtual network	Contains a subnet named Subnet1
Subnet1	Virtual subnet	Part of VNet1
VM1	Virtual machine	Connected to Subnet1 via NIC1

You need to associate Gateway1 with Subnet1. The solution must minimize downtime on VM1.

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

Actions

Disassociate PIP1 from NIC1.

Change the PIP1 SKU to Standard.

Change Assignment to Dynamic for PIP1.

Shutdown VM1.

Start VM1.

Associate PIP1 to NIC1.

Answer Area



Answer:

Actions**Answer Area**

Disassociate PIP1 from NIC1.

Change the PIP1 SKU to Standard.

Change Assignment to Dynamic for PIP1.

Shutdown VM1.

Start VM1.

Associate PIP1 to NIC1.

**Explanation/Reference:**

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

QUESTION 32

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

Explanation/Reference:

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

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

QUESTION 33

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

to an on-premises web server.

You plan to migrate the website to an Azure web app named Web1. The website on Web1 will be published by using an Azure Front Door instance named ContosoFD1.

You build the website on Web1.

You plan to configure ContosoFD1 to publish the website for testing.

When you attempt to configure a custom domain for `www.contoso.com` on ContosoFD1, you receive the error message shown in the exhibit. (Click the Exhibit tab.)

Add a custom domain ✕

Add a custom domain to your Front Door. Create a DNS mapping from your custom domain to the Front Door `azurefd.net` frontend host with your DNS provider. [Learn more](#)

Frontend host end

ContosoFD1.azurefd.net 

Custom host name * 

www.contoso.com



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

You need to test the website and ContosoFD1 without affecting user access to the on-premises web server. Which record should you create in the `contoso.com` DNS domain?

- A. a CNAME record that maps `afdverify.www.contoso.com` to `ContosoFD1.azurefd.net`
- B. a CNAME record that maps `www.contoso.com` to `ContosoFD1.azurefd.net`
- C. a CNAME record that maps `afdverify.www.contoso.com` to `afdverify.ContosoFD1.azurefd.net`
- D. a CNAME record that maps `www.contoso.com` to `Web1.contoso.com`

Correct Answer: C

Explanation/Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#map-the-temporary-afdverify-subdomain>

QUESTION 34

You have an internal Basic Azure Load Balancer named LB1 that has two frontend IP addresses. The backend pool of LB1 contains two Azure virtual machines named VM1 and VM2.

You need to configure the rules on LB1 as shown in the following table.

Rule	Frontend IP address	Protocol	ILB1 port	Destination	VM port
1	65.52.0.1	TCP	80	IP address of the NIC of VM1 and VM2	80
2	65.52.0.2	TCP	80	IP address of the NIC of VM1 and VM2	80

What should you do for each rule?

- A. Enable Floating IP.
- B. Disable Floating IP.
- C. Set Session persistence to Enabled.
- D. Set Session persistence to Disabled.

Correct Answer: A

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-multivip-overview#rule-type-2-backend-port-reuse-by-using-floating-ip>

QUESTION 35

HOTSPOT

-

You have an Azure load balancer that has the following configurations:

- Name: LB1
- Location: East US 2
- SKU: Standard
- Private IP address: 10.3.0.7
- Load balancing rule: rule1 (Tcp/80)
- Health probe: probe1 (Http:80)
- NAT rules: 0 inbound

The backend pool of LB1 has the following configurations:

- Name: backend1
- Virtual network: Vnet2
- Backend pool configuration: NIC
- IP version: IPv4
- Virtual machines: VM1, VM2, VM3

You have an Azure virtual machine named VM4 that has the following network configurations:

- Network interface: vm4981
- Virtual network/subnet: Vnet3/Subnet3
- NIC private IP address: 10.4.0.4
- Accelerated networking: Enabled

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
To add VM4 to LB1, you must create a new backend pool.	<input type="radio"/>	<input type="radio"/>
VM1 is connected to Vnet2.	<input type="radio"/>	<input type="radio"/>
Connections to HTTPS://10.3.0.7 will be load balanced between VM1, VM2, and VM3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
To add VM4 to LB1, you must create a new backend pool.	<input type="radio"/>	<input checked="" type="radio"/>
VM1 is connected to Vnet2.	<input checked="" type="radio"/>	<input type="radio"/>
Connections to HTTPS://10.3.0.7 will be load balanced between VM1, VM2, and VM3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation/Reference:

Box 1: No.

- You can have multiple backend pools, mix of IP backend pool or NIC backend pool, but they must be in the same VNET than the Loadbalancer. Backend pools must be in the same VNet than the Frontend IP. Therefore, a Loadbalancer cannot span multiple vnets.

Box 2: Yes.

- Loadbalancer backend pool is in VNet2 therefore, following the explanations above, all the VMS in the pool are in VNet 2. Therefore, VM1 which is in this backend pool is in VNet2.

Box 3: No.

- Load Balancing rule is set for port 80 which is the default HTTP port. HTTPS is 443. so HTTPS connections will not be handled by this Loadbalancer.

QUESTION 36

HOTSPOT

-

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

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

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

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

You need to configure a DNS record for www.fabrikam.com and upload the certificate to Azure.

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

NOTE: Each correct selection is worth one point.

Answer Area

Upload the certificate to:

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

Set the DNS record target to:

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

Answer:

Answer Area

Upload the certificate to:

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

Set the DNS record target to:

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

Explanation/Reference:

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

QUESTION 37

HOTSPOT

-

You have an Azure subscription that contains an app named App1. App1 is hosted on the Azure App Service instances shown in the following table.

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

You need to implement Azure Traffic Manager to meet the following requirements:

- App1 traffic must be assigned equally to each App Service instance in each Azure region.
- App1 traffic from North Europe must be routed to the App1 instances in the North Europe region.
- App1 traffic from North America must be routed to the App1 instances in the East US Azure region.
- If an App Service instance fails, all the traffic for that instance must be routed to the remaining instances in the same region.

How should you configure the Traffic Manager profiles? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of Traffic Manager profiles required:

1
2
3
4

Routing method for the traffic in each region:

Geographic
Performance
Priority
Weighted

Answer:

Answer Area

Minimum number of Traffic Manager profiles required:

1
2
3
4

Routing method for the traffic in each region:

Geographic
Performance
Priority
Weighted

Explanation/Reference:

One parent profile configured with geographical routing method; 2 child profiles configured with weighted routing method.

QUESTION 38

DRAG DROP

-

You have an Azure subscription.

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

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

- Block malicious bots.
- Throttle client IP addresses that exceed 100 connections per minute.

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

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

NOTE: Each correct selection is worth one point.

Options

A custom rule

A managed rule

Classic

Premium

Standard

Answer Area

SKU:

Option

Block malicious bots:

Option

Throttle client IP addresses:

Option

Answer:

Answer Area

SKU:

Premium

Block malicious bots:

A managed rule

Throttle client IP addresses:

A custom rule

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview>
<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-cdn-comparison#service-comparison:~:text=upgrade%20capability.~,Service%20comparison,-The%20following%20table>

QUESTION 39

Your company has offices in Montreal, Seattle, and Paris. The outbound traffic from each office originates from a specific public IP address.

You create an Azure Front Door instance named FD1 that has Azure Web Application Firewall (WAF) enabled.

You configure a WAF policy named Policy1 that has a rule named Rule1.

Rule1 applies a rate limit of 100 requests for traffic that originates from the office in Montreal.

You need to apply a rate limit of 100 requests for traffic that originates from each office.

What should you do?

- A. Modify the rate limit threshold of Rule1.
- B. Create two additional associations.
- C. Modify the conditions of Rule1.
- D. Modify the rule type of Rule1.

Correct Answer: C

Explanation/Reference:

You should adjust the conditions of Rule1 to include separate conditions for each office (Montreal, Seattle, and Paris) and set the rate limit to 100 requests for each condition. This ensures that traffic originating from each office is subjected to the specified rate limit.

<https://techcommunity.microsoft.com/t5/azure-network-security-blog/rate-limiting-feature-for-azure-waf-on-application-gateway-now/ba-p/3934957#:~:text=Rate%20limiting%20is%20configured%20using.and%20a%20group%20by%20variable.>

QUESTION 40

You have a network security group named NSG1.

You need to enable network security group (NS) flow logs for NSG1. The solution must support retention policies.

What should you create first?

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

Correct Answer: A

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview#how-nsg-flow-logs-work>

QUESTION 41

HOTSPOT

-

You have an Azure application gateway named AppGw1.

You need to create a rewrite rule for AppGw1. The solution must rewrite the URL of requests from <https://www.contoso.com/fashion/shirts> to <https://www.contoso.com/buy.aspx?category=fashion&product=shirts>.

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

NOTE: Each correct selection is worth one point.

If server variable

▼
content_type
query_string
uri_path

 equals to the pattern `/(.+)/(.+)`

Set

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

 to `buy.aspx` and `category={var_uri_path_1}&product={var_uri_path_2}`

Answer:

If server variable

▼
content_type
query_string
uri_path

 equals to the pattern `/(.+)/(.+)`

Set

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

 to `buy.aspx` and `category={var_uri_path_1}&product={var_uri_path_2}`

Explanation/Reference:

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

<https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-portal>

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

QUESTION 42

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains 20 subnets and 500 virtual machines.

Each subnet contains a virtual machine that runs network monitoring software.

You have a network security group (NSG) named NSG1 associated to each subnet.

When a new subnet is created in Vnet1 an automated process creates an additional network monitoring virtual machine in the subnet and links the subnet to NSG1.

You need to create an inbound security rule in NSG1 that will allow connections to the network monitoring virtual machines from an IP address of 131.107.1.15.

The solution must meet the following requirements:

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

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

A. an application security group

- B. a service tag
- C. a virtual network
- D. an IP address

Correct Answer: A

Explanation/Reference:

To ensure that only the network monitoring virtual machines receive a connection from the specified IP address (131.107.1.15) and to minimize changes to NSG1 when a new subnet is created, you should use an application security group (ASG) as the destination in the inbound security rule. An application security group allows you to define network security group rules based on application-level constructs rather than individual IP addresses or subnets. By associating the network monitoring virtual machines with an application security group, you can specify the ASG as the destination in the inbound security rule, ensuring that only VMs within the ASG can receive connections from the specified IP address. Additionally, when a new subnet is created with a network monitoring VM, it can be automatically linked to the same ASG, minimizing changes to NSG1.

QUESTION 43

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

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

Users on HP1 connect to App1 by using a URL of https://app1.contoso.com.

You need to ensure that the IDPS on FW1 can identify security threats in the connections from HP1 to Server1.

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

NOTE: Each correct selection is worth one point.

- A. Enable TLS inspection for FW1.
- B. Import a server certificate to KV1.
- C. Enable threat intelligence for FW1.
- D. Add an application group to HP1.
- E. Add a secured virtual network to FW1.

Correct Answer: AB

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/firewall/premium-certificates>
<https://learn.microsoft.com/en-us/azure/firewall/premium-features#tls-inspection>

QUESTION 44

HOTSPOT

-

You have an Azure subscription that contains 10 virtual machines. The virtual machines are assigned private IP addresses. The subscription contains the resources shown in the following table.

Name	Type	Description
FWPolicy1	Azure Firewall Premium policy	None
Firewall1	Azure firewall	Firewall1 is linked to FWPolicy1. All internet traffic is routed through Firewall1.
VNet1	Virtual network	The virtual machines are connected to VNet1.

You need to configure FWPolicy1 to meet the following requirements:

- Allow incoming connections to the virtual machines from the internet on port 4567.
- Block outbound connections from the virtual machines to an FQDN of *.fabrikam.com.

What should you configure in FWPolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To allow inbound connections:

A DNAT rule

A network rule

An application rule

SNAT private IP ranges

To block outbound connections:

A DNAT rule

A network rule

An application rule

SNAT private IP ranges

The DNS settings

Answer:

Answer Area

To allow inbound connections:

▼

A DNAT rule
A network rule
An application rule
SNAT private IP ranges

To block outbound connections:

▼

A DNAT rule
A network rule
An application rule
SNAT private IP ranges
The DNS settings

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets#rule-types>

QUESTION 45

DRAG DROP

-

You have an Azure subscription that contains an Azure Firewall Premium policy named FWP1.

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

Name	Type
RC1	Network
RC2	Application
RC3	DNAT

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

Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Priorities

100

200

300

Answer Area

RC1:

RC2:

RC3:

Answer:

Answer Area

RC1: 200

RC2: 300

RC3: 100

Explanation/Reference:

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

QUESTION 46

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

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

To enter your password, place your cursor in the Enter password box and click on the password below.

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

Azure Password: xxxxxxxxxx

-

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

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You need to ensure that subnet3-2 can only access resources on subnet3-1.

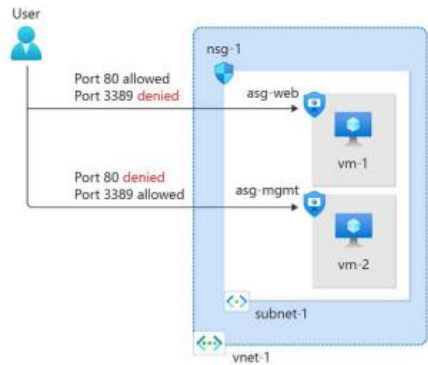
To complete this task, sign in to the Azure portal.

Answer:

Azure network rules

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

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



Stage 1: Create a network security group

A network security group (NSG) secures network traffic in your virtual network.

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

Step 2: Select + Create.

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

Project details

Subscription: Select your subscription.

Resource group: Select test-rg.

Instance details

Name: Enter nsg-1.

Location: Select East US 2.

Step 4: Select Review + create.

Step 5: Select Create.

Stage 2

Associate network security group to subnet

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

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

Step 2: Select nsg-1.

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

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

Home > Network security groups > nsg-1

nsg-1 | Subnets

Network security group

Search

+ Associate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Search subnets

Name	↑↓	Address range	↑↓	Virtual network	↑↓
No results.					

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

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

Stage 3:

Create security rules

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

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

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

Step 4: Select Add.

Reference:

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

QUESTION 47

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

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

You need to ensure that the apps hosted on VM1 can resolve the IP address of the private endpoint for azsql1.database.windows.net.

What should you create first?

- A. a public DNS zone named database.windows.net
- B. a private DNS zone named database.windows.net
- C. a public DNS zone named privatelink.database.windows.net
- D. a private DNS zone named privatelink.database.windows.net

Correct Answer: D

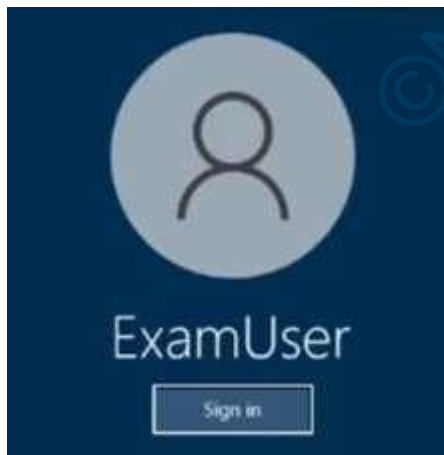
Explanation/Reference:

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

QUESTION 48

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

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

To enter your password, place your cursor in the Enter password box and click on the password below.

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

Azure Password: xxxxxxxxxx

-

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

The following information is for technical support purposes only:

Lab Instance: 12345678

-

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

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

Answer:

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

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

Step 2: Select Private DNS zone.

Step 3: Select Create private dns zone.

On the Create Private DNS zone page, type or select appropriate values:

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

Name: Type private.relecloud.com.

Resource group location:

Step 4: Select Review + Create.

Step 5: Select Create.

Stage 2: Create a CNAME DNS record

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

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

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

Name: Type www.

Type: CNAME

Record set properties: frontdoor1.azurefd.net

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

Reference:

<https://learn.microsoft.com/en-us/azure/dns/private-dns-getstarted-portal>

<https://learn.microsoft.com/en-us/azure/dns/dns-operations-recordsets-portal>

QUESTION 49

You have an Azure subscription that contains an Azure Front Door named FD1.

You plan to deploy an app named App1 by using Azure App Service. Users will access App1 by using FD1.

You need to provide FD1 with access to App1. The solution must meet the following requirements:

- Ensure that users can only access App1 by using FD1.
- Ensure that users cannot access App1 directly from the internet.

What should you create for App1?

- A. an access restriction
- B. a private endpoint
- C. a subnet delegation
- D. a service endpoint

Correct Answer: A

Explanation/Reference:

<https://techcommunity.microsoft.com/t5/azure-architecture-blog/permit-access-only-from-azure-front-door-to-azure-app-service-as/ba-p/2000173>

QUESTION 50

HOTSPOT

-

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

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

You purchase a certificate for app1.contoso.com from a public certification authority (CA) and install the certificate on appservice1.

You need to ensure that App1 can be accessed by using a URL of https://app1.contoso.com. The solution must ensure that all the traffic for App1 is routed via FD1.

Which type of DNS record should you create, and where should you store the certificate? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

DNS record type:

▼

A
CNAME
SRV
TXT

Store the certificate in:

▼

FD1
KeyVault1
KeyVault2

Answer:

Answer Area

DNS record type:

▼

A
CNAME
SRV
TXT

Store the certificate in:

▼

FD1
KeyVault1
KeyVault2

Explanation/Reference:

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

QUESTION 51

You have an Azure subscription that contains four virtual machines. The virtual machines host an app named App1.

You deploy an Azure Standard Load Balancer named LB1 to load balance incoming HTTPS requests to App1.

You need to reduce how long it takes for LB1 to stop sending App1 traffic to failed servers. The solution must minimize administrative effort.

What should you modify?

- A. the Backend pools settings
- B. the Diagnostic settings
- C. the Load-balancing rules
- D. the Health probes settings

Correct Answer: D

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/load-balancer/manage-probes-how-to>

QUESTION 52

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

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

You need to deploy an Azure application gateway named AppGW1 to VNet1.

To where can you deploy AppGW1?

- A. GatewaySubnet only
- B. Subnet2 only
- C. Subnet1 or Subnet2 only
- D. Subnet2 or GatewaySubnet only
- E. Subnet1, Subnet2, and GatewaySubnet

Correct Answer: B

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/application-gateway/configuration-infrastructure>

QUESTION 53

Your on-premises network contains a DNS server named Server1.

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

Name	Type	Description
VNet1	Virtual network	None
VM1	Virtual machine	Connected to VNet1 Connected to storage1 by using a private endpoint
storage1	Storage account	None

The on-premises network is connected to VNet1 by using a Site-to-Site (S2S) VPN.

You need to ensure that Server1 can resolve the DNS name of storage1. The solution must minimize costs and administrative effort.

What should you use?

- A. Azure DNS Private Resolver
- B. an Azure public DNS zone
- C. an Azure Private DNS zone
- D. an Azure virtual machine that hosts a DNS service

Correct Answer: A

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-overview>

QUESTION 54

You have an on-premises network named Site1.

You have an Azure subscription that contains a virtual network named VNet1 and a storage account named storage1.

Site1 and VNet1 are connected by using a Site-to-Site (S2S) VPN.

You need to ensure that the servers in Site1 can connect to storage1 by using the S2S VPN. The solution must minimize administrative effort.

What should you create on VNet1?

- A. an Azure application gateway
- B. an Azure Private Link service
- C. a service endpoint
- D. a private endpoint

Correct Answer: D

Explanation/Reference:

Private endpoints enable secure connectivity between virtual networks and Azure services over the Azure backbone network, ensuring that traffic remains within the Azure network. By creating a private endpoint for storage1 in VNet1, you can ensure that the servers in Site1 can securely connect to storage1 via the S2S VPN without exposing the storage account to the public internet.

Case Study 1 - Litware, Inc

Overview -

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

Existing Environment -

Hybrid Environment -

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

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

Azure Environment -

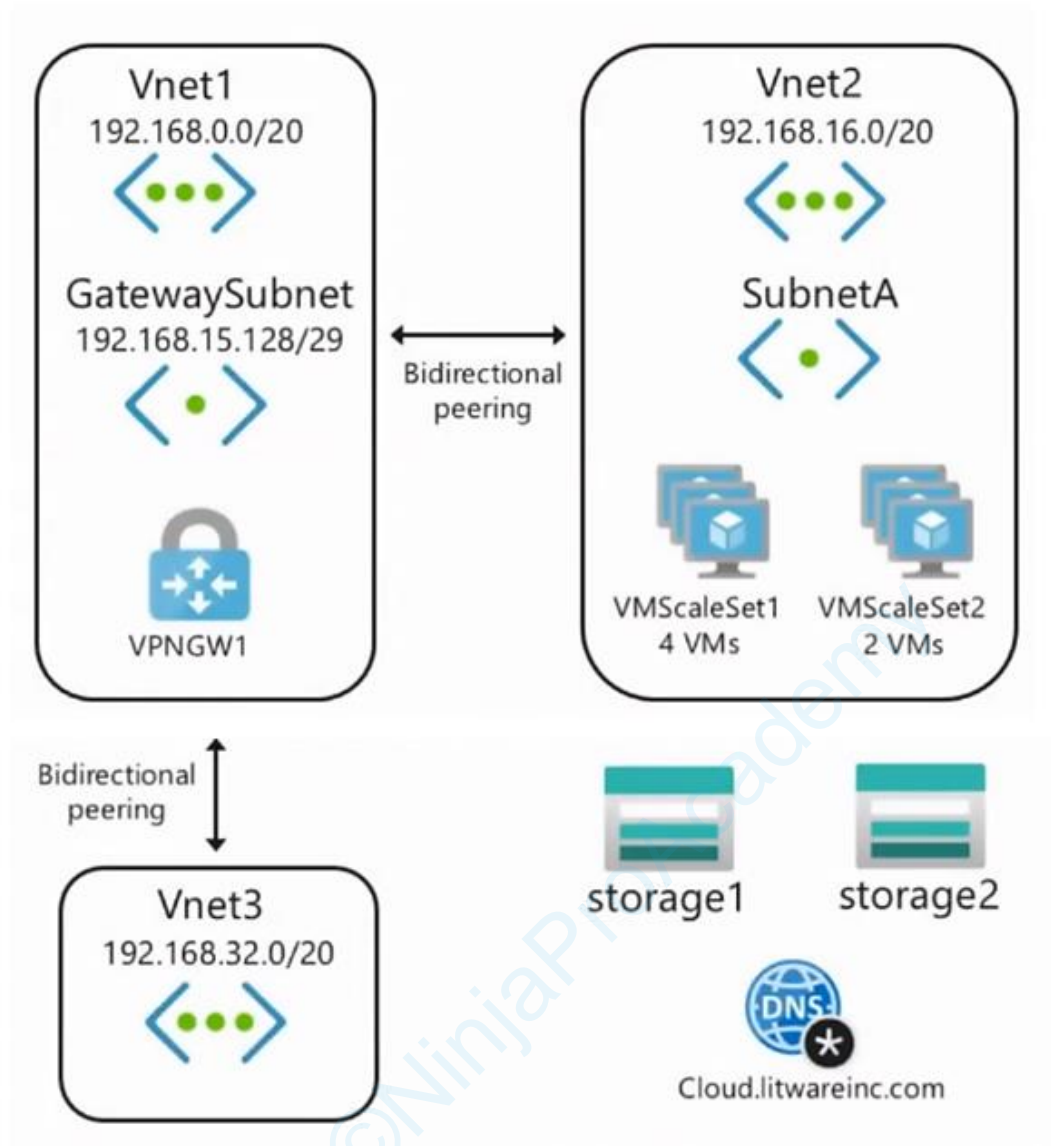
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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

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

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

Azure Network Diagram -



Requirements -

Business Requirements -

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

Virtual Networking Requirements -

Litware identifies the following virtual networking requirements:

- Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.
- Ensure that the records in the cloud.litwareinc.com can be resolved from the on-premises locations.
- Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.
- Minimize the size of the subnets allocated to platform-managed services.
- Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements -

Litware identifies the following hybrid networking requirements:

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

PaaS Networking Requirements -

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

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

QUESTION 55

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

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

Explanation/Reference:

<https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath#gateways>

<https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath#virtual-network-vnet-peering>

QUESTION 56

DRAG DROP -

You need to prepare Vnet1 for the deployment of an ExpressRoute gateway. The solution must meet the hybrid connectivity requirements and the business requirements.

Which three actions should you perform in sequence for Vnet1? To answer, move the appropriate actions from the list of actions to the answer.

Select and Place:

Actions	Answer Area
Delete VPN GW1.	
Create a VPN gateway by using the Basic SKU.	
Set the subnet mask of Gateway Subnet to /27.	
Assign a user-defined route to Gateway Subnet.	
Create a VPN gateway by using the VPN GW1 SKU.	

Answer:

Actions	Answer Area
	Delete VPN GW1.
	Create a VPN gateway by using the Basic SKU.
	Set the subnet mask of Gateway Subnet to /27.
Assign a user-defined route to Gateway Subnet.	
Create a VPN gateway by using the VPN GW1 SKU.	

Explanation/Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>
<https://docs.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal>

QUESTION 57

HOTSPOT -

You need to implement a P2S VPN for the users in the branch office. The solution must meet the hybrid networking requirements.

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

Answer Area

On the VPN gateway in Vnet1, set the P2S VPN tunnel type to:

	▼
IKEv2	
OpenVPN (SSL)	
SSTP (SSL)	

In the litwareinc.com tenant:

	▼
Create a device object	
Create a managed identity	
Grant consent to an Azure AD application	

Answer:

Answer Area

On the VPN gateway in Vnet1, set the P2S VPN tunnel type to:

	▼
IKEv2	
OpenVPN (SSL)	
SSTP (SSL)	

In the litwareinc.com tenant:

	▼
Create a device object	
Create a managed identity	
Grant consent to an Azure AD application	

Explanation/Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>

Case Study 2 - Contoso, Ltd.

Overview -

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas. Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

Existing Environment -

Azure Network Infrastructure -

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

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

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

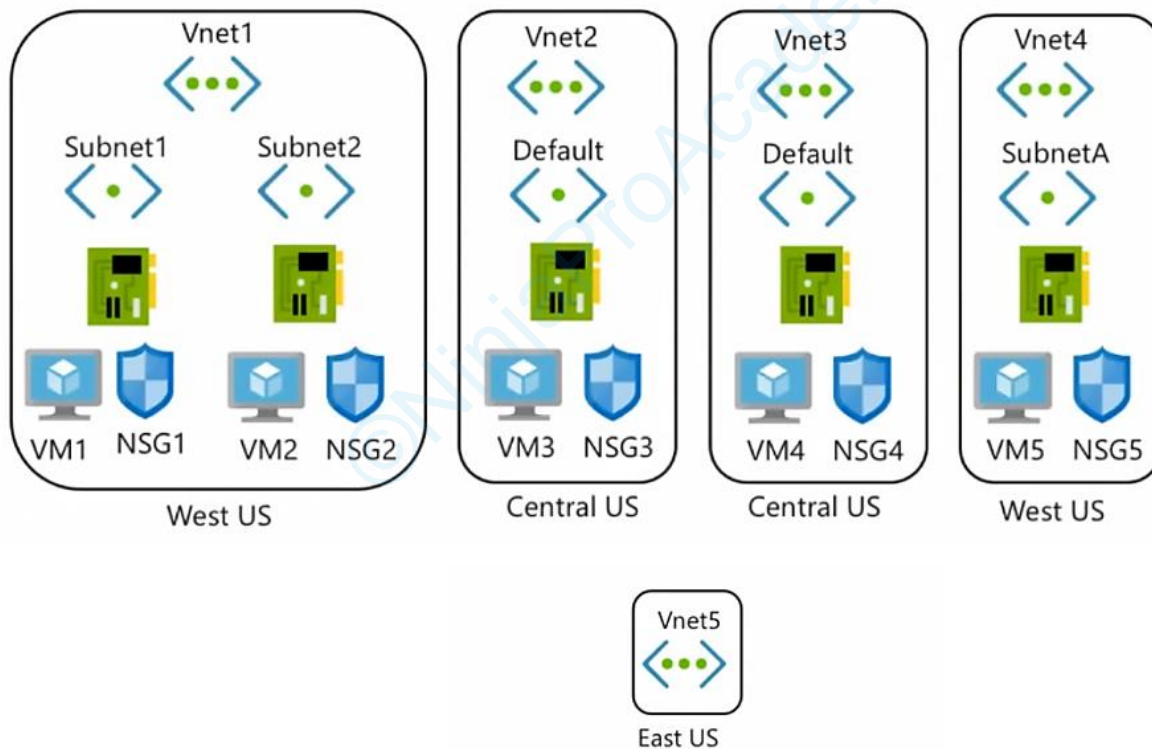
Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

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

The firewall on each virtual machine allows ICMP traffic.

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

Azure Network Infrastructure Diagram



Azure Private DNS Zones -

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

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

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

Name	Virtual Network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources -

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

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

Requirements -

Virtual Network Requirements -

Contoso has the following virtual 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 58

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

Explanation/Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>

QUESTION 59

HOTSPOT -

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	<input type="radio"/>	<input type="radio"/>
VM4 has an automatic registration in zone1.contoso.com.	<input type="radio"/>	<input type="radio"/>
You can link zone2.contoso.com to Vnet3 and enable auto registration.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>
VM4 has an automatic registration in zone1.contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
You can link zone2.contoso.com to Vnet3 and enable auto registration.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation/Reference:

Box 1: No -

Zone2.contoso.com is not linked to any virtual networks. Therefore, no VMs are able to resolve names in the zone.

Box 2: Yes -

VM4 is in VNet3. Zone1.contoso.com has a link to VNet3 and auto-registration is enabled on the link.

Box3: No -

VNet3 is linked to zone1.contoso.com and auto-registration is enabled on the link. A virtual network can only have one registration zone.

You can link zone2.contoso.com to VNet3 but you won't be able to enable auto-registration on the link.

QUESTION 60

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:

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	

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	

Explanation/Reference:

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 61

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

Explanation/Reference:

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.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

QUESTION 62

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	

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	

Explanation/Reference:

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

Start Your AZ-700 Exam Preparation
Get Full AZ-700 Exam Questions & Answers



SPECIAL OFFER

WELCOME15

**ENJOY A LIMITED-TIME
PROMOTION**



**15%
OFF**

TRY NOW

COUPON CODE

WELCOME15

<https://latestexamdumps.com>

<https://latestexamdumps.com/vendors/microsoft/microsoft-az-700-exam/>

**Pass Your Upcoming AZ-700 Exam on Your
First Attempt Like A Pro!**



Thank You For Downloading AZ-700 Dump PDF Demo!