The questions for AZ-700 were last updated on April 23, 2024.

Viewing page **1** out of 10 pages.
Viewing questions 1-27 out of 267 questions

Custom View Settings

Topic 1 - Question Set 1

Question #1

Topic 1

Your company has a single on-premises datacenter in Washington DC. The East US Azure region has a peering location in Washington DC.
The company only has Azure resources in the East US region.
You need to implement ExpressRoute to support up to 1 Gbps. You must use only ExpressRoute Unlimited data plans. The solution must minimize costs.
Which type of ExpressRoute circuits should you create?

A. ExpressRoute Local **Most Voted**

B. ExpressRoute Direct

C. ExpressRoute Premium

D. ExpressRoute Standard

Hide Solution Discussion 19

Correct Answer: *A*
Reference:
https://azure.microsoft.com/en-us/pricing/details/expressroute/

Community vote distribution
A (90%) 10%

Question #2

Topic 1

You are planning an Azure Point-to-Site (P2S) VPN that will use OpenVPN.
Users will authenticate by an on-premises Active Directory domain.
Which additional service should you deploy to support the VPN authentication?

A. an Azure key vault

B. a RADIUS server **Most Voted**

C. a certification authority

D. Azure Active Directory (Azure AD) Application Proxy

Hide Solution Discussion 28

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

Community vote distribution
B (100%)

Question #3 *Topic 1*

You plan to configure BGP for a Site-to-Site VPN connection between a datacenter and Azure.
Which two Azure resources should you configure? Each correct answer presents a part of the solution. (Choose two.)
NOTE: Each correct selection is worth one point.

A. a virtual network gateway **Most Voted**

B. Azure Application Gateway

C. Azure Firewall

D. a local network gateway **Most Voted**

E. Azure Front Door

Hide Solution Discussion 27

Correct Answer: *AD*
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/bgp-howto

Community vote distribution
AD (100%)

Question #4 *Topic 1*

You fail to establish a Site-to-Site VPN connection between your company's main office and an Azure virtual network.
You need to troubleshoot what prevents you from establishing the IPsec tunnel.
Which diagnostic log should you review?

A. IKEDiagnosticLog **Most Voted**

B. RouteDiagnosticLog

C. GatewayDiagnosticLog

D. TunnelDiagnosticLog

Hide Solution Discussion 17

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics

Community vote distribution
A (100%)

Question #5 Topic 1

You have an Azure virtual network and an on-premises datacenter.
You are planning a Site-to-Site VPN connection between the datacenter and the virtual network.
Which two resources should you include in your plan? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a user-defined route

B. a virtual network gateway **Most Voted**

C. Azure Firewall

D. Azure Web Application Firewall (WAF)

E. an on-premises data gateway

F. an Azure application gateway

G. a local network gateway **Most Voted**

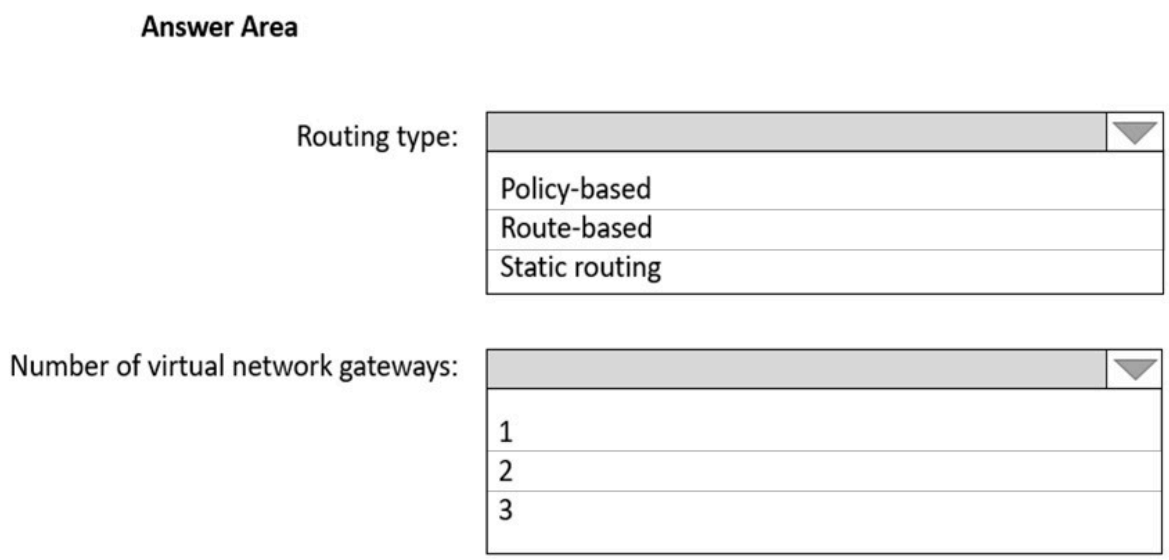
Hide Solution Discussion 14

Correct Answer: *BG*
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal

Community vote distribution
BG (100%)

Question #6 *Topic 1*

HOTSPOT -
You need to connect an on-premises network and an Azure environment. The solution must use ExpressRoute and support failing over to a Site-to-Site VPN connection if there is an ExpressRoute failure.
What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

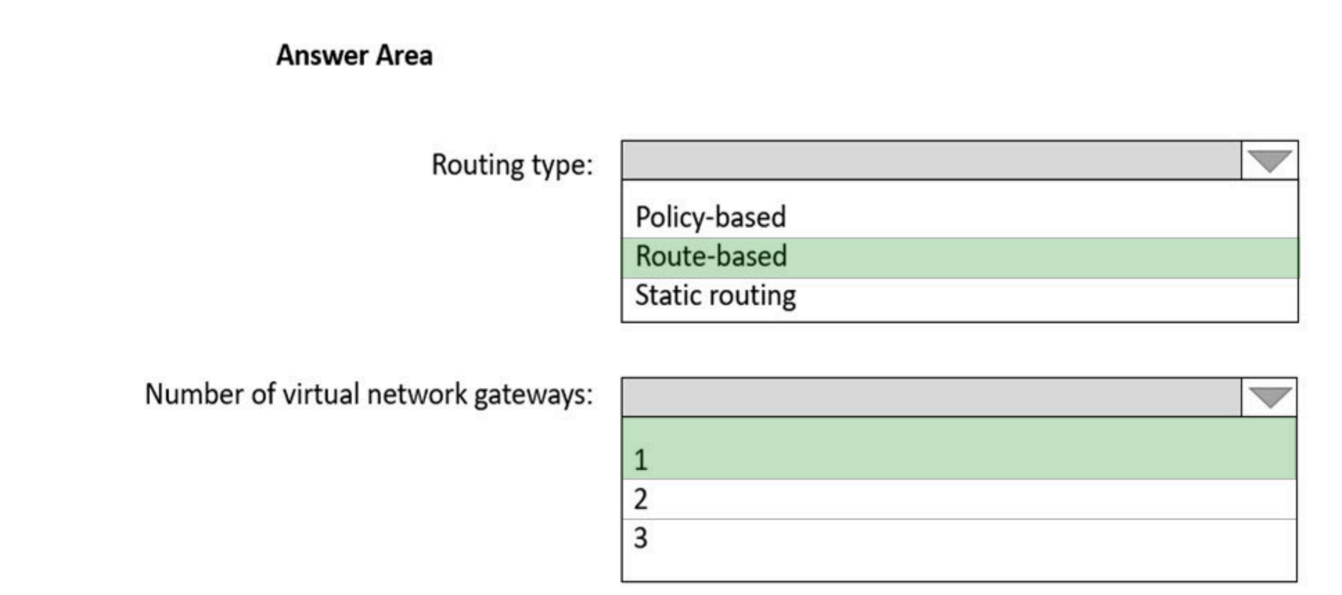
Routing type:
- Policy-based
- Route-based
- Static routing

Number of virtual network gateways:
- 1
- 2
- 3

Hide Solution

Discussion 49

Correct Answer:



Answer Area

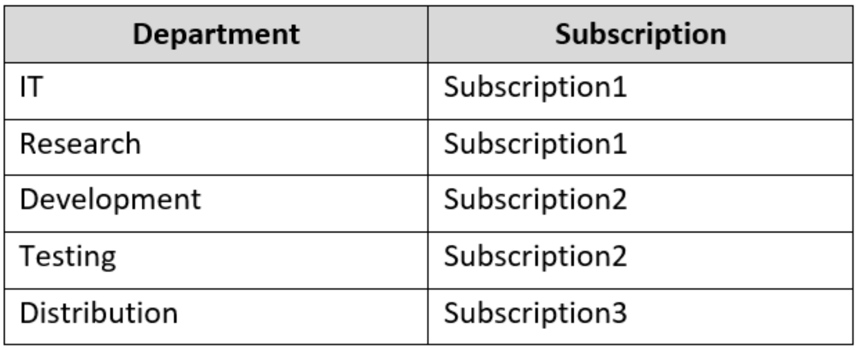
Routing type:
- Policy-based
- [✓ Route-based]
- Static routing

Number of virtual network gateways:
- [✓ 1]
- 2
- 3

Reference:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager

Question #7 *Topic 1*

Your company has an on-premises network and three Azure subscriptions named Subscription1, Subscription2, and Subscription3.
The departments at the company use the Azure subscriptions as shown in the following table.



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

All the resources in the subscriptions are in either the West US Azure region or the West US 2 Azure region.
You plan to connect all the subscriptions to the on-premises network by using ExpressRoute.
What is the minimum number of ExpressRoute circuits required?

A. 1 **Most Voted**
B. 2
C. 3
D. 4
E. 5

Hide Solution   Discussion 22

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction

Community vote distribution
A (88%) 13%

Question #8 *Topic 1*

Your company has offices in New York and Amsterdam. The company has an Azure subscription. Both offices connect to Azure by using a Site-to-Site VPN connection.
The office in Amsterdam uses resources in the North Europe Azure region. The office in New York uses resources in the East US Azure region.
You need to implement ExpressRoute circuits to connect each office to the nearest Azure region. Once the ExpressRoute circuits are connected, the on-premises computers in the Amsterdam office must be able to connect to the on-premises servers in the New York office by using the ExpressRoute circuits.
Which ExpressRoute option should you use?

A. ExpressRoute FastPath
B. ExpressRoute Global Reach **Most Voted**
C. ExpressRoute Direct
D. ExpressRoute Local

Hide Solution   Discussion 16

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach

Community vote distribution
B (100%)

Question #9 *Topic 1*

HOTSPOT -

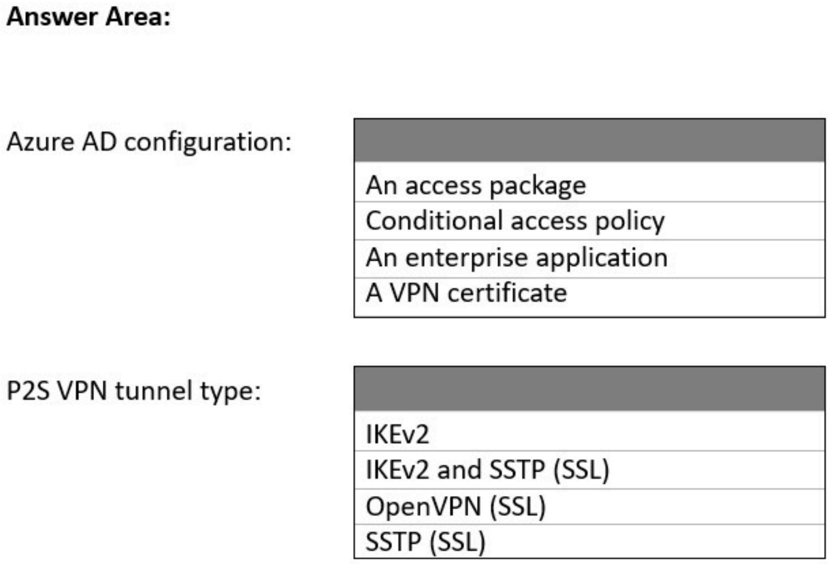
You have an Azure subscription that contains a single virtual network and a virtual network gateway.

You need to ensure that administrators can use Point-to-Site (P2S) VPN connections to access resources in the virtual network. The connections must be authenticated by Azure Active Directory (Azure AD).

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

NOTE: Each correct selection is worth one point.

Hot Area:



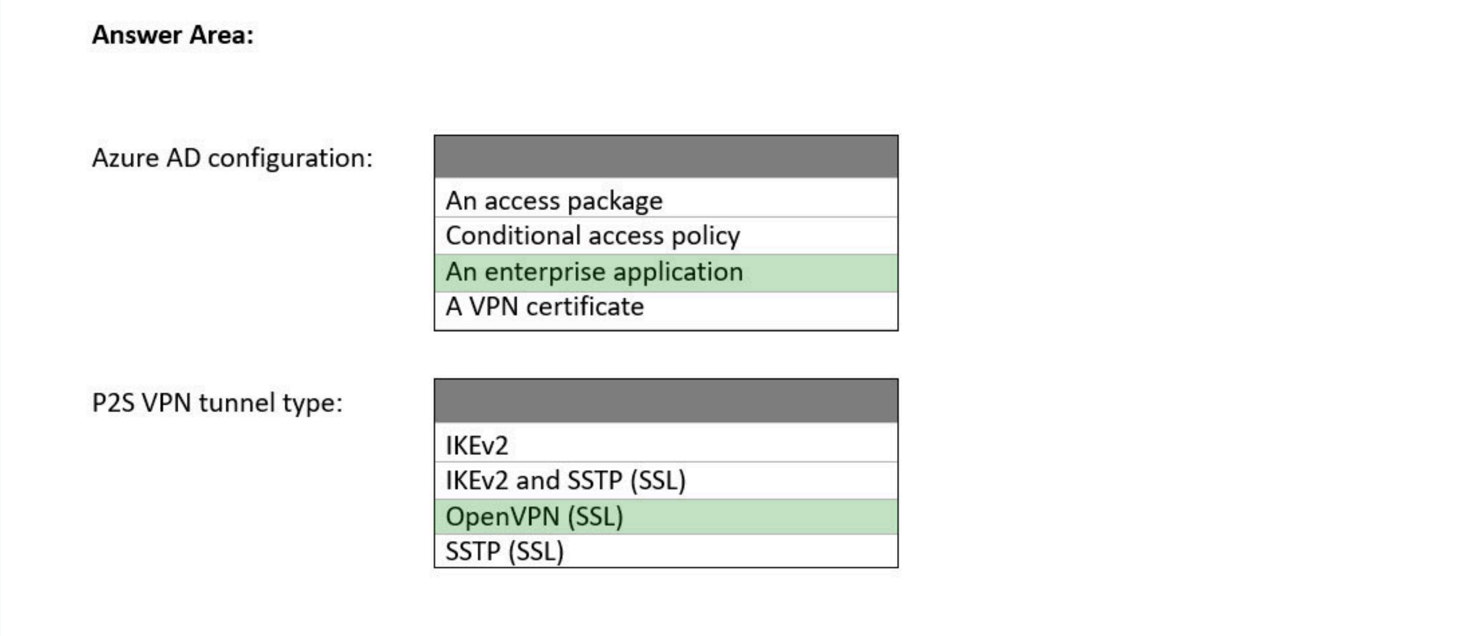
Answer Area:

Azure AD configuration:
- An access package
- Conditional access policy
- An enterprise application
- A VPN certificate

P2S VPN tunnel type:
- IKEv2
- IKEv2 and SSTP (SSL)
- OpenVPN (SSL)
- SSTP (SSL)

Hide Solution Discussion 12

Correct Answer:



Answer Area:

Azure AD configuration:
- An access package
- Conditional access policy
- [✓ An enterprise application]
- A VPN certificate

P2S VPN tunnel type:
- IKEv2
- IKEv2 and SSTP (SSL)
- [✓ OpenVPN (SSL)]
- SSTP (SSL)

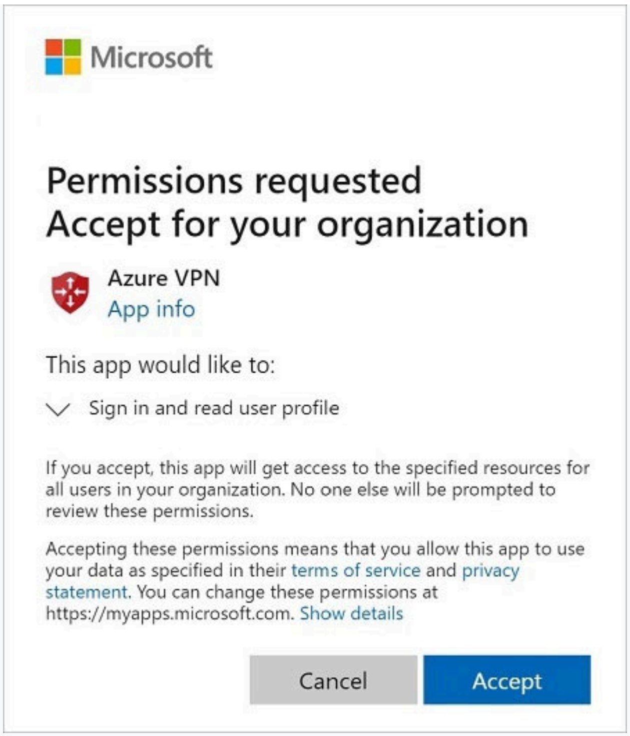
Box 1: An enterprise application

Enable Azure AD authentication on the VPN gateway:

1. Locate the Directory ID of the directory that you want to use for authentication. It's listed in the properties section of the Active Directory page.
2. Under your Azure AD, in Enterprise applications, you see Azure VPN listed.

Copy the Directory ID.

3. Sign in to the Azure portal as a user that is assigned the Global administrator role.
4. Next, give admin consent. Copy and paste the URL that pertains to your deployment location in the address bar of your browser.
5. Select the Global Admin account if prompted.
6. Select Accept when prompted.



Microsoft

Permissions requested
Accept for your organization

Azure VPN
App info

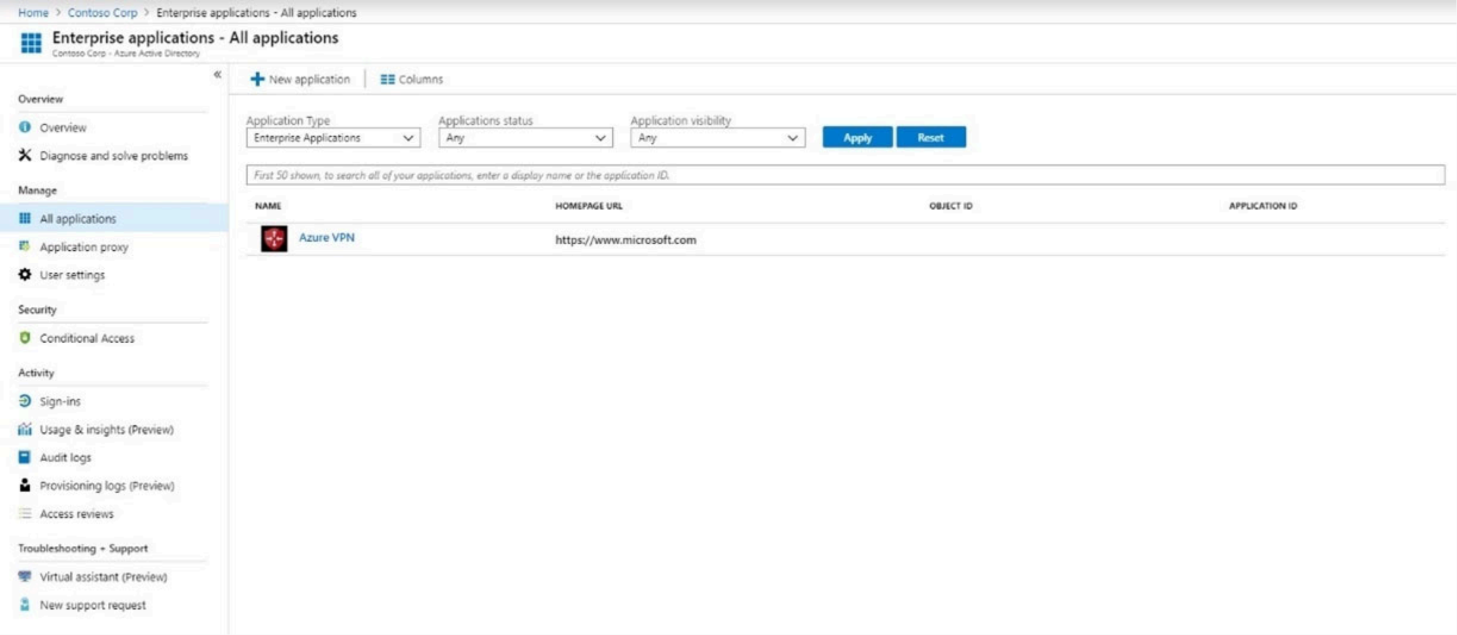
This app would like to:

Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

7. Under your Azure AD, in Enterprise applications, you see Azure VPN listed.



Home > Contoso Corp > Enterprise applications - All applications

Enterprise applications - All applications
Contoso Corp - Azure Active Directory

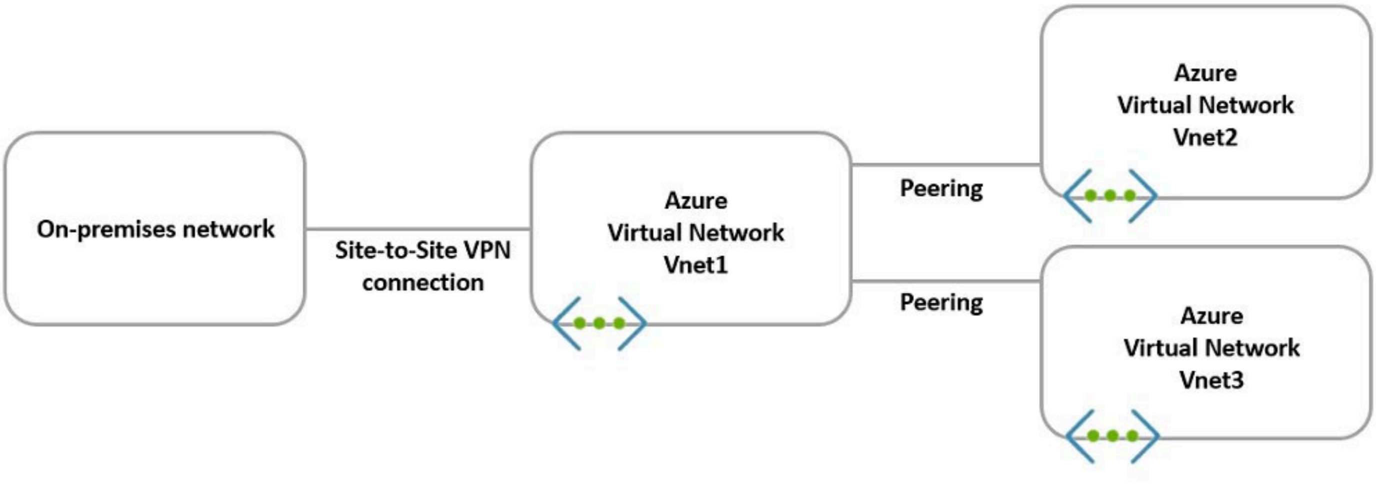
Application Type: Enterprise Applications
Applications status: Any
Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

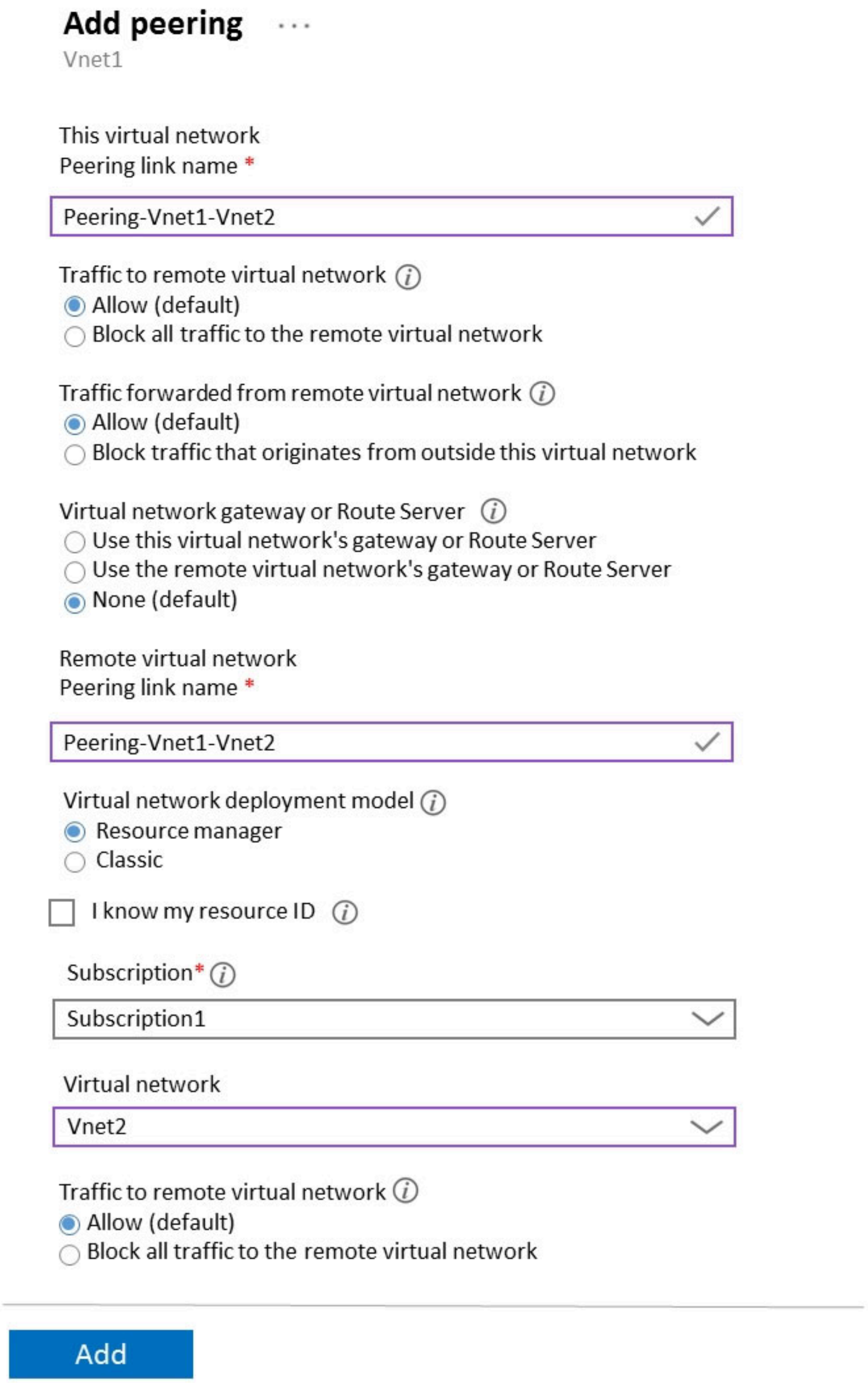
NAME	HOMEPAGE URL	OBJECT ID	APPLICATION ID
Azure VPN	https://www.microsoft.com		

Box 2: Open VPN (SSL)
When you connect to your VNet using Point-to-Site, you have a choice of which protocol to use. The protocol you use determines the authentication options that are available to you. If you want to use Azure Active Directory authentication, you can do so when using the OpenVPN protocol.
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant

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


On-premises network
Site-to-Site VPN connection
Azure Virtual Network Vnet1
Peering
Peering
Azure Virtual Network Vnet2
Azure Virtual Network Vnet3

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

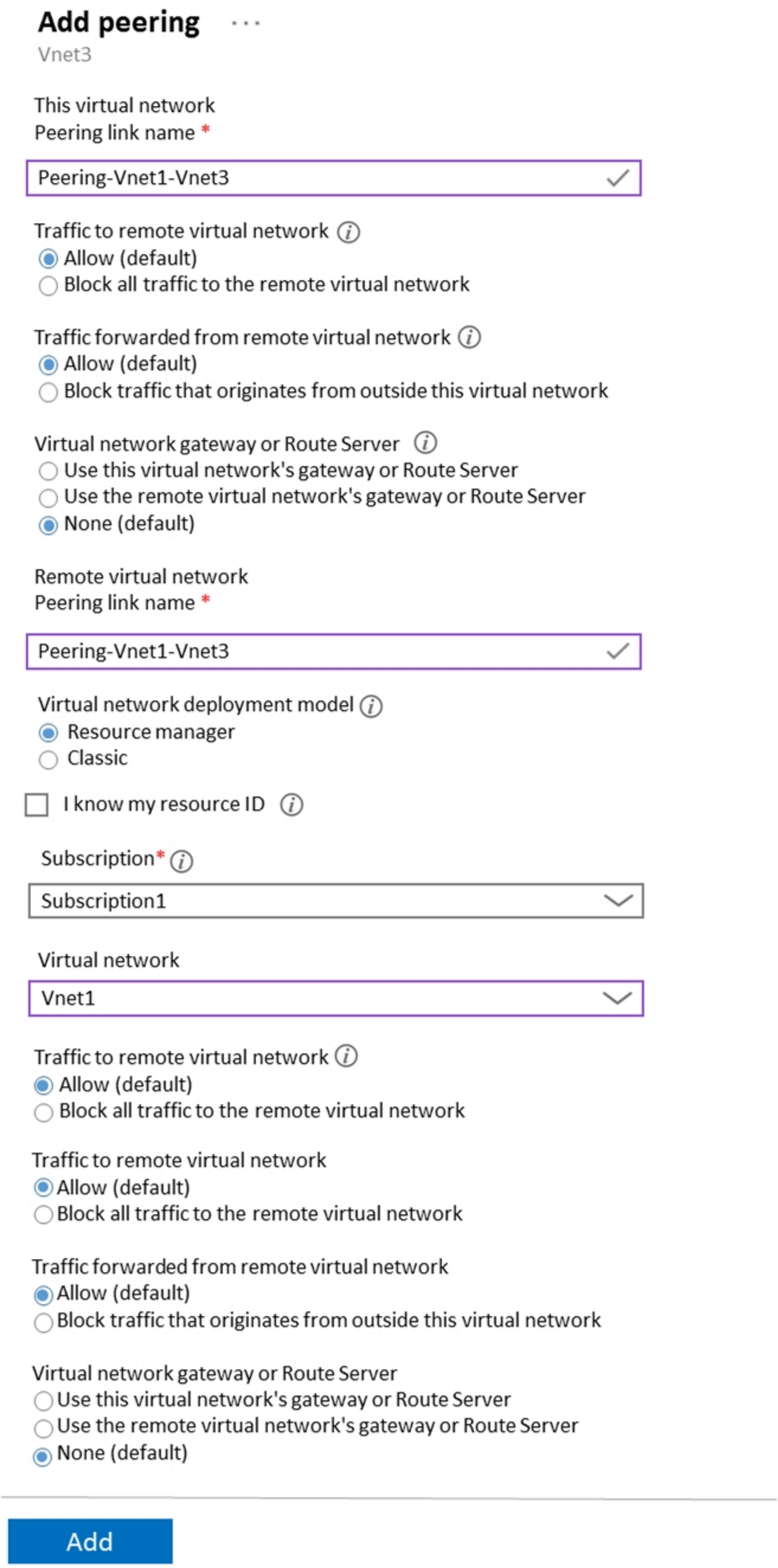
Traffic to remote virtual network ⓘ

● 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.



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

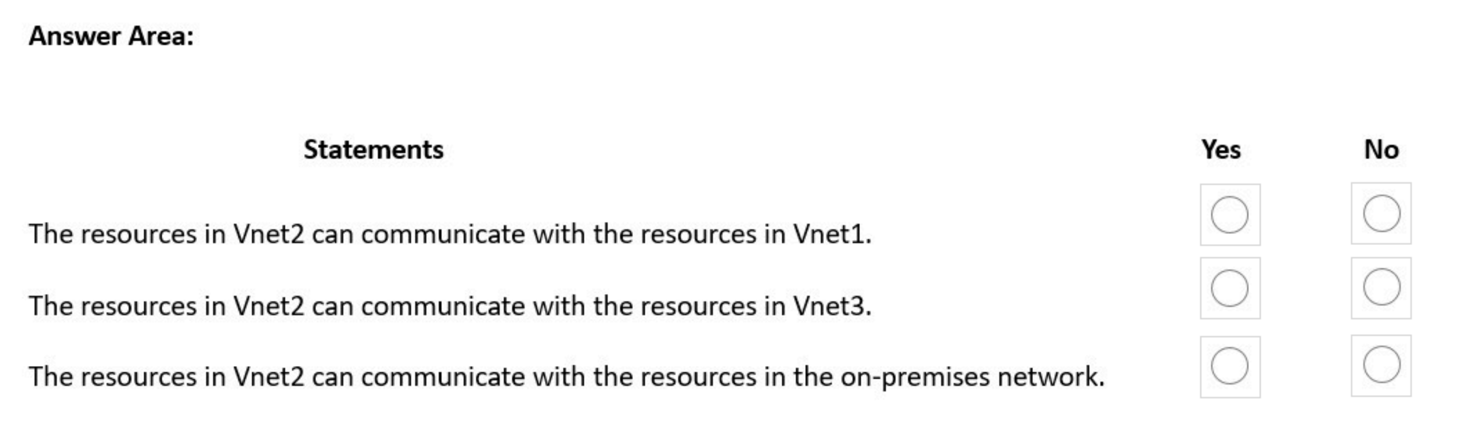
○ Use this virtual network's gateway or Route Server

○ Use the remote virtual network's gateway or Route Server

● None (default)

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:

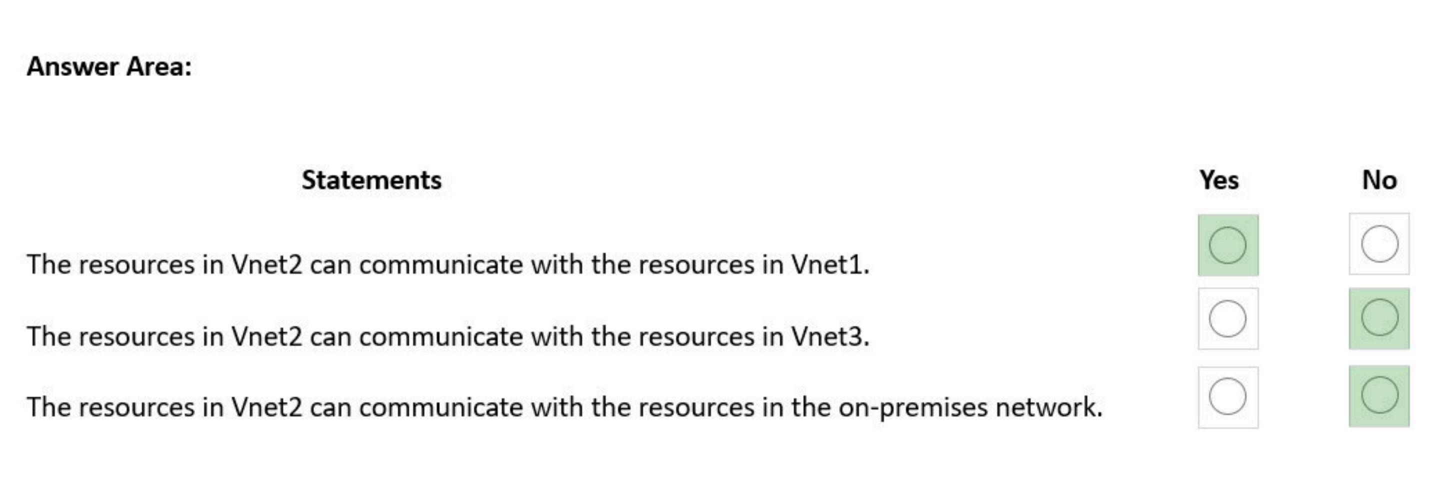


Answer Area:

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

Hide Solution Discussion 17

Correct Answer:

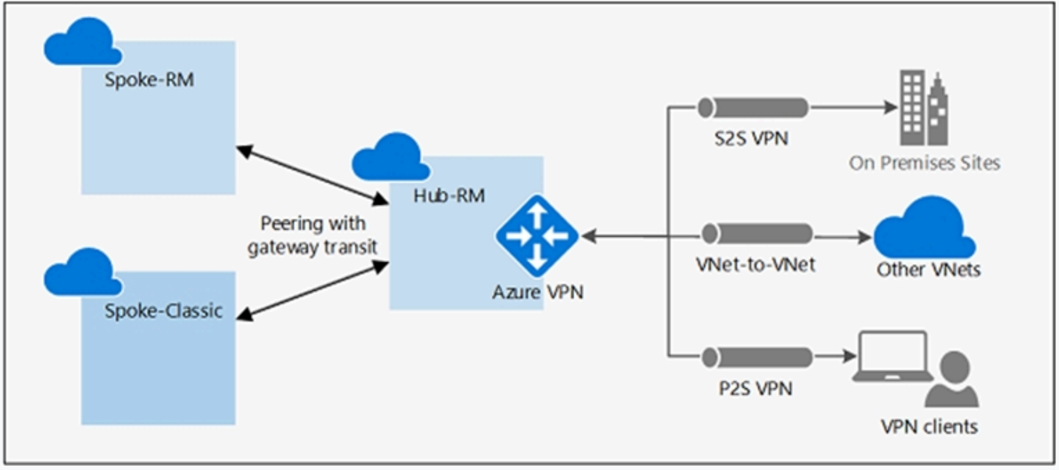


Answer Area:

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

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.



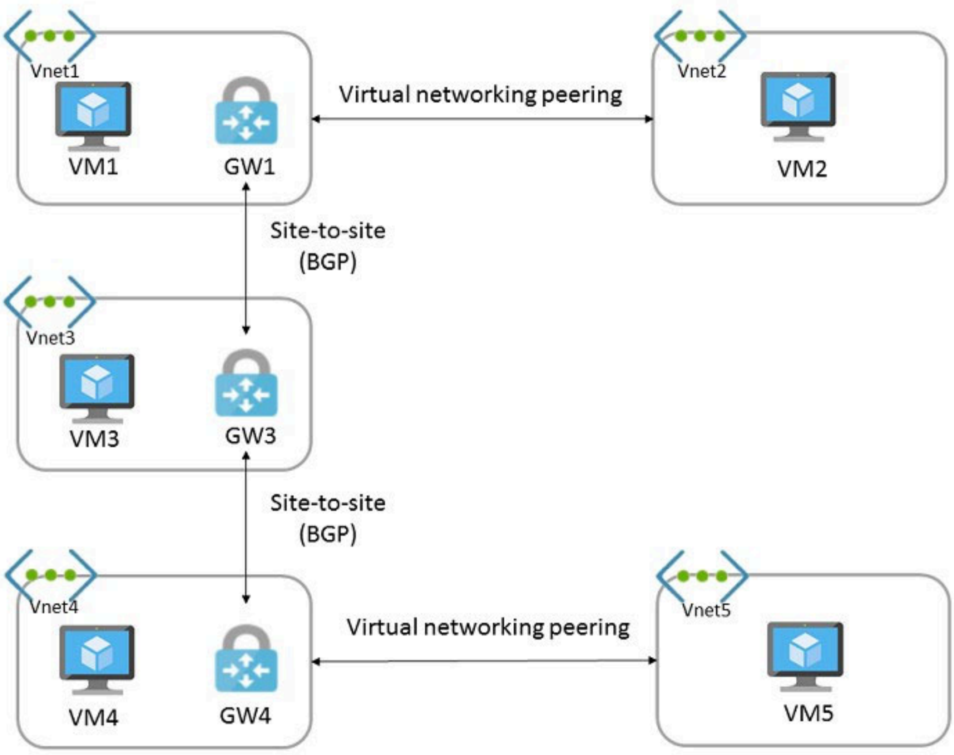
In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual networks.

Box 3: No -
No Virtual Gateway is used.
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

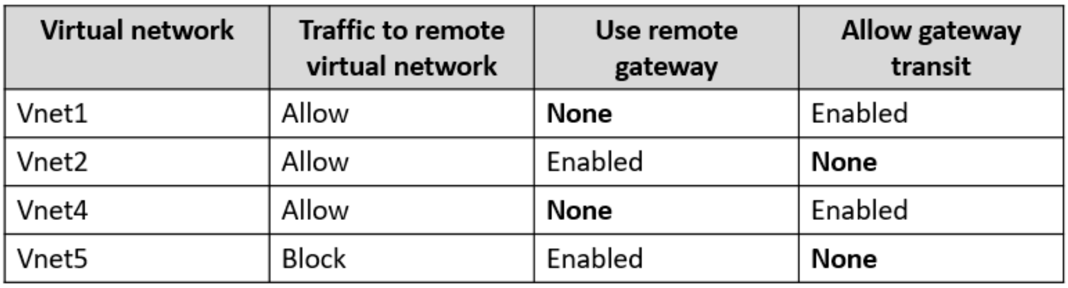
Question #11 *Topic 1*

HOTSPOT -

You have the Azure environment shown in the exhibit.



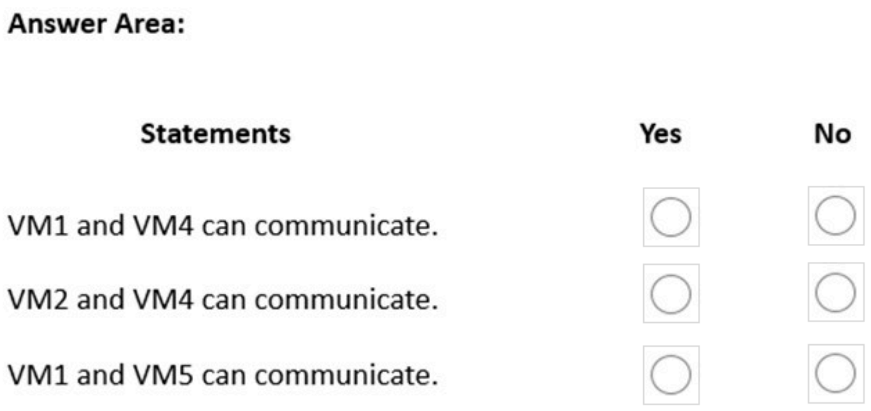
You have virtual network peering between Vnet1 and Vnet2. You have virtual network peering between Vnet4 and Vnet5. The virtual network peering is configured as shown in the following table.



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

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

Hot Area:

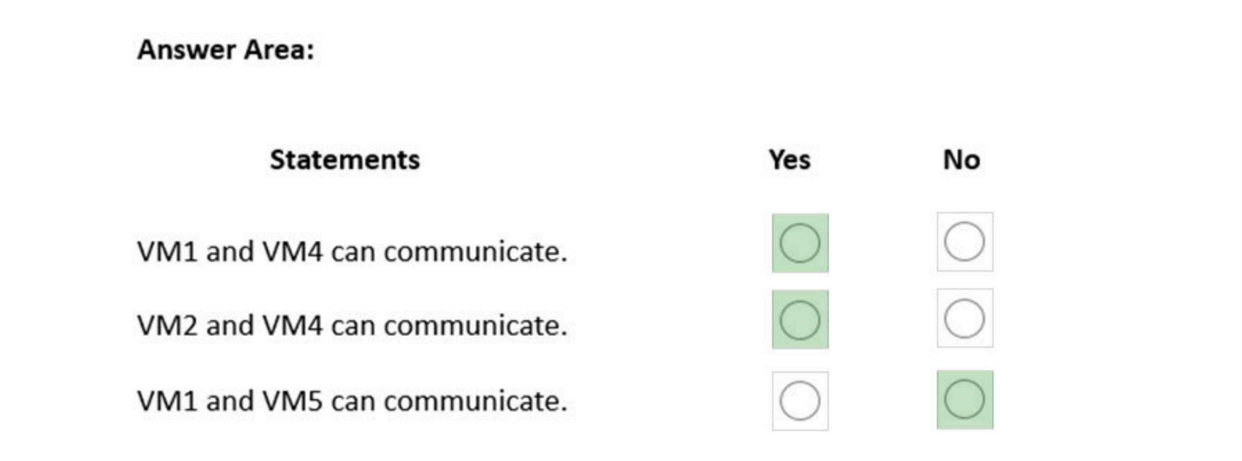


Answer Area:

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

Hide Solution   Discussion 31

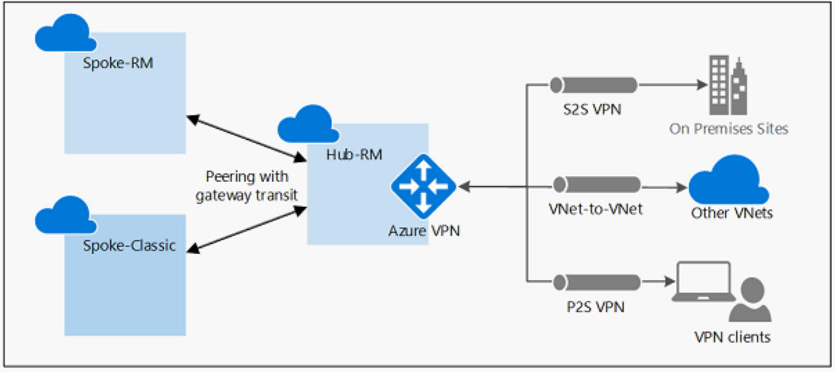
Correct Answer:



Answer Area:

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

Box 1: Yes -
Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes.
Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity.
The following diagram shows how gateway transit works with virtual network peering.



In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual networks.
In hub-and-spoke network architecture, gateway transit allows spoke virtual networks to share the VPN gateway in the hub, instead of deploying VPN gateways in every spoke virtual network.

Box 2: Yes -
VM2 uses the remote gateway GW1 to reach VM4.

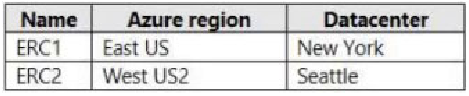
Box 3: No -
VM2 can reach VM4 through GW1, but not VM5 as VNEt1 does not use remote Gateways.
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-troubleshoot-peering-issues

Question #12 *Topic 1*

HOTSPOT -

You have on-premises datacenters in New York and Seattle.

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



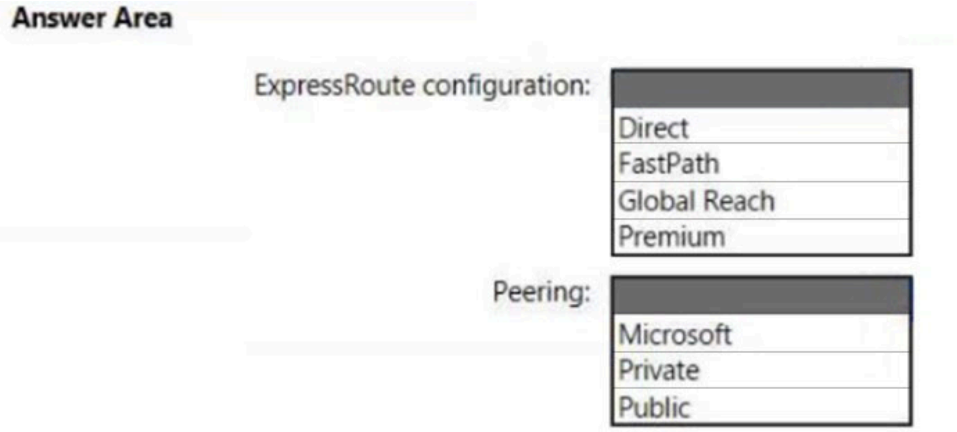
Name	Azure region	Datacenter
ERC1	East US	New York
ERC2	West US2	Seattle

You need to ensure that all the data sent between the datacenters is routed via the ExpressRoute circuits. The solution must minimize costs.

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

NOTE: Each correct selection is worth one point.

Hot Area:



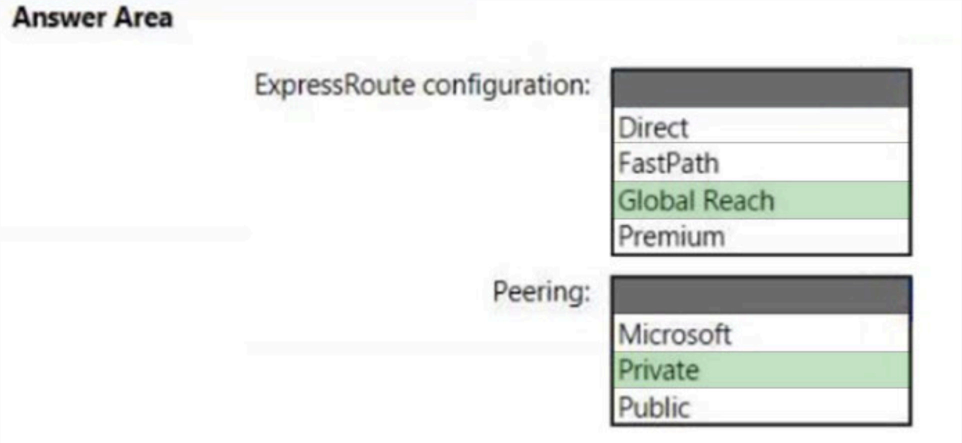
Answer Area

ExpressRoute configuration:
- Direct
- FastPath
- Global Reach
- Premium

Peering:
- Microsoft
- Private
- Public

Hide Solution Discussion 18

Correct Answer:



Answer Area

ExpressRoute configuration:
- Direct
- FastPath
- [✓ Global Reach]
- Premium

Peering:
- Microsoft
- [✓ Private]
- Public

Box 1: Global Reach -

ExpressRoute Global Reach is the service where if you have two datacenters, which are located at different geo-locations and both are connected to Microsoft

Azure via Express Route then these two datacenters can also connect to each other securely via Microsoft's backbone.

Incorrect:

FastPath is designed to improve the data path performance between your on-premises network and your virtual network. When enabled, FastPath sends network traffic directly to virtual machines in the virtual network, bypassing the gateway.

Box 2: Private -

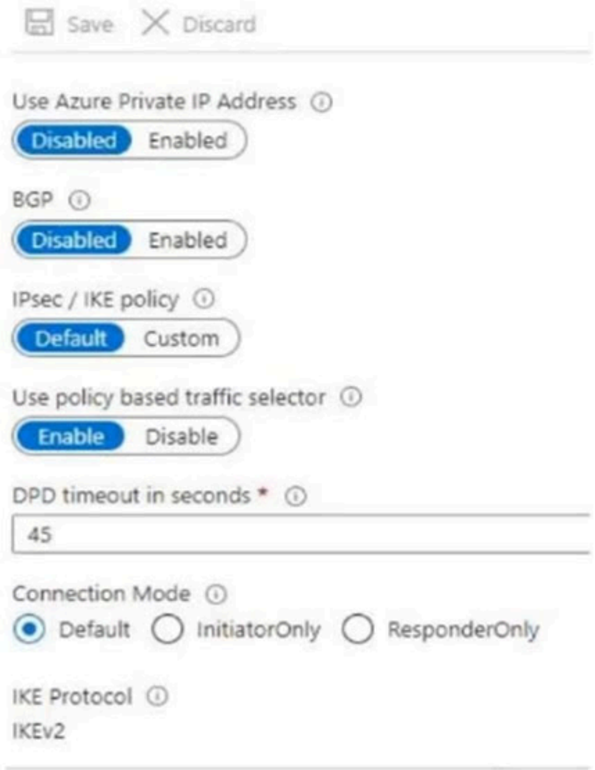
With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks.

Reference:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach

Question #13 *Topic 1*

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.



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. Most Voted

Hide Solution Discussion 25

Correct Answer: *B*
BGP is the standard routing protocol commonly used in the Internet to exchange routing and reachability information between two or more networks. BGP enables the Azure VPN Gateways and your on-premises VPN devices, called BGP peers or neighbors, to exchange "routes" that will inform both gateways on the availability and reachability for those prefixes to go through the gateways or routers involved. BGP can also enable transit routing among multiple networks by propagating routes a BGP gateway learns from one BGP peer to all other BGP peers.
Incorrect:
Not C: A VPN gateway must have a Public IP address. Verify that you have an externally facing public IPv4 address for your VPN device.
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-resource-manager-ps https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-cli

Community vote distribution
D (90%) 10%

Question #14 Topic 1

HOTSPOT

-

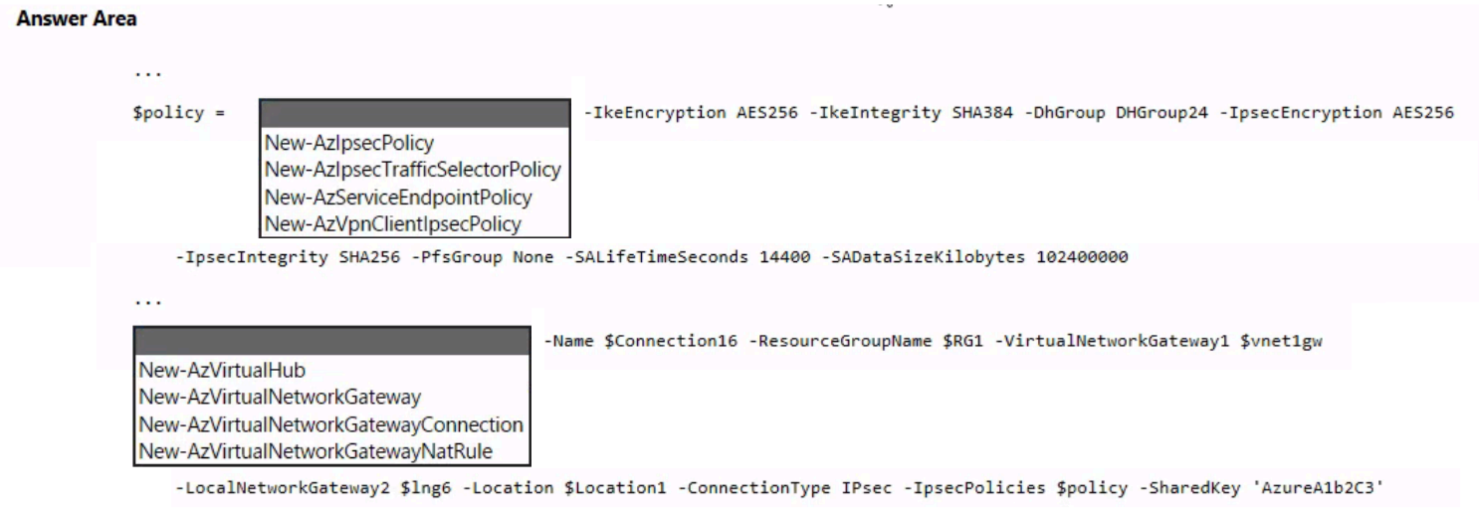
Your on-premises network contains a VPN device.

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.

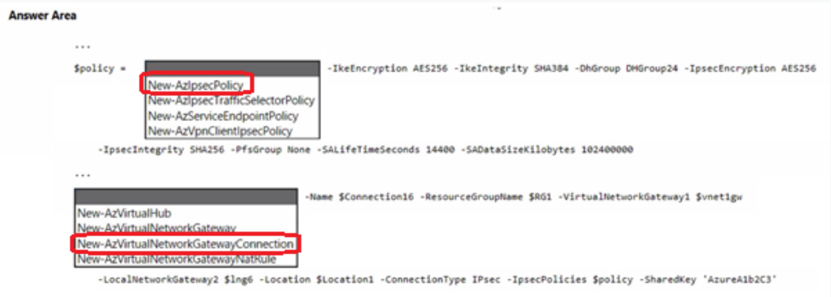


Answer Area

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

Hide Solution Discussion 10

Correct Answer:



Answer Area

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

[✓ New-AzIpsecPolicy]

[✓ New-AzVirtualNetworkGatewayConnection]

Question #15 *Topic 1*

HOTSPOT

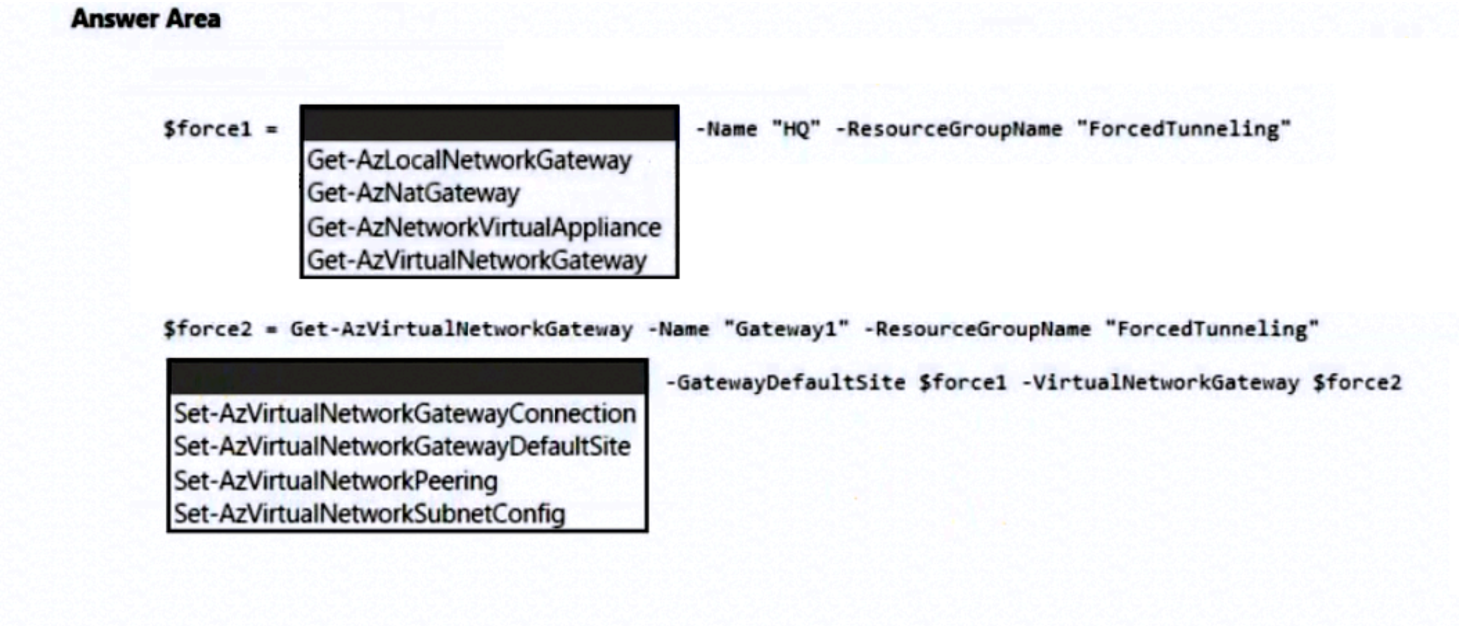
-

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"
```

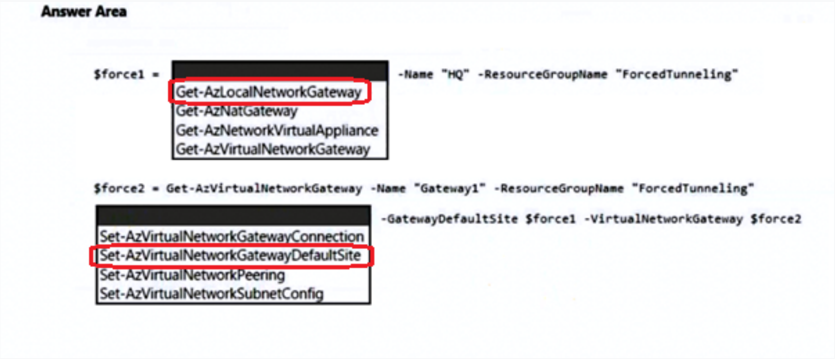
- Get-AzLocalNetworkGateway
- Get-AzNatGateway
- Get-AzNetworkVirtualAppliance
- Get-AzVirtualNetworkGateway

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

- Set-AzVirtualNetworkGatewayConnection
- Set-AzVirtualNetworkGatewayDefaultSite
- Set-AzVirtualNetworkPeering
- Set-AzVirtualNetworkSubnetConfig

Hide Solution Discussion 4

Correct Answer:



Answer Area

```
$force1 = [▼] -Name "HQ" -ResourceGroupName "ForcedTunneling"
```

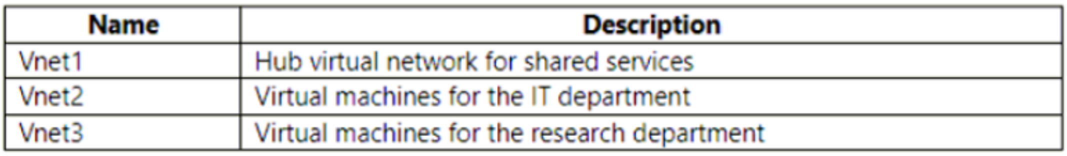
- [✓ Get-AzLocalNetworkGateway]
- Get-AzNatGateway
- Get-AzNetworkVirtualAppliance
- Get-AzVirtualNetworkGateway

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

- Set-AzVirtualNetworkGatewayConnection
- [✓ Set-AzVirtualNetworkGatewayDefaultSite]
- Set-AzVirtualNetworkPeering
- Set-AzVirtualNetworkSubnetConfig

Question #16 *Topic 1*

You are planning an Azure deployment that will contain three virtual networks in the East US Azure region as shown in the following table.



Name	Description
Vnet1	Hub virtual network for shared services
Vnet2	Virtual machines for the IT department
Vnet3	Virtual machines for the research department

A Site-to-Site VPN will connect Vnet1 to your company's on-premises network.

You need to recommend a solution that ensures that the virtual machines on all the virtual networks can communicate with the on-premises network. The solution must minimize costs.

What should you recommend for Vnet2 and Vnet3?

A. VNet-to-VNet VPN connections

B. peering **Most Voted**

C. service endpoints

D. route tables

Hide Solution Discussion 8

Correct Answer: *B*

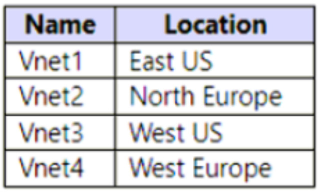
Community vote distribution

B (100%)

Question #17 *Topic 1*

Your company has an office in New York.

The company has an Azure subscription that contains the virtual networks shown in the following table.



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

You need to connect the virtual networks to the office by using ExpressRoute. The solution must meet the following requirements:

- The connection must have up to 1 Gbps of bandwidth.
- The office must have access to all the virtual networks.
- Costs must be minimized.

How many ExpressRoute circuits should be provisioned, and which ExpressRoute SKU should you enable?

A. one ExpressRoute Premium circuit **Most Voted**

B. two ExpressRoute Premium circuits

C. four ExpressRoute Standard circuits

D. one ExpressRoute Standard circuit

Hide Solution Discussion 17

Correct Answer: *A*

Community vote distribution

A (100%)

Question #18 *Topic 1*

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 **Most Voted**
D. VpnGw5AZ

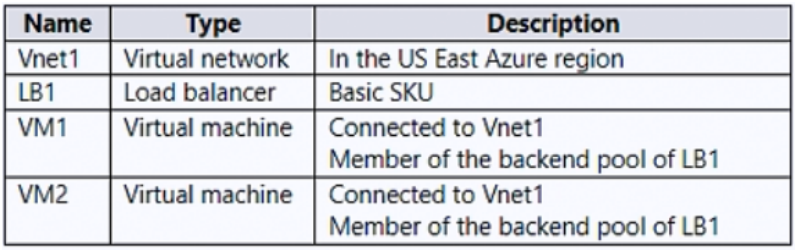
Hide Solution | Discussion 10

Correct Answer: *C*

Community vote distribution
C (100%)

Question #19 *Topic 1*

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



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

You create a virtual network named Vnet2 in the West US region.

You plan to enable peering between Vnet1 and Vnet2.

You need to ensure that the virtual machines connected to Vnet2 can connect to VM1 and VM2 via LB1.

What should you do?

A. From the Peerings settings of Vnet2, set Traffic forwarded from remote virtual network to Allow.
B. Change the Floating IP configurations of LB1.
C. From the Peerings settings of Vnet1, set Traffic forwarded from remote virtual network to Allow.
D. Change the SKU of LB1. **Most Voted**

Hide Solution | Discussion 12

Correct Answer: *D*

Community vote distribution
D (100%)

Question #20 *Topic 1*

DRAG DROP

-

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

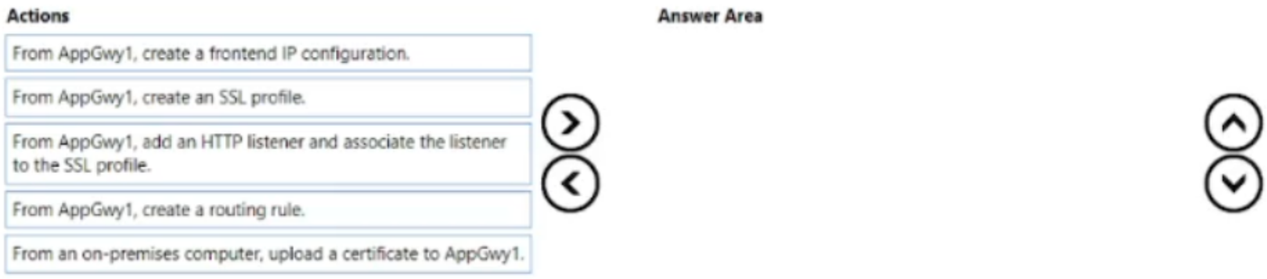
You have an Azure subscription.

You deploy an Azure application gateway named AppGwy1 and perform the following actions:

- Configure an HTTP listener
- Associate a routing rule with the listener

You need to configure AppGwy1 to perform mutual authentication for requests from domain-joined computers to contoso.com.

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



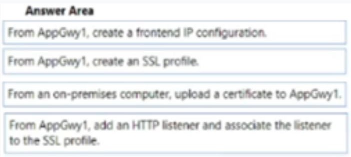
Actions

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

Answer Area

Hide Solution Discussion 20

Correct Answer:

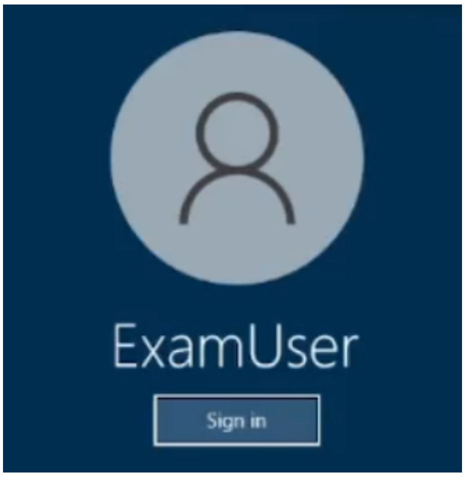


Answer Area

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

Question #21 *Topic 1*

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.

Hide Solution Discussion 4

Correct Answer:

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

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

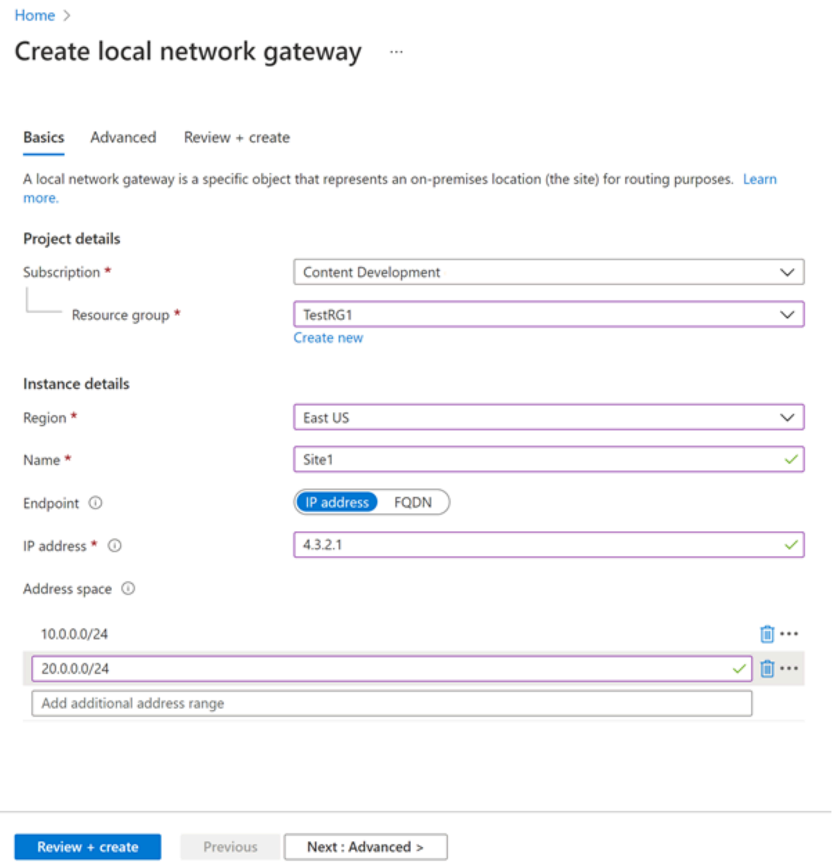
Step 1: From the Azure portal, in Search resources, services, and docs (G+/) type local network gateway. Locate local network gateway under Marketplace in the search results and select it. This opens the Create local network gateway page.

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

* Select Endpoint type: IP address

* Endpoint: Enter 131.107.50.60 (The Firewall public IP address)
(IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device, select the IP address option and fill in the IP address as shown in the example. This is the public IP address of the VPN device that you want Azure VPN gateway to connect to. If you don't have the IP address right now, you can use the values shown in the example, but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure won't be able to connect.)
* Address Space: Enter 10.10.0.0/16 (The internal address range)

Select the endpoint type for the on-premises VPN device - IP address or FQDN (Fully Qualified Domain Name).
IP address: If you have a static public IP address allocated from your Internet service provider for your VPN device.



Create local network gateway ...

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

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

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.

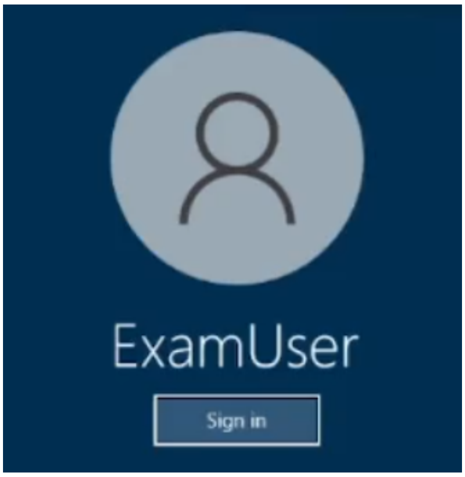
Step 5: Select Create to create the local network gateway object.

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

Question #22

Topic 1

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.

Hide Solution   Discussion 7

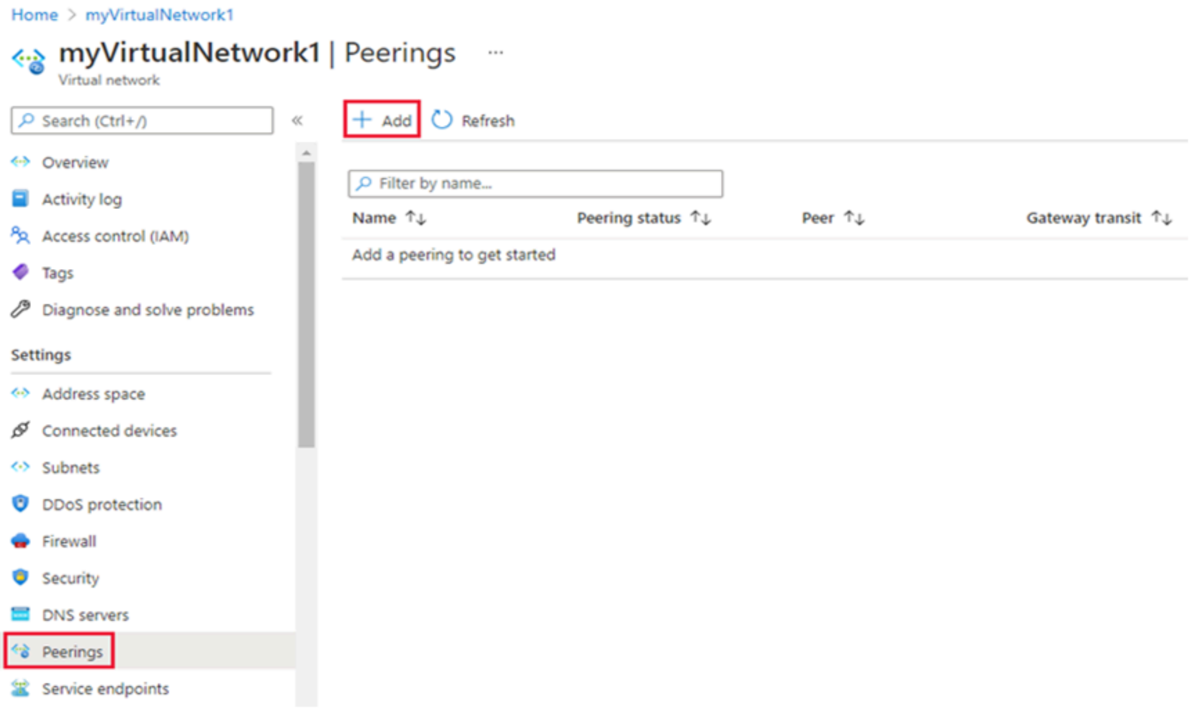
Correct Answer:

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.

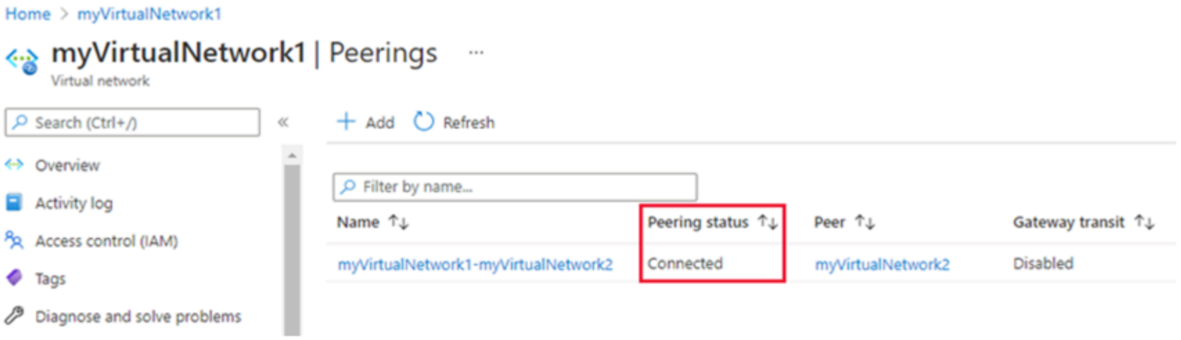
Step 2: Under Settings, select Peerings, and then select + Add, as shown in the following picture:



Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓
Add a peering to get started			

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:



Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓
myVirtualNetwork1-myVirtualNetwork2	Connected	myVirtualNetwork2	Disabled

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 #23 *Topic 1*

HOTSPOT

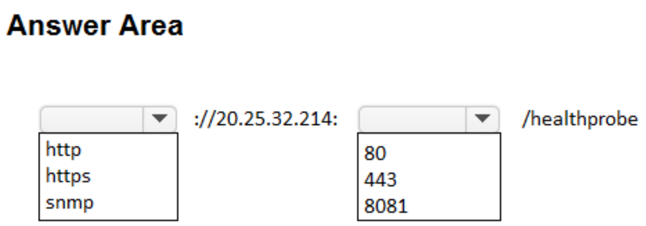
-

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

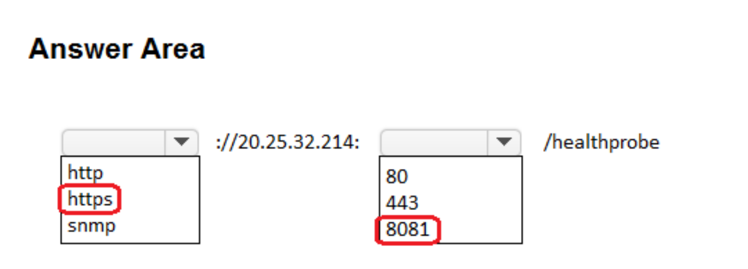
http
https
snmp

80
443
8081

Hide Solution

Discussion 2

Correct Answer:



Answer Area

▼ ://20.25.32.214: ▼ /healthprobe

http
[✓ https]
snmp

80
443
[✓ 8081]

Question #24 *Topic 1*

HOTSPOT
-

You have an on-premises datacenter.

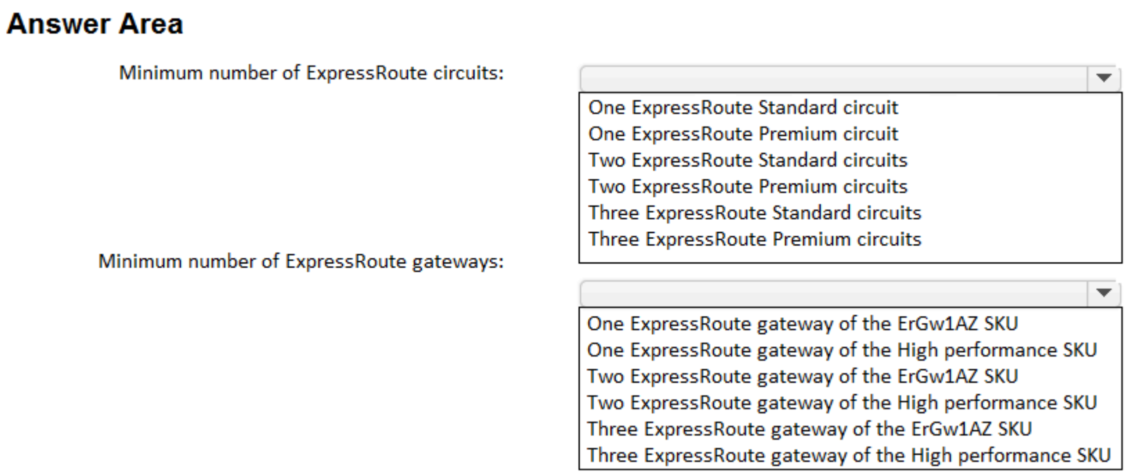
You have an Azure subscription that contains 10 virtual machines and a virtual network named VNet1 in the East US Azure region. The virtual machines are connected to VNet1 and replicate across three availability zones.

You need to connect the datacenter to VNet1 by using ExpressRoute. The solution must meet the following requirements:

• Maintain connectivity to the virtual machines if two availability zones fail.
• Support 1000-Mbps connections.
• Minimize costs.

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

NOTE: Each correct selection is worth one point.



Answer Area

Minimum number of ExpressRoute circuits:

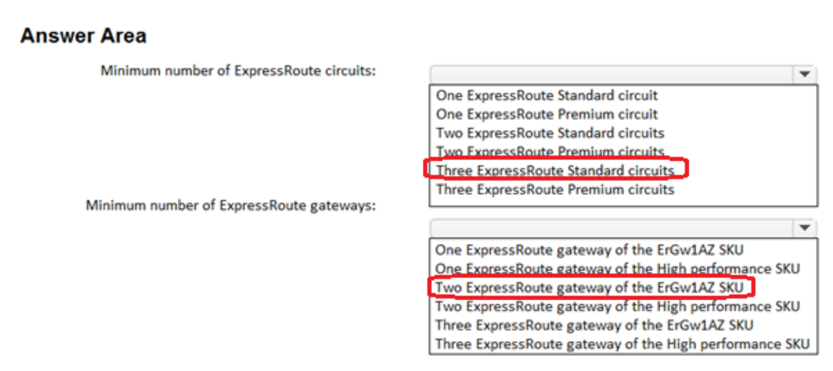
- One ExpressRoute Standard circuit
- One ExpressRoute Premium circuit
- Two ExpressRoute Standard circuits
- Two ExpressRoute Premium circuits
- Three ExpressRoute Standard circuits
- Three ExpressRoute Premium circuits

Minimum number of ExpressRoute gateways:

- One ExpressRoute gateway of the ErGw1AZ SKU
- One ExpressRoute gateway of the High performance SKU
- Two ExpressRoute gateway of the ErGw1AZ SKU
- Two ExpressRoute gateway of the High performance SKU
- Three ExpressRoute gateway of the ErGw1AZ SKU
- Three ExpressRoute gateway of the High performance SKU

Hide Solution Discussion 24

Correct Answer:



Answer Area

Minimum number of ExpressRoute circuits:

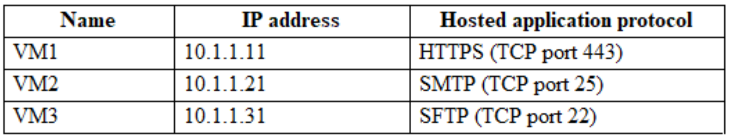
- One ExpressRoute Standard circuit
- One ExpressRoute Premium circuit
- Two ExpressRoute Standard circuits
- Two ExpressRoute Premium circuits
- [✓ Three ExpressRoute Standard circuits]
- Three ExpressRoute Premium circuits

Minimum number of ExpressRoute gateways:

- One ExpressRoute gateway of the ErGw1AZ SKU
- One ExpressRoute gateway of the High performance SKU
- [✓ Two ExpressRoute gateway of the ErGw1AZ SKU]
- Two ExpressRoute gateway of the High performance SKU
- Three ExpressRoute gateway of the ErGw1AZ SKU
- Three ExpressRoute gateway of the High performance SKU

Question #25 Topic 1

You have an Azure subscription that contains a virtual network named VNet1 and the virtual machines shown in the following table.



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

All the virtual machines are connected to Vnet1.

You need to ensure that the applications hosted on the virtual machines can be accessed from the internet. The solution must ensure that the virtual machines share a single public IP address.

What should you use?

A. an internal load balancer

B. Azure Application Gateway

C. a NAT gateway

D. a public load balancer Most Voted

Hide Solution Discussion 14

Correct Answer: *D*

Community vote distribution

D (100%)

Question #26 *Topic 1*

Case Study -

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

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

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

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

Overview -

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

Existing Environment -

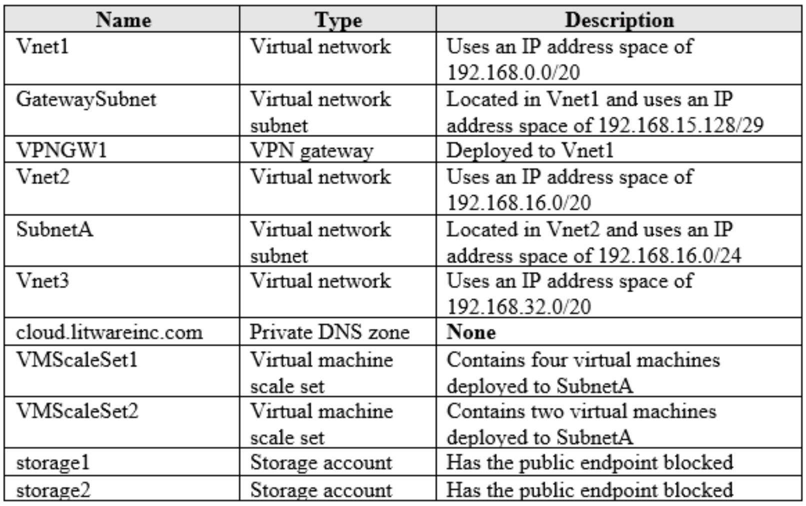
Hybrid Environment -

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

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

Azure Environment -

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

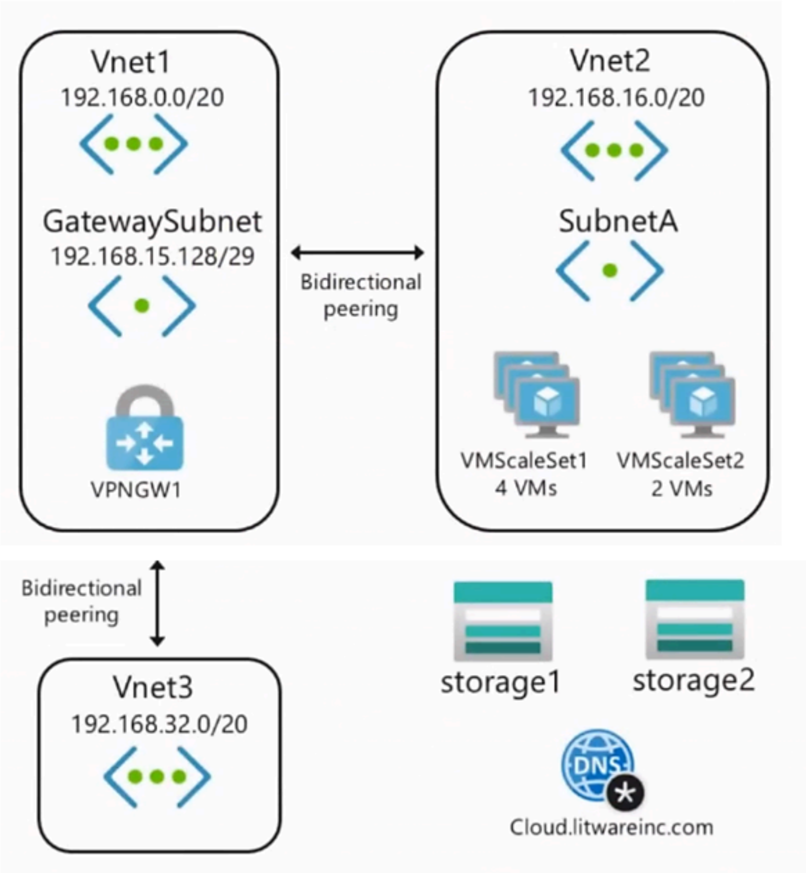


Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA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

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.

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. Most Voted

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. Most Voted

Hide Solution Discussion 10

Correct Answer: *AE*

Community vote distribution

BE (82%) AE (18%)

Question #27 *Topic 1*

HOTSPOT
-

You have an Azure subscription.

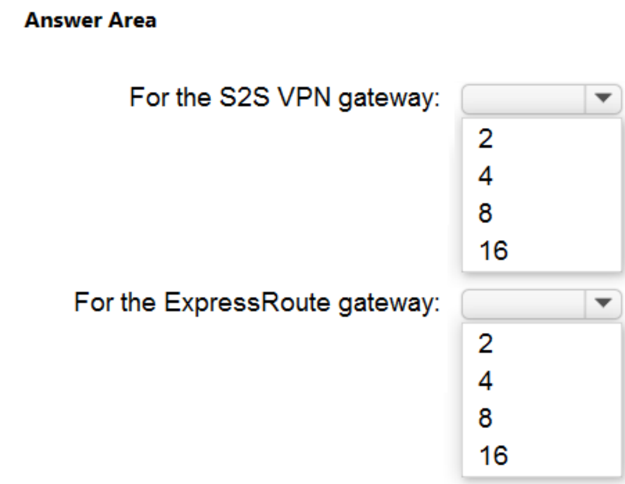
You plan to use Azure Virtual WAN.

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.



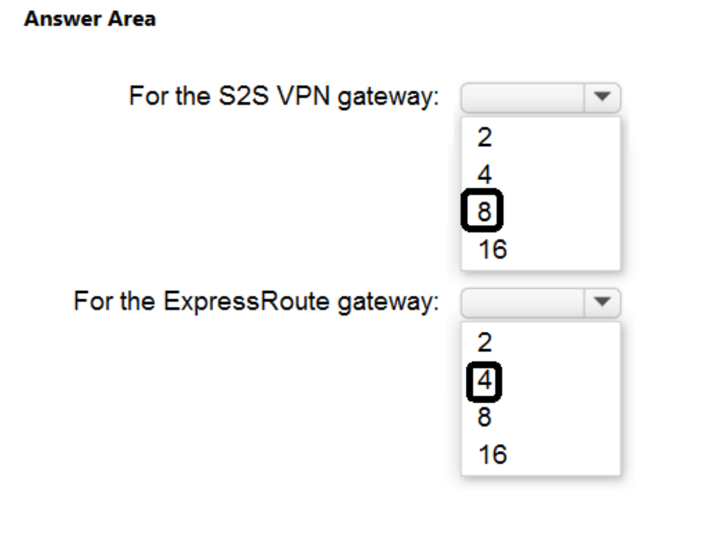
Answer Area

For the S2S VPN gateway: 2 / 4 / 8 / 16

For the ExpressRoute gateway: 2 / 4 / 8 / 16

Hide Solution Discussion 4

Correct Answer:



Answer Area

For the S2S VPN gateway: 2 / 4 / [✓ 8] / 16

For the ExpressRoute gateway: 2 / [✓ 4] / 8 / 16

Next Questions