



- Expert Verified, Online, **Free**.

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
- B. ExpressRoute Direct
- C. ExpressRoute Premium
- D. ExpressRoute Standard

**Correct Answer:** A

Reference:

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

*Community vote distribution*

A (88%) 13%

👤 **Tightbot** Highly Voted 6 months, 2 weeks ago

**Selected Answer: A**

Expressroute Local supports this particular networking scenario for two reasons. 1) The Washington DC peering location has East US as its Local Azure region. So, you don't need access to all the Geopolitical locations in order to connect the on-prem DC to Azure. Which means you won't necessarily need Expressroute standard.

2) ExpressRoute Local is a more economical solution compared to the standard.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#what-are-the-benefits-of-expressroute-local>  
<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations-providers#global-commercial-azure>

upvoted 11 times

👤 **ESAJRR** Most Recent 2 months, 3 weeks ago

**Selected Answer: A**

Correct.

upvoted 1 times

👤 **saurabhjsshukla** 3 months ago

Circuit bandwidth Local Standard Premium Inbound Outbound  
1 Gbps \$1,200 \$5,700 \$6,450 Unlimited Unlimited

So Answer is Expressroute Local (Option A)

upvoted 1 times

👤 **dani999** 4 months, 4 weeks ago

**Selected Answer: A**

-Local

(if available) provides free egress data transfer and gives you access to only 1-2 Azure regions in the same metro as your circuit.

-Standard

gives you access to all Azure regions in the same geopolitical region as your circuit.

-Premium provides support for more than 4K routes, ability to connect to more than 10 virtual networks, and global connectivity. Premium also gives you access to your services deployed worldwide.

upvoted 1 times

👤 **TJ001** 5 months ago

will go with A - one region and unlimited data is fulfilled. It is a classic use case for local SKU

upvoted 1 times

👤 **Naish2006** 6 months ago

Exam 20/12

upvoted 1 times

👤 **nstromer89** 6 months, 1 week ago

Correct one is A

upvoted 1 times

✉ **IHensch** 6 months, 2 weeks ago

**Selected Answer: D**

To minimize costs and support up to 1 Gbps, you should create ExpressRoute Standard circuits. ExpressRoute Standard circuits support up to 1 Gbps and are available with ExpressRoute Unlimited data plans, which provide a cost-effective solution for high-bandwidth connectivity. ExpressRoute Local and ExpressRoute Direct circuits are not suitable for this scenario because they do not support the required bandwidth, and ExpressRoute Premium circuits are not cost-effective for this scenario because they are more expensive than ExpressRoute Standard circuits.

upvoted 2 times

✉ **EdwardY** 4 months, 1 week ago

"Compared to a Standard ExpressRoute circuit, a Local circuit has the same set of features except:

Scope of access to Azure regions as described above

ExpressRoute Global Reach isn't available on Local"

Still A

upvoted 2 times

✉ **gunjant25** 9 months ago

ExpressRoute local, standard, global offer unlimited data plans.

ExpressRoute local: access azure region locally

ExpressRoute Standard: access azure multiple regions within a geopolotical location.

ExpressRoute Global: access azure regions globally/all over the world

upvoted 4 times

✉ **n0t4u2c** 9 months ago

Wouldn't the answer be ExpressRoute Premium as that allows for unlimited data on both inbound and outbound traffic? Local only allows for unlimited inbound per the Microsoft document.

upvoted 1 times

✉ **paweu** 9 months, 1 week ago

**Selected Answer: A**

so as in my previous message, A

upvoted 1 times

✉ **paweu** 9 months, 1 week ago

Looks ok

<https://docs.microsoft.com/pl-pl/azure/expressroute/expressroute-faqs#what-is-expressroute-local>

upvoted 1 times

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

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

**Correct Answer: B**

Reference:

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

*Community vote distribution*

B (100%)

 **walkwolf3** Highly Voted 1 year, 7 months ago  
B. a RADIUS server

AD Domain authentication allows users to connect to Azure using their organization domain credentials. It requires a RADIUS server that integrates with the AD server.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>  
upvoted 14 times

 **sserna** Most Recent 5 months ago  
En examen 20/01/2023  
upvoted 1 times

 **TJ001** 5 months ago  
correct Answer B  
upvoted 1 times

 **nstromer89** 6 months, 1 week ago  
It's Radius server. Please check the Documentation it is clearly given.  
upvoted 1 times

 **nstromer89** 6 months, 1 week ago  
correct answer B  
upvoted 1 times

 **IHensch** 6 months, 2 weeks ago  
Selected Answer: B  
The correct answer is B. a RADIUS server.

In order to support the VPN authentication for your Azure Point-to-Site (P2S) VPN using OpenVPN, you will need to deploy a RADIUS server on your on-premises network. The RADIUS server will be used to authenticate users who are trying to connect to the VPN using their Active Directory credentials. This will allow you to securely and efficiently manage user access to the VPN.

A certification authority is not necessary for this scenario, because you are not using certificates for authentication. Similarly, an Azure key vault is not needed, because you are not using keys for authentication. Azure Active Directory (Azure AD) Application Proxy is not relevant to this scenario, because it is used for publishing web applications, not for VPN authentication.  
upvoted 4 times

 **jilguens** 9 months, 3 weeks ago  
Selected Answer: B  
radius server  
upvoted 2 times

 **1particle** 10 months, 3 weeks ago  
B.  
AD Domain authentication allows users to connect to Azure using their organization domain credentials. It requires a RADIUS server that integrates with the AD server. Organizations can also leverage their existing RADIUS deployment.  
<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#authenticate-using-active-directory-ad-domain-server>

upvoted 3 times

 **zerocool114** 11 months, 2 weeks ago

correct, on exam today

upvoted 1 times

 **wooyourdaddy** 11 months, 2 weeks ago

**Selected Answer: B**

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

upvoted 1 times

 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam 6/28/22

upvoted 1 times

 **kogunribido** 11 months, 4 weeks ago

This came out 6/27/2022

upvoted 1 times

 **Edward1** 1 year, 2 months ago

**Selected Answer: B**

I think the correct answer is B: AD Domain authentication allows users to connect to Azure using their organization domain credentials. It requires a RADIUS server that integrates with the AD server. Organizations can also leverage their existing RADIUS deployment.

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

upvoted 1 times

 **jj22222** 1 year, 2 months ago

**Selected Answer: B**

B. a RADIUS server

upvoted 1 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **d0bermannn** 1 year, 4 months ago

**Selected Answer: B**

B. a RADIUS server is correct

upvoted 1 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

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

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

NOTE: Each correct selection is worth one point.

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

**Correct Answer:** AD

Reference:

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

*Community vote distribution*

AD (100%)

 **crawfish**  1 year, 7 months ago

Looks like the question number got changed/updated. Now, this question is around setting up BGP for a Site-to-Site VPN .

The given answers: A)Virtual Network Gateways and D) Local Network Gateways are correct as they are the key component required to setup S2S VPN tunnel.

upvoted 18 times

 **IHensch**  6 months, 2 weeks ago

**Selected Answer: AD**

The correct answers are A. a virtual network gateway and D. a local network gateway.

To configure BGP for a Site-to-Site VPN connection between a datacenter and Azure, you will need to configure a virtual network gateway and a local network gateway. The virtual network gateway will be used to establish the VPN connection between your datacenter and Azure, and the local network gateway will be used to define the on-premises network that you want to connect to Azure.

Azure Application Gateway, Azure Firewall, and Azure Front Door are not relevant to this scenario, because they are not used for configuring BGP for a Site-to-Site VPN connection.

upvoted 5 times

 **JennyHuang36**  3 months, 3 weeks ago

In exam Feb, 2023

upvoted 2 times

 **JennyHuang36** 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 1 times

 **sserna** 5 months ago

En examen 20/01/2023

upvoted 1 times

 **TJ001** 5 months ago

Correct Answers are A and D

upvoted 2 times

 **sshera** 5 months, 2 weeks ago

in exam 4jan23

upvoted 2 times

 **Naish2006** 6 months ago

in exam 20/12

upvoted 1 times

 **nstromer89** 6 months, 1 week ago

Answer is AD

upvoted 1 times

 **1particle** 10 months, 3 weeks ago

A.

If the IPsec tunnel fails to establish, Azure will keep retrying every few seconds. For this reason, troubleshooting "VPN down" issues is very convenient on IKEDiagnosticLog because you do not have to wait for a specific time to reproduce the issue.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics#IKEDiagnosticLog>  
upvoted 3 times

 **1particle** 10 months, 3 weeks ago

A & D

PART 1 STEP 2: Create the VPN gateway for TestVNet1 with BGP parameters  
In this step, you create a VPN gateway with the corresponding BGP parameters.

In the Azure portal, navigate to the Virtual Network Gateway resource from the Marketplace, and select Create.

PART2 STEP 1: Configure BGP on the local network gateway

In this step, you configure BGP on the local network gateway.

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

upvoted 2 times

 **zerocool114** 11 months, 2 weeks ago

on exam today

upvoted 1 times

 **Edward1** 1 year, 2 months ago

**Selected Answer: AD**

I think the correct answer is A y D:

-To establish a cross-premises connection, you need to create a Local Network Gateway to represent your on-premises VPN device, and a Connection to connect the VPN gateway with the local network gateway.

-BGP requires a Route-Based VPN gateway, and also the addition parameter, -Asn, to set the ASN (AS Number) for VNet.

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

upvoted 2 times

 **milan92stankovic** 1 year, 2 months ago

**Selected Answer: AD**

Correct answer A & D.

upvoted 2 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **d0bermannn** 1 year, 4 months ago

**Selected Answer: AD**

A&D is correct as virt NGW & local NGW are prereq for s2s vpn

upvoted 1 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

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

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

Which diagnostic log should you review?

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

**Correct Answer: A**

Reference:

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

*Community vote distribution*

A (100%)

 **crawfish** Highly Voted 1 year, 7 months ago

Answer is correct - IKEDiagnosticLog

IKEDiagnosticLog = The IKEDiagnosticLog table offers verbose debug logging for IKE/IPsec. This is very useful to review when troubleshooting disconnections, or failure to connect VPN scenarios.

GatewayDiagnosticLog = Configuration changes are audited in the GatewayDiagnosticLog table.

TunnelDiagnosticLog = The TunnelDiagnosticLog table is very useful to inspect the historical connectivity statuses of the tunnel.

RouteDiagnosticLog = The RouteDiagnosticLog table traces the activity for statically modified routes or routes received via BGP.

P2SDiagnosticLog = The last available table for VPN diagnostics is P2SDiagnosticLog. This table traces the activity for Point to Site.

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

upvoted 43 times

 **TJ001** Most Recent 5 months ago

correct Answer

upvoted 1 times

 **charada83** 8 months, 3 weeks ago

correct

upvoted 1 times

 **1particle** 10 months, 3 weeks ago

A.

If the IPsec tunnel fails to establish, Azure will keep retrying every few seconds. For this reason, troubleshooting "VPN down" issues is very convenient on IKEDiagnosticLog because you do not have to wait for a specific time to reproduce the issue.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics#IKEDiagnosticLog>

upvoted 1 times

 **derrrp** 11 months ago

If you have trouble remembering this question and you start to think the answer is TunnelDiagnosticLog, then you need to remember to tunnel deeper - as the answer is IKEDiagnosticLog. Although it is very easy to immediately see the word tunnel thinking it may be the right answer.

upvoted 1 times

 **Edward1** 1 year, 2 months ago

Selected Answer: A

A.

<https://docs.microsoft.com/es-es/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics>

upvoted 1 times

 **dObermann** 1 year, 4 months ago

Selected Answer: A

A. IKEDiagnosticLog

upvoted 1 times

 **Joshalom** 1 year, 4 months ago

on exam 6/2/2022  
upvoted 1 times

 **Pravda** 1 year, 5 months ago

On exam 1/6/2022  
upvoted 1 times

 **AidenYoukhana** 1 year, 5 months ago

**Selected Answer: A**  
IKEDiagnosticLog  
upvoted 4 times

 **dusty\_dev** 1 year, 6 months ago

same question in whizlabs is marked gatewaydiagnosticlogs but i feel ikediagnosticlog is more accurate.  
upvoted 3 times

 **Pamban** 1 year, 6 months ago

appeared on exam 5th Dec 2021  
upvoted 1 times

 **chreaxa** 1 year, 7 months ago

Correct  
upvoted 1 times

 **RandomUser** 1 year, 8 months ago

Yeah, that's the most detailed log. The only that would help you troubleshooting the most common issue - IKE errors.  
upvoted 1 times

 **AmalMOQ** 1 year, 8 months ago

correct !  
The IKEDiagnosticLog table offers verbose debug logging for IKE/IPsec. This is very useful to review when troubleshooting disconnections, or failure to connect VPN scenarios.  
upvoted 3 times

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
- 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

**Correct Answer: BG**

Reference:

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

*Community vote distribution*

BG (100%)

 **omgMerrick** Highly Voted 4 months, 1 week ago

**Selected Answer: BG**

- B. a virtual network gateway
- G. a local network gateway

To establish a Site-to-Site VPN connection between an on-premises datacenter and an Azure virtual network, you must include two resources in your plan: a virtual network gateway in Azure and a local network gateway in the datacenter.

A virtual network gateway acts as the VPN endpoint in Azure and allows the VPN connection to be established with the datacenter.

A local network gateway represents the on-premises VPN device and its IP address. This allows Azure to establish a VPN connection with the datacenter over the public Internet.

The virtual network gateway and the local network gateway work together to create the VPN connection, allowing secure communication between the datacenter and the virtual network.

upvoted 6 times

 **ESAJRR** Most Recent 2 months, 3 weeks ago

**Selected Answer: BG**

It's corrects.

upvoted 2 times

 **sserna** 5 months ago

En examen 20/01/2023

upvoted 1 times

 **TJ001** 5 months ago

BG is correct

upvoted 1 times

 **sshera** 5 months, 2 weeks ago

in exam 4jan23

upvoted 1 times

 **MyPractice** 6 months, 1 week ago

This came in Dec 2022

upvoted 1 times

 **HasanHHH** 8 months, 2 weeks ago

**Selected Answer: BG**

Main Component of S2S VPN

local network gateway & virtual network gateway

upvoted 3 times

✉ **BlackZero9** 9 months ago

**Selected Answer: BG**

similar to another question with less options

upvoted 3 times

✉ **1particle** 10 months, 3 weeks ago

B & G.

In Search resources, services, and docs (G+) type virtual network gateway. Locate Virtual network gateway in the Marketplace search results and select it to open the Create virtual network gateway page.

<https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal#create-the-gateway>

The local network gateway is a specific object that represents your on-premises location (the site) for routing purposes.

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

upvoted 2 times

✉ **zerocool114** 11 months, 2 weeks ago

on exam today

upvoted 1 times

✉ **kogunribido** 11 months, 4 weeks ago

This came out 6/27/2022

upvoted 1 times

✉ **milan92stankovic** 1 year ago

**Selected Answer: BG**

Correct Answer

upvoted 3 times

✉ **Whatsamattr81** 1 year ago

B and G... None of the other things on there own will do S2S

upvoted 2 times

**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

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>

✉️  **nawere**  1 year, 1 month ago

The correct answer is route based and two virtual network gateways - one for ExpressRoute connection (ExpressRoute virtual network gateway) and the second for the VPN connection (VPN virtual network gateway).

Check the architecture and read the description at the source.

Source: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute-vpn-failover>  
upvoted 69 times

✉️  **Libaax01** 3 months, 2 weeks ago

You are 100 Percent! correct, in a Virtual Network (VNET) you can have two Gateways.

- One VPN Gateway
- One Express Route Gateway

upvoted 1 times

✉️  **Libaax01** 3 months, 2 weeks ago

in the question, they asked "The solution must use ExpressRoute(Express Route Gateway) and support failing over to a Site-to-Site VPN(VPN Gateway) so a total of two Network Virtual Gateways are required.

upvoted 1 times

✉️👤 **MightyMonarch74** 4 months ago

all you have to do is look at the architecture diagram at <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute-vpn-failover>

This confirms 1 ER gateway and 1 VPN gateway (both in the gateway subnet)

upvoted 1 times

✉️👤 **lasmas** 1 year ago

how about this?

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

maybe 1 is correct as via powershell you can do it

upvoted 1 times

✉️👤 **jellybiscuit** 8 months, 3 weeks ago

The doc is correct. You are misreading it.

"If you have a virtual network that has only one virtual network gateway (let's say, Site-to-Site VPN gateway) and you want to add another gateway of a different type (let's say, ExpressRoute gateway), "

Another gateway of a different type. Two total.

upvoted 5 times

✉️👤 **NotBillGates** 1 year ago

No, that just means you can have an ExpressRoute gateway and a virtual network gateway in the same subnet, hence the term co-existence, they co-exist together. ExpressRoute Gateways don't provide S2S, hence, you need two.

upvoted 3 times

✉️👤 **rac\_sp** 11 months, 1 week ago

This is correct and I did a lab that worked really fine with this architecture

upvoted 1 times

✉️👤 **henryhung** [Most Recent] 2 months, 1 week ago

Route-based

2 virtual network gateways

From ChatGPT Plus (GPT-4)

For this scenario, the routing type that should be configured is "Route-based" because it allows for more flexibility in routing and is recommended for ExpressRoute connections.

As for the number of virtual network gateways, you should deploy 2 virtual network gateways for redundancy and failover purposes, one for the ExpressRoute connection and another for the Site-to-Site VPN connection. This is because a virtual network gateway can only be associated with one connection at a time. So, having two virtual network gateways allows you to switch between them if one of the connections fails.

upvoted 1 times

✉️👤 **Nibo** 3 months, 2 weeks ago

its route based but you need two VNG

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroute-vpn-failover>

upvoted 2 times

✉️👤 **mVic** 4 months, 2 weeks ago

Route based and 2 Gateways of VPN and ExpressRoute type

upvoted 2 times

✉️👤 **sserna** 5 months ago

En examen 20/01/2023

upvoted 2 times

✉️👤 **TJ001** 5 months ago

Route based and 2 Gateways of VPN and ExpressRoute type

upvoted 4 times

✉️👤 **NoeHdzMII** 5 months, 1 week ago

Route based and 2 Gateways, as you can see in the Powershell commands to coexist

\$gw = New-AzVirtualNetworkGateway -Name "VPNGateway" -ResourceGroupName

\$gw = New-AzVirtualNetworkGateway -Name "ERGateway" -ResourceGroupName

upvoted 1 times

✉️👤 **jozamaymen** 5 months, 2 weeks ago

Correct answer:

You choose a Route-based when you create a VNG. Then in VNG you can add multi connection (S2S) and another one with ExpressRoute. No need to new VNG.

upvoted 1 times

✉ **sshera** 5 months, 2 weeks ago

in exam 4jan23

upvoted 2 times

✉ **varundhiman** 6 months ago

Correct Answer is route Based and 2 Gateway S2S gateway and ER Gateway. Though you can use the same gateway subnet for both of them.

upvoted 1 times

✉ **MyPractice** 6 months, 1 week ago

This came in Dec 2022

upvoted 1 times

✉ **Pradh** 8 months, 2 weeks ago

ROUTE BASED

2 VNG

This is the right answer .

upvoted 3 times

✉ **HasanHHH** 8 months, 2 weeks ago

The correct answer is route based and two virtual network gateways

ExpressRoute virtual network gateway. The ExpressRoute virtual network gateway enables the VNet to connect to the ExpressRoute circuit used for connectivity with your on-premises network.

VPN virtual network gateway. The VPN virtual network gateway enables the VNet to connect to the VPN appliance in the on-premises network. The VPN virtual network gateway is configured to accept requests from the on-premises network only through the VPN appliance

upvoted 2 times

✉ **Sai\_cebu** 8 months, 2 weeks ago

Possible, when you add connection on the Vnet GW connection type options are : Vnet-to-Vnet, Site-to-site and ExpressRoute. I'll go with 1 Vnet Gateway

upvoted 1 times

✉ **BlackZeros** 9 months ago

two gateways = 1 gateway should be onprem (for site to site) and 2nd one is combined in Azure for S2S and ER.

upvoted 1 times

✉ **AdityaGupta** 9 months, 1 week ago

Route Based and 2 VNet Gateway, as gateway type is different for ER and S2S connections.

upvoted 1 times

✉ **GetulioJr** 9 months, 1 week ago

Route Based

2

upvoted 2 times

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
- B. 2
- C. 3
- D. 4
- E. 5

**Correct Answer: A**

Reference:

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

*Community vote distribution*

A (86%) 14%

✉️  **Hawaii\_IT**  10 months, 1 week ago

Answer: A - 1

Managing Authorization

The circuit owner can share a circuit with up to 10 Azure subscriptions. The circuit owner can view who has been authorized to the circuit. The owner can revoke the authorization at any time.

<https://azure.microsoft.com/en-us/blog/enable-multiple-subscription-expressroute/#:~:text=The%20circuit%20owner%20can%20share,the%20authorization%20at%20any%20time.>

upvoted 17 times

✉️  **jellybiscuit** 8 months, 3 weeks ago

You are correct, though network topology can negate the ExpressRoute subscription limit anyway. For example, connect the ExpressRoute to a hub vnet and peer the subscription vnets to it.

upvoted 5 times

✉️  **AdityaGupta**  9 months ago

**Selected Answer: A**

1 Express Route Circuit standard sku would be good enough. With 1 er circuit you can connect upto 10 vnets and standard sku allows you to connect within same geopolitical region without additional cost.

upvoted 6 times

✉️  **Ajdfasudfo0** 6 months, 2 weeks ago

it's in the same metro, so local is fine

upvoted 2 times

✉️  **Ben\_88**  1 week, 2 days ago

**Selected Answer: A**

1 Express Route Circuit standard sku would be good enough. With 1 er circuit you can connect upto 10 vnets and standard sku allows you to connect within same geopolitical region without additional cost.

upvoted 1 times

 **ESAJRR** 1 month, 3 weeks ago

**Selected Answer: A**

Answer: A - 1

upvoted 1 times

 **khanda** 2 months, 1 week ago

**Selected Answer: A**

You can link up to 10 virtual networks to a standard ExpressRoute circuit. All virtual networks must be in the same geopolitical region when using a standard ExpressRoute circuit. West US and West US 2 are in the same Azure geopolitical region, so you would need only one ER circuits.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager#connect-a-vnet-to-a-circuit---different-subscription>

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations-providers>

upvoted 1 times

 **mauchi** 3 months ago

if the express route would be with a standard SKU, then yes, I think A - 1 express route would be enough

upvoted 1 times

 **Mo22** 4 months, 1 week ago

**Selected Answer: B**

B. 2

You need at least two ExpressRoute circuits to connect all three Azure subscriptions to the on-premises network. One circuit connects the West US Azure region and another circuit connects the West US 2 Azure region. All the resources in the subscriptions are in either the West US Azure region or the West US 2 Azure region, so you need to connect both regions.

upvoted 3 times

 **sapien45** 9 months, 1 week ago

**Selected Answer: A**

Not true for Local SKU though.

. With a Local SKU ExpressRoute circuit you can connect to resources in Azure regions in the same metro as the peering site. In this case, your on-premises network can access UK South Azure resources over ExpressRoute. For more information, see What is ExpressRoute Local?. When you configure a Standard SKU ExpressRoute circuit, connectivity to Azure resources will expand to all Azure regions in a geopolitical area.

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

upvoted 1 times

 **Ajdifasudfo0** 6 months, 2 weeks ago

same metro, so local is fine

upvoted 1 times

 **AdityaGupta** 9 months, 1 week ago

1 Express Route Circuit standard sku would be good enough. With 1 er circuit you can connect upto 10 vnets and standard sku allows you to connect within same geopolitical region without additional cost.

upvoted 1 times

 **Alessandro365** 9 months, 1 week ago

**Selected Answer: A**

Answer: A - 1

upvoted 1 times

 **Jamesat** 10 months, 2 weeks ago

**Selected Answer: A**

ExpressRoute circuits can be shared between subscriptions.

Correct answer is A

upvoted 3 times

 **iwikneerg** 10 months, 2 weeks ago

Looks like the correct answer is A

You can have an ExpressRoute Circuit going into one region and gain access to other regions from there...

Connectivity to all regions within a geopolitical region

You can connect to Microsoft in one of our peering locations and access regions within the geopolitical region.

For example, if you connect to Microsoft in Amsterdam through ExpressRoute. You'll have access to all Microsoft cloud services hosted in Northern and Western Europe. For an overview of the geopolitical regions, the associated Microsoft cloud regions, and corresponding ExpressRoute peering locations, see the ExpressRoute partners and peering locations article.

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction#connectivity-to-all-regions-within-a-geopolitical-region>

upvoted 2 times

✉  **iwikneerg** 10 months, 2 weeks ago  
<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations#locations>

See North America geopolitical region  
upvoted 1 times

✉  **milan92stankovic** 1 year, 1 month ago

**Selected Answer: A**

Answer: A  
upvoted 4 times

✉  **7254kazu** 1 year, 1 month ago

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-linkvnet-portal-resource-manager#connect-a-vnet-to-a-circuit---different-subscription>  
upvoted 3 times

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
- C. ExpressRoute Direct
- D. ExpressRoute Local

**Correct Answer: B**

Reference:

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

*Community vote distribution*

B (100%)

 **ESAJRR** 1 month, 3 weeks ago

**Selected Answer: B**

Global Reach classic

upvoted 1 times

 **Mo22** 4 months, 1 week ago

**Selected Answer: B**

B. ExpressRoute Global Reach

ExpressRoute Global Reach provides the ability to connect multiple Azure regions and on-premises locations with a single ExpressRoute circuit. In this scenario, you need to connect the Amsterdam office to the North Europe Azure region and the New York office to the East US Azure region. ExpressRoute Global Reach enables the communication between the on-premises computers in the Amsterdam office and the on-premises servers in the New York office through the ExpressRoute circuits. Hence, ExpressRoute Global Reach is the most suitable option to use in this scenario.

upvoted 2 times

 **TJ001** 5 months ago

Global Reach classic use case

upvoted 3 times

 **Takloy** 7 months, 2 weeks ago

**Selected Answer: B**

ExpressRoute Global Reach is the right answer.

upvoted 1 times

 **HasanHHH** 8 months, 2 weeks ago

**Selected Answer: B**

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

upvoted 3 times

 **jellybiscuit** 8 months, 3 weeks ago

**Selected Answer: B**

I am thinking global reach is the answer they're looking for. This assumes that the two offices do not have existing connectivity to each other. I don't like having to make that assumption though.

upvoted 1 times

 **AdityaGupta** 9 months, 1 week ago

**Selected Answer: B**

Express Route global reach is correct answer, since each data centre is connected to nearest Azure region by using ER circuit, you only need to enable Global Reach feature on bith ER circuit.

upvoted 1 times

 **Alessandro365** 9 months, 1 week ago

**Selected Answer: B**

ExpressRoute Global Reach

upvoted 1 times

 **azeem0077** 10 months ago

**Selected Answer: B**

ExpressRoute Global Reach is the correct answer

upvoted 2 times

 **iwikneerg** 10 months, 2 weeks ago

**Selected Answer: B**

With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks. In the above example, with the addition of ExpressRoute Global Reach, your San Francisco office (10.0.1.0/24) can directly exchange data with your London office (10.0.2.0/24) through the existing ExpressRoute circuits and via Microsoft's global network.

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

upvoted 3 times

 **1particle** 10 months, 3 weeks ago

B.  
With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks. In the above example, with the addition of ExpressRoute Global Reach, your San Francisco office (10.0.1.0/24) can directly exchange data with your London office (10.0.2.0/24) through the existing ExpressRoute circuits and via Microsoft's global network.

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

upvoted 3 times

 **derrp** 11 months ago

"Once the ExpressRoute circuits are connected..." Remember that the ExpressRoute has already been established. The ExpressRoute Global Reach service option is like the delicious sauce on top of the already-existing ExpressRoute

upvoted 4 times

 **derrp** 11 months ago

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

In the Microsoft Support Documentation, we're shown a diagram of an on-prem network connected to an Azure datacenter through an express route in one geopolitical region - and another on-prem datacenter connected to Azure in another geopolitical region. Two ExpressRoutes are shown. ExpressRoute Global Reach is the peering between these two ExpressRoutes despite being in different geopolitical regions.

upvoted 2 times

 **milan92stankovic** 1 year ago

**Selected Answer: B**

Correct answer - Global Reach!

upvoted 3 times

**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)

**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.



## Permissions requested Accept for your organization



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](#)

Cancel

Accept

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

The screenshot shows the Azure Active Directory interface. On the left, there's a sidebar with options like Overview, Manage (selected), Security, Activity, and Troubleshooting + Support. Under Manage, 'All applications' is selected. The main area shows a table of enterprise applications. The table has columns for NAME, HOMEPAGE URL, OBJECT ID, and APPLICATION ID. One row is visible for 'Azure VPN' with the URL 'https://www.microsoft.com'.

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>

✉️ **sapien45** Highly Voted 9 months, 1 week ago

Azure AD authentication is supported only for OpenVPN® protocol connections and requires the Azure VPN Client.  
<https://learn.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant>

upvoted 8 times

✉️ **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb,2023

upvoted 2 times

✉️ **sserna** 5 months ago

En examen 20/01/2023

upvoted 2 times

✉️ **TJ001** 5 months ago

correct answers

upvoted 1 times

 **sshera** 5 months, 2 weeks ago

in exam 04jan23

upvoted 2 times

 **MyPractice** 6 months, 1 week ago

This came in Dec 2022

upvoted 1 times

 **Takloy** 9 months, 1 week ago

The answer is correct!

Enterprise Application and OpenVPN (SSL).

upvoted 2 times

 **BillyB2022** 9 months, 2 weeks ago

Correct, enterprise application

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

upvoted 3 times

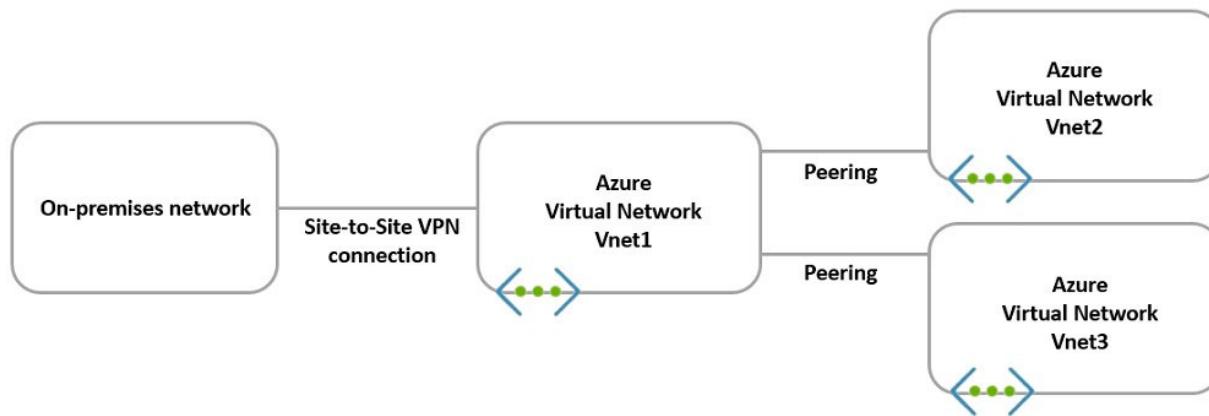
 **DerekKey** 9 months, 3 weeks ago

Correct

upvoted 2 times

**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 [\(i\)](#)

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

Traffic forwarded from remote virtual network [\(i\)](#)

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

Virtual network gateway or Route Server [\(i\)](#)

- 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 [\(i\)](#)

- Resource manager
- Classic

I know my resource ID [\(i\)](#)

Subscription\* [\(i\)](#)

Subscription1



Virtual network

Vnet2



Traffic to remote virtual network [\(i\)](#)

- 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 [\(i\)](#)

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

Traffic forwarded from remote virtual network [\(i\)](#)

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

Virtual network gateway or Route Server [\(i\)](#)

- 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 [\(i\)](#)

- Resource manager
- Classic

I know my resource ID [\(i\)](#)

Subscription\* [\(i\)](#)

Subscription1



Virtual network

Vnet1



Traffic to remote virtual network [\(i\)](#)

- 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"/>

**Correct 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"/>

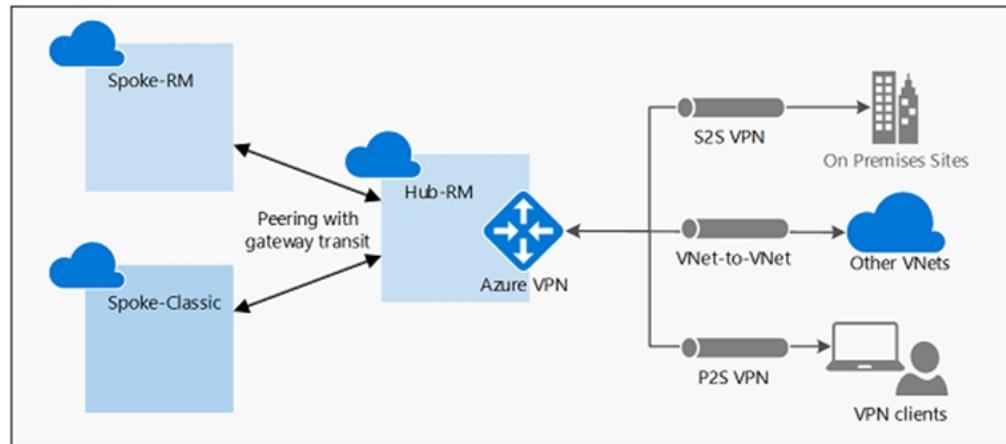
Box 1: Yes -

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>

✉  **amt2022**  4 months, 1 week ago

Correct answer Y,N,N.

Remember Azure VNET Peering is NON-Transitive. Meaning, only direct peered VNETs can talk to each other. To make it transitive you either use VNET Gateway or NVAs/Azure FireWall.

upvoted 6 times

✉  **Prutser2**  8 months, 1 week ago

correct, vnet1 cannot be a trnsit between vnets2 and 3, without using the gateway as transit

upvoted 6 times

✉  **omgMerrick**  3 months, 4 weeks ago

Answer is correct.

Y

N

N

upvoted 1 times

✉  **TJ001** 5 months ago

yes,no,no

upvoted 1 times

✉  **zukako** 5 months, 3 weeks ago

correct vnet1 not use its gateway for vnet2

upvoted 1 times

✉  **DeepMoon** 9 months ago

Doesn't the 2nd Link name on both those peerings are wrong matter?

upvoted 1 times

✉  **GetulioJr** 9 months, 1 week ago

Answer is correct, The option: Use the remote virtual network's gateway" is not enabled

upvoted 2 times

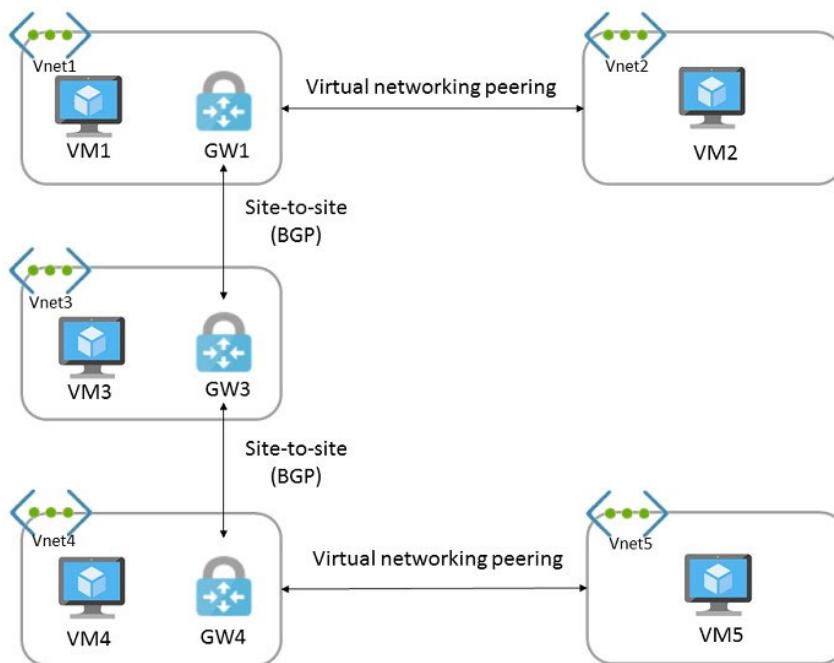
✉  **DerekKey** 9 months, 3 weeks ago

Correct

upvoted 3 times

**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	<b>None</b>	Enabled
Vnet2	Allow	Enabled	<b>None</b>
Vnet4	Allow	<b>None</b>	Enabled
Vnet5	Block	Enabled	<b>None</b>

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.

**Correct Answer:**

**Answer Area:**

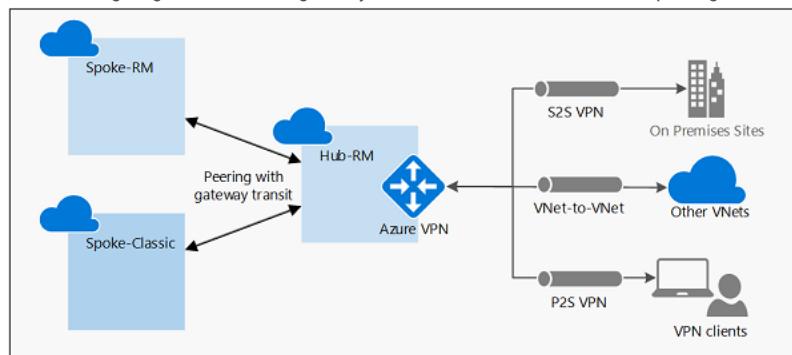
Statements	Yes	No
VM1 and VM4 can communicate.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VM2 and VM4 can communicate.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VM1 and VM5 can communicate.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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>

**zenithcsa1** Highly Voted 9 months, 2 weeks ago

YYY / tested in lab

VM1 and VM5 can communicate.

'Traffic to remove virtual network : Block' setting in Vnet5 does not block communication between VM5 and GW4, while it blocks communication between VM5 and VM4.

upvoted 22 times

**Aiwa23** 9 months, 2 weeks ago

it blocks communication from VNET5 to VNET4 but allows VNET4 to VNET5

upvoted 4 times

**Pratheeshp** 1 month, 1 week ago

How about the the return traffic VNET5 to VNET4 ?

upvoted 1 times

**zenithcsa1** 9 months, 1 week ago

That's not true. 'Block' option is about NSG's VirtualNetwork tag whether it contains network address of Vnet4 or not. When you choose 'block' and create security rules on VM5's NSG, VM5 still can communicate with resources in Vnet4.

upvoted 2 times

✉️ **A\_way** 9 months, 1 week ago

Could you pls clarify? This is referring the vnet peering settings not NSG

upvoted 6 times

✉️ **dani999** 4 months, 3 weeks ago

Microsoft:

NOTE: Selecting the Block all traffic to remote virtual network setting only changes the definition of the VirtualNetwork service tag. It doesn't fully prevent traffic flow across the peer connection, as explained in this setting description.

upvoted 1 times

✉️ **Alessandro365** Highly Voted 9 months ago

YYY, tested in lab.

vnet5 peering is disabled, but remote gateway is enabled, allowing the vm5 to be accessed from other vnets. Only VM4 cannot access VM5 (peering blocked).

Note that BGP needs to be configured, user routes does not work.

upvoted 8 times

✉️ **Oklama** Most Recent 4 weeks ago

YYY is correct

upvoted 1 times

✉️ **arnaudhelin** 2 months, 3 weeks ago

Hi everyone,

I tried a lot of configuration to test the last point. With wireshark on both sides, and traffic flow always on (ping and http request), the result is quite clear even if it is not logical at the first look. When you choose the option BLOCK on one side, the entire communication is blocked. If you want to have the "expected" behavior (vm4 to vm5 ok but not the other way), you must set a NSG with an explicit rule which allows the traffic.

upvoted 7 times

✉️ **mm2** 4 months, 2 weeks ago

YYY:

for 3rd:

- Select Block all traffic to the remote virtual network if you don't want traffic to flow to the peered virtual network by default. You can select this setting if you have peering between two virtual networks but occasionally want to disable default traffic flow between the two. You may find enabling/disabling is more convenient than deleting and re-creating peerings. When this setting is selected, traffic doesn't flow between the peered virtual networks by default; however, traffic may still flow if explicitly allowed through a network security group rule that includes the appropriate IP addresses or application security groups.

upvoted 1 times

✉️ **thainy** 1 month, 3 weeks ago

When this setting is selected, traffic doesn't flow between the peered virtual networks by default; however, traffic may still flow if explicitly allowed through a network security group rule that includes the appropriate IP addresses or application security groups.

There is no point to NSG so I think 3rd is NO

upvoted 2 times

✉️ **tester2023** 4 months, 3 weeks ago

YYN

To test the 'block' on the peering between vNet4 and vNet5 I did the following:

Deployed two vNets. On the second vNet, I selected the "Block all traffic to the remote virtual network" and the Portal displays "Resources in vnet-2 cannot communicate to resources in the vnet-1"

When I do a Connection Troubleshoot test, it fails with "Traffic blocked due to the following network security group rule: DefaultRule\_DenyAllInBound".

When I set the peering setting to "Allow (default)", the Connection Troubleshoot is successful.

upvoted 4 times

✉️ **mauchi** 4 months, 3 weeks ago

To me YYN seems correct.

I think the last option is a NO, bc the statement says "VM1 and VM5 can communicate" to me it implies a bidirectional communication. And the table states that Vnet 5 blocks traffic going to a different vnet, such as vnet1, thus (bidirectional) communication between them is not possible.

upvoted 5 times

✉️ **TJ001** 5 months ago

YYY seems right

upvoted 1 times

✉️ **MyPractice** 6 months, 1 week ago

This came in Dec 2022

upvoted 1 times

 **geuser** 6 months, 3 weeks ago

I say YYN

No because: Select Block all traffic to the remote virtual network if you don't want traffic to flow to the peered virtual network by default. You can select this setting if you have peering between two virtual networks but occasionally want to disable default traffic flow between the two. You may find enabling/disabling is more convenient than deleting or re-creating peerings.

upvoted 3 times

 **Takloy** 7 months, 2 weeks ago

YYY

For the 3rd question, if you read carefully and look closely to the chart, it means Traffic to remote network from VNET5. Meaning, From VNET5 to any of the remote networks will be blocked but not inbound. This is why the answer is Yes.

upvoted 2 times

 **GokuSS** 8 months ago

YYN, for 3rd questions, does this explanation makes sense? "VM1 can reach VM4 through GW1, but not VM5 as VNET1 does not use remote Gateways."

upvoted 1 times

 **ACSLearning1** 8 months, 1 week ago

How can "VM1 and VM5 can communicate" be yes if "use remote gateway" is set to none on vnet1?

upvoted 1 times

 **TJ001** 5 months ago

that is only for peering not for BGP

upvoted 1 times

 **mingorad** 8 months, 3 weeks ago

correct is YYY ; traffic to remote virtual network is blocked on Vnet5 so from Vnet5 to exterior not from Vnet4 to Vnet5

upvoted 1 times

**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

**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>

✉️  **bakamon** 3 weeks ago

:: Global Reach  
:: Private  
upvoted 1 times

✉️  **Himank20** 1 month, 3 weeks ago

From MS Docs:-

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#what-is-expressroute-global-reach>

If a metro in a supported country/region has more than one ExpressRoute peering location, you can connect together the ExpressRoute circuits created at different peering locations in that metro.

upvoted 1 times

✉️ **sserna** 5 months ago

En examen 20/01/2023

upvoted 2 times

✉️ **Tightbot** 6 months, 2 weeks ago

Global reach

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs#what-is-expressroute-global-reach>

upvoted 2 times

✉️ **Takloy** 7 months, 2 weeks ago

Global reach functions like a "Transit gateway" for on-premise networks, hence, allowing them 2 different on-premise locations to communicate.

upvoted 1 times

✉️ **sikbeats** 8 months, 2 weeks ago

Why is it called "Global Reach" if it is within US regions. I thought Global Reach was for different global regions like if a US provider doesn't have a locations in the other region.

upvoted 2 times

✉️ **TJ001** 5 months ago

East US and West US does not fall in the same geopolitical,,,East US and East US 2 may

upvoted 1 times

✉️ **mauchi** 4 months, 3 weeks ago

that's not right, they are indeed under the same geopolitical region - check here <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations>

upvoted 2 times

✉️ **AppTech** 3 months, 1 week ago

I agree. Geopolitical region is North America. It includes East US, West US, East US 2, West US 2, West US 3, Central US, South Central US, North Central US, West Central US, Canada Central, Canada East

upvoted 1 times

✉️ **BlackZeros** 9 months ago

seems like a right answer

Global Reach

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-global-reach>

Peering

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

upvoted 4 times

✉️ **AdityaGupta** 9 months ago

Global Reach is a feature for connecting your On-Prem Datacenters over Express Route.

And Private Peering allows you to connect On-Prem to Azure Platform Private Networks.

upvoted 1 times

✉️ **DerekKey** 9 months, 3 weeks ago

Configure ExpressRoute Global Reach -> Azure private peering is configured on your ExpressRoute circuits.

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-set-global-reach>

upvoted 1 times

✉️ **WhiteRhino1743** 9 months, 3 weeks ago

Looks correct. To confirm the second question - <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-set-global-reach>.

upvoted 2 times

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.

The screenshot shows the configuration settings for a Site-to-Site VPN connection. The settings are as follows:

- Use Azure Private IP Address:** Enabled
- BGP:** Disabled
- IPsec / IKE policy:** Default
- Use policy based traffic selector:** Enable
- DPD timeout in seconds \***: 45
- Connection Mode:** Default
- 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?

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

**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%

**RageshBethapudi** Highly Voted 9 months, 3 weeks ago

correct answer is D.

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

upvoted 14 times

**mrgreat** Highly Voted 2 months, 3 weeks ago

D. Set IPsec / IKE policy to Custom.

In order to ensure that the on-premises network can connect to the route-based virtual network gateway, you need to set the IPsec / IKE policy

to Custom. The default policy settings for a virtual network gateway are not compatible with policy-based VPN devices. By setting the IPsec / IKE policy to Custom, you can configure the policy to match the requirements of the on-premises VPN devices.

Option A, "Set Connection Mode to ResponderOnly," is not a valid option for a route-based VPN gateway.

Option B, "Set BGP to Enabled," is not necessary to enable connectivity between a route-based gateway and a policy-based VPN device.

Option C, "Set Use Azure Private IP Address to Enabled," is not relevant to this scenario. This setting is used to specify whether the virtual network gateway should use a private or public IP address for the VPN connection.

upvoted 9 times

 **khanda** Most Recent 2 months, 1 week ago

**Selected Answer: D**

Correct answer is D

upvoted 1 times

 **Chezzer83** 2 months, 2 weeks ago

**Selected Answer: D**

I assumed D for this. BGP is not required to configure a VPN connection.

upvoted 1 times

 **where2go** 2 months, 3 weeks ago

Its D --- The configuration option is part of the custom IPsec/IKE connection policy. If you enable the policy-based traffic selector option, you must specify the complete policy (IPsec/IKE encryption and integrity algorithms, key strengths, and SA lifetimes).

The configuration option is part of the custom IPsec/IKE connection policy. If you enable the policy-based traffic selector option, you must specify the complete policy (IPsec/IKE encryption and integrity algorithms, key strengths, and SA lifetimes).

upvoted 1 times

 **bennasu** 3 months, 1 week ago

If you set the IPsec/IKE config to default, under most of the circumstances, azure VPN GW will automatically match the on prem Firewall's IPsec Phase 1 and phase 2 configuration(modern FW like fortigate,sonicwall). But if you are using cisco ASA then it's a different story. You would need to configure the phase manually

upvoted 1 times

 **Bbb78** 4 months, 2 weeks ago

I am not sure any of the 4 answers are correct. Mainly because this is ENABLED - "Use policy based traffic selector " ...if the onPrem device(s) is route based then this is not needed ?

upvoted 1 times

 **sserna** 5 months ago

En examen 20/01/2023

upvoted 2 times

 **mm2** 5 months, 1 week ago

**Selected Answer: D**

route-based also mean static routes and all others routing protocols, when policy based, based on configured networks that should be routed for this specific VPN.

From network perspective route-based use ROUTING TABLE to make route decision, this includes all directly connected networks and mentioned static routes. Making an assumption that BGP=Route-based as a must - is wrong imho

however you can configure route-based to communicate with multiple policy base devices. Please notice POLICY BASE DEVICES for on prem, not DEVICE [one], there are multiple in question.

upvoted 1 times

 **mm2** 5 months, 1 week ago

route-based also mean static routes and all others routing protocols, when policy based, based on configured networks that should be routed for this specific VPN.

From network perspective route-based use ROUTING TABLE to make route decision, this includes all directly connected networks and mentioned static routes. Making an assumption that BGP=Route-based as a must - is wrong imho.

upvoted 1 times

 **zukako** 5 months, 3 weeks ago

Not have to set BGP if onpremise is act/stanby

upvoted 1 times

 **Andre369** 6 months, 2 weeks ago

**Selected Answer: D**

correct answer is D.

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

upvoted 1 times

 **JRodJ** 6 months, 3 weeks ago

I don't think any of these answers is correct. In order to talk to on premises there is another button that must be enabled not visible on this screenshot. Use custom traffic selectors and it needs to be enabled. I have verified this works by configuring it at my customer's location with 3

separate sites.

upvoted 1 times

 **Libaax01** 7 months, 3 weeks ago

The correct answer is D, you can not have Policy based VPN one end and Route Based VPN on the other. Both ends need to match on the type of VPN being used.

upvoted 1 times

 **Prutser2** 8 months, 1 week ago

**Selected Answer: D**

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

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

upvoted 4 times

 **HasanHHH** 8 months, 2 weeks ago

**Selected Answer: D**

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

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

upvoted 2 times

 **jellybiscuit** 8 months, 3 weeks ago

**Selected Answer: B**

Agree with B.

VpnGw1 is a route based-gateway (they also tell you this).

Explained in the link others posted.

upvoted 2 times

**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-AzIpsecPolicy
          New-AzIpsecTrafficSelectorPolicy
          New-AzServiceEndpointPolicy
          New-AzVpnClientIpsecPolicy
          -IpsecEncryption AES256 -IkeEncryption AES256 -IkeIntegrity SHA384 -DhGroup DHGroup24 -IpsecEncryption AES256
          -IpsecIntegrity SHA256 -PfsGroup None -SALifeTimeSeconds 14400 -SADataSizeKilobytes 102400000
          ...
          -Name $Connection16 -ResourceGroupName $RG1 -VirtualNetworkGateway1 $vnet1gw
          New-AzVirtualHub
          New-AzVirtualNetworkGateway
          New-AzVirtualNetworkGatewayConnection
          New-AzVirtualNetworkGatewayNatRule
          -LocalNetworkGateway2 $lNG6 -Location $Location1 -ConnectionType IPsec -IpsecPolicies $policy -SharedKey 'AzureA1b2C3'
          ...
          ]
```

**Answer Area**

```
...
$policy = [New-AzIpsecPolicy
          New-AzIpsecTrafficSelectorPolicy
          New-AzServiceEndpointPolicy
          New-AzVpnClientIpsecPolicy
          -IpsecEncryption AES256 -IkeEncryption AES256 -IkeIntegrity SHA384 -DhGroup DHGroup24 -IpsecEncryption AES256
          -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'
          ...
          ]
```

**Correct Answer:**

**Goofer** (Highly Voted) 5 months, 1 week ago

1 = New-AzIpsecPolicy

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

2 = New-AzVirtualNetworkGatewayConnection

<https://learn.microsoft.com/en-us/powershell/module/az.network/new-azvirtualnetworkgatewayconnection?view=azps-9.2.0#example-1>  
upvoted 8 times

**Aunehwet79** 5 months, 1 week ago

Thanks - agreed

upvoted 1 times

**Rajan395** (Most Recent) 4 months, 3 weeks ago

answer looks correct

upvoted 3 times

**liono** 5 months ago

Given Answer is correct

upvoted 1 times

**TJ001** 5 months ago

Given answers looks good

upvoted 1 times

 **Goofer** 5 months, 1 week ago

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

## 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 = Get-AzLocalNetworkGateway -Name "HQ" -ResourceGroupName "ForcedTunneling"
Get-AzNatGateway
Get-AzNetworkVirtualAppliance
Get-AzVirtualNetworkGateway

$force2 = Get-AzVirtualNetworkGateway -Name "Gateway1" -ResourceGroupName "ForcedTunneling"
Set-AzVirtualNetworkGatewayConnection
Set-AzVirtualNetworkGatewayDefaultSite
Set-AzVirtualNetworkPeering
Set-AzVirtualNetworkSubnetConfig
```

**Answer Area**

```
$force1 = Get-AzLocalNetworkGateway -Name "HQ" -ResourceGroupName "ForcedTunneling"
Get-AzNatGateway
Get-AzNetworkVirtualAppliance
Get-AzVirtualNetworkGateway

$force2 = Get-AzVirtualNetworkGateway -Name "Gateway1" -ResourceGroupName "ForcedTunneling"
Set-AzVirtualNetworkGatewayConnection
Set-AzVirtualNetworkGatewayDefaultSite
Set-AzVirtualNetworkPeering
Set-AzVirtualNetworkSubnetConfig
```

**Correct Answer:**

**DavidSapery** Highly Voted 5 months, 1 week ago

Answer is correct. It's the exact example in <https://learn.microsoft.com/en-us/powershell/module/az.network/set-azvirtualnetworkgatewaydefaultsite?view=azps-9.2.0>

upvoted 9 times

**dani999** Most Recent 4 months, 3 weeks ago

Correct answer :

```
$LocalGateway = Get-AzLocalNetworkGateway -Name "ContosoLocalGateway" -ResourceGroupName "ContosoResourceGroup"
$VirtualGateway = Get-AzVirtualNetworkGateway -Name "ContosoVirtualGateway"
Set-AzVirtualNetworkGatewayDefaultSite -GatewayDefaultSite $LocalGateway -VirtualNetworkGateway $VirtualGateway
```

upvoted 3 times

**liono** 5 months ago

Correct. Local Network gateway for sending all internet traffic via on-prem DC

upvoted 2 times

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
- C. service endpoints
- D. route tables

**Correct Answer: B**

*Community vote distribution*

B (100%)

 **Rick0304** 1 month ago

Peering is the correct answer!  
upvoted 2 times

 **ESAJRR** 2 months, 4 weeks ago

**Selected Answer: B**  
Peering is correct!  
upvoted 1 times

 **mVic** 4 months, 2 weeks ago

**Selected Answer: B**  
Peering is correct.  
upvoted 4 times

 **Rajan395** 4 months, 3 weeks ago

Correct. VNET peering is the answer.  
upvoted 3 times

 **lono** 5 months ago

VNET Peering!  
upvoted 1 times

 **krishnadasns96** 5 months ago

**Selected Answer: B**  
Correct, Peering  
upvoted 3 times

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?

- one ExpressRoute Premium circuit
- two ExpressRoute Premium circuits
- four ExpressRoute Standard circuits
- one ExpressRoute Standard circuit

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **sumandev** Highly Voted 5 months, 1 week ago

Express Route Premium SKU provides ability to connect from on-premises to any of the Azure regions across the globe.  
upvoted 6 times

 **Pratheeshp** Most Recent 1 month, 1 week ago

4 x Local SKU ER is cheaper than 1 x Premium SKU ER. However since it is not an option, i would go with Answer A  
upvoted 1 times

 **xamkiller** 1 month, 3 weeks ago

Answer is A  
If there was 2x standard ExpressRoute circuits available, that would be the most cost-effective answer.  
upvoted 1 times

 **Rafael1984** 2 months, 2 weeks ago

I think is D because you must be minimized cost  
upvoted 1 times

 **ryswick7** 2 months, 2 weeks ago

ER Standard SKU doesn't allow you to connect across a geopolitical area. Hence, it is A  
ref: <https://eighty20solutions.com.au/azure-expressroute/>  
upvoted 3 times

 **jarz** 1 month, 4 weeks ago

This is a much better explanation compared to MS garble!  
upvoted 1 times

 **ESAJRR** 2 months, 4 weeks ago

**Selected Answer: A**

An ExpressRoute Premium circuit is a higher-end offering for Azure ExpressRoute that provides increased resiliency and higher bandwidth capabilities compared to the standard ExpressRoute circuits.

upvoted 2 times

 **blah1234\_5** 3 months, 4 weeks ago

Express route premium allows 4 circuits - <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-faqs>

upvoted 1 times

 **SeanPan** 4 months, 1 week ago

A is correct

upvoted 2 times

 **dani999** 4 months, 2 weeks ago

**Selected Answer: A**

A is correct

upvoted 4 times

 **liono** 5 months ago

One ExpressRoute circuit is required for the office with premium SKU

upvoted 1 times

 **DeepMoon** 5 months, 1 week ago

If you need to connect to multiple geo's then you need express route premium sku. If it is only a single region, then you can use a standard sku.

upvoted 3 times

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?

- VpnGw1AZ
- VpnGw2AZ
- VpnGw4AZ
- VpnGw5AZ

**Correct Answer: C**

*Community vote distribution*

C (100%)

✉ **DavidSapery** Highly Voted 5 months, 1 week ago

Basic SKU supports max 10 S2S connections. SKUs 1, 2, and 3 support max 30 S2S connections. SKUs 4 & 5 support max 100 S2S. Of those 2, SKU4 minimizes the cost.

Answer C

upvoted 26 times

✉ **DeepMoon** 5 months, 1 week ago

Ditto.

upvoted 1 times

✉ **Rick0304** Most Recent 1 month ago

Generation2 VpnGw4AZ Max. 100\* Max. 128 Max. 5000 5 Gbps Supported

upvoted 1 times

✉ **ESAJRR** 2 months, 4 weeks ago

**Selected Answer: C**

VPN GTW SKU S2S V2V PS2 P2S THROUGHPUT BGP

Generation2 VpnGw2AZ Max. 30 Max. 128 Max. 500 1.25 Gbps Supported

Generation2 VpnGw3AZ Max. 30 Max. 128 Max. 1000 2.5 Gbps Supported Yes

Generation2 VpnGw4AZ Max. 100\* Max. 128 Max. 5000 5 Gbps Supported

Generation2 VpnGw5AZ Max. 100\* Max. 128 Max. 10000 10 Gbps Supported

upvoted 3 times

✉ **wooyourdaddy** 3 months, 1 week ago

**Selected Answer: C**

Answer can be derived from the table at:

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

In the columns marked "S2S/Vnet-to-Vnet Tunnels" and "Zone-Redundant".

All SKUs that end in AZ are zone-redundant, which covers the datacenter failure scenario, so all 4 answers are still valid at this point.

From the chart, we see the following max connections:

- VpnGw1AZ - Max 30 connections
- VpnGw2AZ - Max 30 connections
- VpnGw4AZ - Max 100 connections
- VpnGw5AZ - Max 100 connections

So while VpnGw4AZ and VpnGw5AZ can both handle the 90 connections, the final deciding criteria is cost. So C, VpnGw4AZ would be the correct answer.

upvoted 2 times

✉ **dani999** 4 months, 2 weeks ago

**Selected Answer: C**

VpnGw4AZ Max. 100 s2s  
Zone-redundant is support  
upvoted 4 times

 **sserna** 5 months ago  
En examen 20/01/2023  
upvoted 2 times

 **liono** 5 months ago  
Correct! SKU4  
upvoted 2 times

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.

**Correct Answer: D**

*Community vote distribution*

D (100%)

 **DeepMoon** Highly Voted 5 months, 1 week ago

Basic sku won't support cross-region traffic.  
<https://learn.microsoft.com/en-us/azure/load-balancer/skus>  
<https://learn.microsoft.com/en-us/azure/load-balancer/cross-region-overview>  
 upvoted 7 times

 **khanda** Most Recent 2 months, 1 week ago

**Selected Answer: D**  
 Azure Standard Load Balancer supports cross-region load balancing.  
 upvoted 1 times

 **ESAJRR** 2 months, 4 weeks ago

**Selected Answer: D**  
 SCENARIO Standard Load Balancer Basic Load Balancer  
 Global VNet Peering Support Standard ILB is supported via Global VNet Peering Not supported  
 upvoted 1 times

 **liona** 5 months ago

Correct. Change SKU to Standard.  
 upvoted 2 times

 **Stevy\_nash** 5 months ago

**Selected Answer: D**  
 we should also change the SKU of VMs' IP addresses to standard or remove them  
 upvoted 2 times

The question didn't mention that the VMs have public IP addresses.

upvoted 1 times

 **TT924** 5 months, 1 week ago

**Selected Answer: D**

Standard ILB is supported via Global VNet Peering

Standard ILB is supported via Global VNet Peering  
upvoted 2 times

 **TT924** 5 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/load-balancer/skus#skus>  
upvoted 1 times

## 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



## Correct Answer:

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

**aklas** Highly Voted 1 month ago

Given answer and all the discussions are incorrect.

1. Create an SSL profile
2. Upload a certificate
3. Add an HTTP listener and associate the listener to the profile
4. Create a routing rule

The question says you already deploy an App Gateway and configure a listener and a routing rule. You can't deploy a listener without a frontend IP so that assumes you already have one.

Listener needs a routing rule otherwise it's useless.

upvoted 6 times

**kienvu** Highly Voted 4 months ago

1. From AppGwy1, create a frontend IP configuration
2. From AppGwy1, create a routing rule
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

upvoted 5 times

**omgMerrick** 4 months ago

This is incorrect! There is no need to create a routing rule.

The given answer is correct.

<https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal>  
upvoted 7 times

✉️  **xamkiller** Most Recent 1 month, 3 weeks ago

The given answer is correct!

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

upvoted 3 times

✉️  **khanda** 2 months, 1 week ago

Answer is correct: <https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-portal>

upvoted 1 times

✉️  **rj\_289** 2 months, 3 weeks ago

Given answer is correct!

upvoted 2 times

✉️  **Aziza\_Adam** 4 months ago

The given answer is correct

upvoted 2 times

✉️  **TedSund69543** 4 months, 1 week ago

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

upvoted 5 times

✉️  **tryhard97** 4 months, 1 week ago

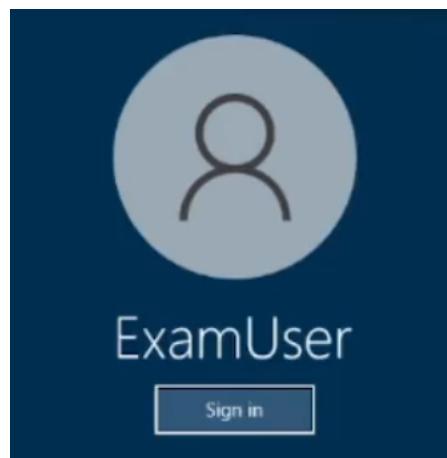
help answer plz

upvoted 1 times

✉️  **harshit101** 4 months, 2 weeks ago

what is going on here?

upvoted 3 times

**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: xxxxxxxxxxxx

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.

#### 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, 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.

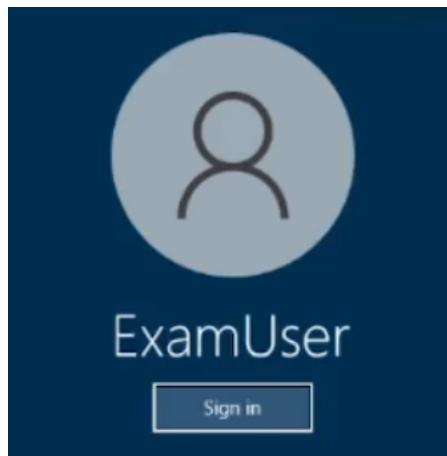
Step 5: Select Create to create the local network gateway object.

#### Reference:

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

✉️  MrBlueSky 2 months, 3 weeks ago

Given answer is correct, you would need to create a Local Network Gateway, which will represent the on-prem IP address  
upvoted 1 times

**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: xxxxxxxxxxx

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.

#### 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:

The screenshot shows the 'myVirtualNetwork1 | Peerings' page in the Azure portal. On the left, there's a sidebar with various settings like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and a 'Peering' section which is currently selected and highlighted with a red box. At the top right, there's a search bar, a '+ Add' button (which is also highlighted with a red box), and a 'Refresh' button. Below the search bar, there's a 'Filter by name...' input field and a table header with columns: Name ↑↓, Peering status ↑↓, Peer ↑↓, and Gateway transit ↑↓. A single row in the table is visible, showing '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:

The screenshot shows the 'myVirtualNetwork1 | Peerings' page again. The sidebar and top navigation are identical to the previous screenshot. The table now contains one row: 'myVirtualNetwork1-myVirtualNetwork2' in the 'Name' column, 'Connected' in the 'Peering status' column (which is highlighted with a red box), 'myVirtualNetwork2' in the 'Peer' column, and 'Disabled' in the 'Gateway transit' column.

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>

✉️ **thor04** 4 days, 13 hours ago

Do we need to create the connection for VPN site-to-site ?  
upvoted 1 times

**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
<input type="checkbox"/> http	80
<input type="checkbox"/> https	443
<input type="checkbox"/> snmp	8081

**Answer Area**

**Correct Answer:**

://20.25.32.214:	/healthprobe
<input type="checkbox"/> http	80
<input checked="" type="checkbox"/> https	443
<input type="checkbox"/> snmp	8081

 **ckyap** Highly Voted 2 months, 2 weeks ago

Correct. See <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>

upvoted 6 times

 **xamkiller** Most Recent 1 month, 3 weeks ago

It was on 24/04/2023. The answer is correct.

Active/Passive: `https://<YourVirtualNetworkGatewayIP>:8081/healthprobe`

Actve/Active: `https://<YourVirtualNetworkGatewayIP2>:8083/healthprobe` (Second IP)

<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>

upvoted 2 times

**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

**Answer Area**

Minimum number of ExpressRoute circuits:

One ExpressRoute Standard circuit
One ExpressRoute Premium circuit
Two ExpressRoute Standard circuits
Two ExpressRoute Premium circuits
<b>Three ExpressRoute Standard circuits</b>
Three ExpressRoute Premium circuits

**Correct Answer:**

Minimum number of ExpressRoute gateways:

One ExpressRoute gateway of the ErGw1AZ SKU
One ExpressRoute gateway of the High performance SKU
<b>Two ExpressRoute gateway of the ErGw1AZ SKU</b>
Two ExpressRoute gateway of the High performance SKU
Three ExpressRoute gateway of the ErGw1AZ SKU
Three ExpressRoute gateway of the High performance SKU

 **bakamon** 3 weeks ago

Answer :

- > One ExpressRoute Standard circuit
  - > One ExpressRoute gateway of the ErGw1AZ SKU
- upvoted 3 times

 **aklas** 1 month ago

For number of GW's, correct answer should be 1 ErGw1AZ:

"For a VPN gateway, the two gateway instances will be deployed in any 2 out of these three zones to provide zone-redundancy. For an ExpressRoute gateway, since there can be more than two instances, the gateway can span across all the three zones."

<https://learn.microsoft.com/en-us/azure/vpn-gateway/about-zone-redundant-vnet-gateways#pipzrg>

upvoted 2 times

✉️ **xamkiller** 1 month, 3 weeks ago

1. Maintain connectivity to the virtual machines if two availability zones fail - Needs two VPN gateways to tolerate two AV zones.

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

2. Support 1000-Mbps connections - Standard/ERGw1Az supports up to 1Gbps and support across geopolitical areas, which is more than enough.

<https://learn.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways#testing-conditions>

Therefore, the most cost-effective solution is;

One ExpressRoute Standard circuit

2x ExpressRoute gateways (ErGw1AZ)

upvoted 4 times

✉️ **headspace** 1 month, 1 week ago

It never mentioned a VPN connection, so I'm thinking 1 ER Standard, SKU 1 ErGw1AZ

upvoted 2 times

✉️ **henryhung** 2 months, 1 week ago

Update: Answer from ChatGPT Plus(GPT 4.0)

To meet the requirements, you need to have the following:

Minimum number of ExpressRoute circuits:

Two ExpressRoute Standard circuits

This is because ExpressRoute Standard circuits do not provide connectivity across multiple regions, and you need to maintain connectivity if two availability zones fail. Therefore, you will need two ExpressRoute Standard circuits to ensure connectivity in case of failure.

Minimum number of ExpressRoute gateways:

Two ExpressRoute gateways of the ErGw1AZ SKU

The ErGw1AZ SKU supports up to 2,000 Mbps, which meets the 1,000 Mbps requirement, and it also provides Zone Redundant Gateway for increased reliability. Having two ExpressRoute gateways of the ErGw1AZ SKU ensures that connectivity is maintained even if two availability zones fail, meeting the requirement.

upvoted 1 times

✉️ **oakl** 2 months, 1 week ago

I don't think ChatGPT is correct here.

First of all, connectivity across multiple regions doesn't matter in terms of availability zones because they are usually located in the same region. This would only matter for services with cross-regional replication such as storage accounts. Not entirely sure if two circuits are necessary - I think one would be enough.

For ExpressRoute gateways you should only need one because it spans across three availability zones if you configure the public IP with standard SKU and zone redundancy. Regular VPN Gateways only span two availability zones. In that case you would probably need two Gateways.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/about-zone-redundant-vnet-gateways#pipzrg>

upvoted 2 times

✉️ **henryhung** 2 months, 1 week ago

Answer from ChatGPT:

To maintain connectivity to the virtual machines if two availability zones fail, at least two ExpressRoute circuits are required for redundancy, one of which must be in a different availability zone.

For supporting a 1000-Mbps connection, ExpressRoute Premium is required. Therefore, the minimum number of circuits needed is two ExpressRoute Premium circuits.

Regarding the minimum number of ExpressRoute gateways, at least one ExpressRoute gateway is required for each circuit. Therefore, two ExpressRoute gateways are required, one in each availability zone.

Since the solution must minimize costs, the recommended SKU for the ExpressRoute gateway is the ErGw1AZ SKU, which is less expensive than the High performance SKU.

Therefore, the answers are:

Minimum number of ExpressRoute circuits: Two ExpressRoute Premium circuits

Minimum number of ExpressRoute gateways: Two ExpressRoute gateways of the ErGw1AZ SKU

upvoted 1 times

✉️ **henryhung** 2 months, 1 week ago

Please ignore this ChatGPT 3.5 answer.

upvoted 2 times

✉️ **\_fvt** 2 months, 2 weeks ago

Express Route Zone redundant gateways can span to three AZ.

I am not sure there, but I think the active ER GW only use the circuit so even if it would have been better to have one primary and one secondary

circuit, you may have one ExpressRoute Standard circuit only, with 3 instances of Zone Redundant ER GW.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/about-zone-redundant-vnet-gateways>

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

#### Zone-redundant gateways

When you create a public IP address using the Standard public IP SKU without specifying a zone, the behavior differs depending on whether the gateway is a VPN gateway, or an ExpressRoute gateway.

For a VPN gateway, the two gateway instances will be deployed in any 2 out of these three zones to provide zone-redundancy.

For an ExpressRoute gateway, since there can be more than two instances, the gateway can span across all the three zones.

upvoted 1 times

 **\_fvt** 2 months, 2 weeks ago

I tested in lab, deployed an ErGw1AZ in a Region (France Central) with 3Az an I well have 3 Instances of the Public IP and ER Gateway.

So the Answer is:

- one ErGw1AZ
- one Circuit.

upvoted 12 times

 **jarz** 1 month, 4 weeks ago

Standard or Premium ER CCT?

upvoted 2 times

 **JohnnyChimp0** 1 month, 3 weeks ago

Standard. Premium is viable when it spans over several regions and that is not the case here

upvoted 2 times

 **khanda** 2 months, 1 week ago

This correct.

upvoted 1 times

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

**Correct Answer:** D

*Community vote distribution*

D (100%)

 **Ben\_88** 1 week, 2 days ago

why not a nat gateway ?

upvoted 1 times

 **Ben\_88** 1 week, 2 days ago

bad idea , just realized that nat gateway can only handle outbound traffic . so it can only be D

upvoted 3 times

 **Oklama** 4 weeks ago

**Selected Answer: D**

Given answer is correct

upvoted 2 times

 **jameess** 1 month ago

Why not Azure Application Gateway with different listeners?

upvoted 1 times

 **ubdubdoo** 1 month, 1 week ago

an Azure NAT Gateway is a dedicated network appliance that provides outbound NAT functionality for virtual networks in Azure. It allows resources within a virtual network to access the internet or other resources outside of the virtual network using a single or a pool of public IP addresses.

upvoted 1 times

 **crypto700** 1 month, 1 week ago

**Selected Answer: D**

Given answer is correct

upvoted 3 times

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**

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

Reference:

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

*Community vote distribution*

B (100%)

 **AmalMOQ** Highly Voted 1 year, 8 months ago

correct !If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 11 times

 **liono** 5 months ago

Agree!

upvoted 1 times

 **FunkyB** 9 months, 4 weeks ago

Correct

About Point-to-Site VPN routing

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

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

upvoted 2 times

 **khanda** Most Recent 2 months, 1 week ago

Selected Answer: B

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

upvoted 1 times

 **sunsetblvdfightclub** 3 months, 2 weeks ago

This question should be more clear that you made changes AFTER you have clients connecting via P2S. This one stumped on the test due to wording, thinking they were still explaining the scenario, not making changes from one sentence to the next

upvoted 1 times

 **Rajan395** 4 months, 3 weeks ago

correct

upvoted 1 times

 **HasanHHH** 8 months, 2 weeks ago

Selected Answer: B

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 1 times

 **AdityaGupta** 9 months, 1 week ago

**Selected Answer: B**

Since you implemented VNET peering later, you need to download and install VPN client to get topology changes.

upvoted 1 times

 **hogs** 10 months ago

Appeared on exam Aug2022

upvoted 1 times

 **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

 **Edward1** 1 year, 2 months ago

**Selected Answer: B**

correct

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 1 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

 **Ben\_Dover2** 1 year, 4 months ago

**Selected Answer: B**

download VPN config and reconnect

upvoted 3 times

 **AckeyGraham** 1 year, 4 months ago

Would help if there was more context to such a question, presuming like an exam than was probably told prior to this question, as it isn't made clear when the client was downloaded onto the windows 10 machine.

upvoted 3 times

 **Takloy** 1 year, 5 months ago

Download the p2s configuration file and reconnect is the solution.

So correct answer here is, NO.

upvoted 2 times

 **AidenYoukhana** 1 year, 5 months ago

**Selected Answer: B**

Correct: NO.

upvoted 2 times

 **Pamban** 1 year, 6 months ago

appeared on exam 5th Dec 2021

upvoted 1 times

 **RandomUser** 1 year, 8 months ago

Correct

upvoted 1 times

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

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

You have two Azure virtual networks named Vnet1 and Vnet2.

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

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

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You enable BGP on the gateway of Vnet1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

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

Reference:

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

*Community vote distribution*

B (100%)

✉  **Takloy**  1 year, 5 months ago

**Selected Answer: B**

Solution: Download the P2S configuration package, install it on the client device and reconnect.

Answer: NO

upvoted 11 times

✉  **Rajan395**  4 months, 3 weeks ago

Correct Answer! re-downloading of the client is required as topology changed

upvoted 1 times

✉  **HasanHHH** 8 months, 2 weeks ago

**Selected Answer: B**

If you make a change to the topology of your network and have Windows VPN clients, the VPN client package for Windows clients must be downloaded and installed again in order for the changes to be applied to the client.

upvoted 1 times

✉  **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 2 times

✉  **Edward1** 1 year, 2 months ago

**Selected Answer: B**

Correct!

upvoted 1 times

✉  **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 2 times

✉  **aftab7500** 1 year, 6 months ago

BGP is an optional feature you can use with Azure Route-Based VPN gateways.

upvoted 4 times

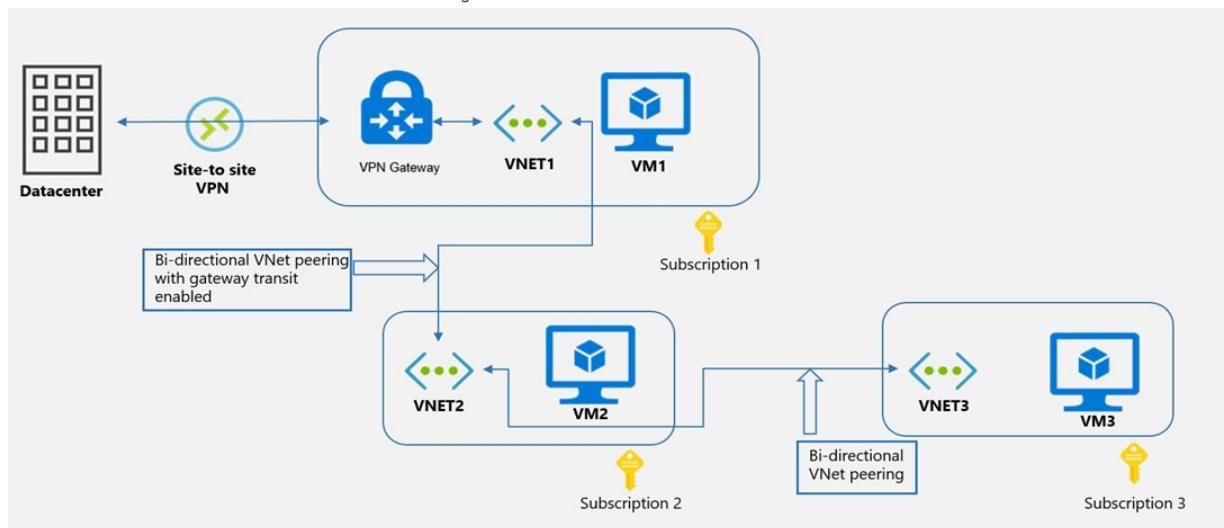
✉  **Charl** 1 year, 7 months ago

Correct!

upvoted 2 times

**HOTSPOT -**

You have the Azure environment shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

VM1 can communicate with (answer choice):

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

VM2 can communicate with (answer choice):

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

**Correct Answer:**

**Answer Area**

VM1 can communicate with (answer choice):

VM2 only
VM2 and VM3 only
<b>the on-premises datacenter and VM2 only</b>
the on-premises datacenter, VM2, and VM3 only

VM2 can communicate with (answer choice):

VM1 only
VM1 and VM3 only
the on-premises datacenter and VM3 only
<b>the on-premises datacenter, VM1, and VM3 only</b>

Reference:

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

✉ **RickMorais** Highly Voted 1 year, 8 months ago

Given answers are correct

upvoted 30 times

✉ **Vivek\_Dwivedi** Highly Voted 1 year, 7 months ago

Use Remote gateway in VNET 2 peering is not mentioned. Which means VM2 can connect only to Vm1 and Vm3.

upvoted 15 times

✉ **sallymaher** 1 year, 5 months ago

That is mentioned in Enable transit gateway :- Virtual network gateway: Use this virtual network's gateway ( in the vnet that contains the GW ) and ( Virtual network gateway: Use the remote virtual network's gateway) in the remote one so the answer is correct .

upvoted 10 times

✉ **kpallivishal** 1 year, 5 months ago

enable transit gateway means selecting both in vnet peering ( Use this virtual network's gateway + Use the remote virtual network's gateway ) . so above answer is correct as mentioned in diagram

upvoted 8 times

✉ **khanda** Most Recent 2 months, 1 week ago

Given answer is correct.

upvoted 1 times

✉ **liono** 5 months ago

Correct.

upvoted 2 times

✉ **Goofer** 5 months, 3 weeks ago

VNET1 and VNET2 do not have a router configured to route traffic to another VNET

VNET2 and VNET3 do not have UDR configured to route traffic to the router.

VN1 --> on-premises and VM2

VM2 --> VM1 and VM3

upvoted 1 times

✉ **Bill831231** 7 months, 3 weeks ago

what if for the S2S VPN without BGP enabled? VM2 can still communicate with On-premise?

upvoted 1 times

✉ **HasanHHH** 8 months, 2 weeks ago

Correct:

1. VM1 Can Communicate with On-Premise datacenter due to S2S VPN and VM2 due to Bi-Directional VNet Peering

2. VM2 can Communicate with On-Premise datacenter, VM1 due Gateway transit(VNET1-VNET2) & S2S VPN (VNET1-Datacenter), and VM3 (VNET2-VNET3 VNet Peering)

upvoted 6 times

✉ **sapien45** 8 months, 2 weeks ago

Responses provided are correct. 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.

It means that both options are selected in the vnettovnnet peering :

Use the remote virtual network's gateway  
Use this virtual network's gateway

Therefore VM2 can communicate with on premises  
upvoted 1 times

✉ **AdityaGupta** 9 months, 1 week ago

Correct Answer  
upvoted 1 times

✉ **1particle** 10 months, 3 weeks ago

Correct.  
VM2 uses VM1's gateway to reach the Datacenter.  
upvoted 1 times

✉ **unclegrandfather** 11 months, 3 weeks ago

A slightly modified version of this was on the exam on 6/28/22. Make sure you understand WHY the answers are correct.  
upvoted 2 times

✉ **WickedMJ** 10 months ago

Can you advise whether it varies due to the placement of the "VPN Gateway" on the graph? TIA  
upvoted 1 times

✉ **wsrudmen** 1 year, 1 month ago

Correct

VM1 can't access VM3 because (an UDR should be needed to achieve this): <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>  
upvoted 2 times

✉ **Edward1** 1 year, 2 months ago

Correct:  
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.  
upvoted 2 times

✉ **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.  
upvoted 2 times

✉ **[Removed]** 1 year, 4 months ago

Answer is correct. If you wanted VM1 to connect to VM3 you'd set up a virtual appliance and configure some routing rules  
upvoted 5 times

✉ **Joshalom** 1 year, 4 months ago

on exam 6/2/2022  
upvoted 1 times

✉ **Joshalom** 1 year, 4 months ago

on exam 28/1/22  
upvoted 1 times

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**

Reference:

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

*Community vote distribution*

ADE (91%) 9%

 **srikanth1987** Highly Voted 1 year, 8 months ago

yes..ADE is the correct answer.

upvoted 25 times

 **d0bermannn** Highly Voted 1 year, 4 months ago

Selected Answer: ADE  
all GW types and Bastion must have dedicated subnets

upvoted 9 times

 **ESAJRR** Most Recent 2 months, 4 weeks ago

A. Azure Bastion = Name unique - AzureBastionSubnet  
D. Azure Application Gateway v2 = Name does not have to be unique, just the subnet  
E. VPN gateway = Name unique - GatewaySubnet

upvoted 2 times

 **somenick** 3 months, 2 weeks ago

Selected Answer: ADE

Correct

upvoted 1 times

 **liono** 5 months ago

Given answers are correct.

upvoted 1 times

 **nstromer89** 6 months, 1 week ago

FYI The answers are correct but AADS also needs a separate subnet it won't allow stuff to be deployed in this specific subnet.  
upvoted 3 times

 **Webfacat33** 6 months, 1 week ago

Selected Answer: ADE

It's correct

upvoted 1 times

 **HasanHHH** 8 months, 2 weeks ago

Selected Answer: ADE

Network Application Gateway- WAF-Dedicated Subnet-YES

VPN Gateway-Dedicated Subnet-YES

Azure Firewall-Dedicated Subnet-YES

Azure Bastion-Dedicated Subnet-YES

Network Virtual Appliances-Dedicated Subnet-NO

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network>

upvoted 2 times

 **kevino81** 8 months, 3 weeks ago

**Selected Answer: ADE**

correct

upvoted 1 times

 **Alessandro365** 9 months ago

**Selected Answer: ADE**

ADE are correct

upvoted 1 times

 **AdityaGupta** 9 months, 1 week ago

**Selected Answer: ADE**

Aure Bastion, Azure Application Gateway, VNET Gateway and Azure Firewall need dedicated subnet

upvoted 3 times

 **Jitusrit** 10 months, 2 weeks ago

**Selected Answer: ADE**

ADE are correct.

upvoted 2 times

 **1particle** 10 months, 3 weeks ago

A,D, & E

<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#gwsu>

upvoted 4 times

 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam 6/28/22

upvoted 3 times

 **aldanetcloud** 1 year ago

**Selected Answer: ADE**

ade correct answer

upvoted 3 times

 **lasmas** 1 year ago

**Selected Answer: ADE**

ADE seems correct

upvoted 3 times

 **jpfsm** 1 year, 1 month ago

**Selected Answer: ADE**

Correct

upvoted 3 times

HOTSPOT -

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

Name	IP address
Vnet1	10.1.0.0/16
Vnet2	10.2.0.0/16

The links have auto registration enabled.

You create the virtual machines shown in the following table.

Name	IP address
VM1	10.1.10.10
VM2	10.2.10.10
VM3	10.2.10.11

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

⇒ Name: VM1

IP address: 10.1.10.9 -

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	<input type="radio"/>	<input type="radio"/>
Deleting VM1 will delete all VM1 records automatically	<input type="radio"/>	<input type="radio"/>
Changing the IP address of VM3 will update the DNS record of VM3 automatically	<input type="radio"/>	<input type="radio"/>

Correct Answer:

### Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	<input type="radio"/>	<input checked="" type="radio"/>
Deleting VM1 will delete all VM1 records automatically	<input type="radio"/>	<input checked="" type="radio"/>
Changing the IP address of VM3 will update the DNS record of VM3 automatically	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

The manual DNS record will overwrite the auto-registered DNS record so VM1 will resolve to 10.1.10.9.

Box 2: No -

The DNS record for VM1 is now a manually created record rather than an auto-registered record. Only auto-registered DNS records are deleted when a VM is deleted.

Box 3: No -

This answer depends on how the IP address is changed. To change the IP address of a VM manually, you would need to select 'Static' as the IP address assignment. In this case, the DNS record will not be updated because only DHCP assigned IP addresses are auto-registered.

Reference:

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

👤 **walkwolf3** Highly Voted 1 year, 7 months ago

Answer is correct, N,N,N, lab tested.

For box3, when IP of VM3 is changed, VM3 will reboot, DNS record will disappear. Then VM3 is back, and registers to the new IP in the DNS zone.

upvoted 32 times

👤 **wooyourdaddy** 3 months, 1 week ago

Agree that answer should be N,N,N as this link:

<https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration#restrictions>

States:

DNS records are created automatically only if the primary virtual machine NIC is using DHCP. If you're using static IPs, such as a configuration with multiple IP addresses in Azure, auto registration doesn't create records for that virtual machine.

Assuming that "changing of the IP address of VM3" means that the NIC is configured with a static IP.

upvoted 2 times

👤 **Apptech** 2 months, 2 weeks ago

You say for question 3 answer should be YES! Private DNS zone will remove and re-add the new static IP address. But question asks for UPDATE the entry. Remove and Re-add after is not an Update, right?

upvoted 1 times

👤 **yokoka2259** 1 year, 7 months ago

if it comes back and registers, then the answer is YES right?

upvoted 4 times

👤 **JamRackie** 1 year, 7 months ago

So are you saying answer 3 should be Yes as it registers itself after a reboot?

upvoted 5 times

👤 **Acrophat** 1 year, 6 months ago

I also labbed this out for question 3 and it should be YES! Private DNS zone will remove and re-add the new static IP address.

upvoted 13 times

👤 **rakesh333** Highly Voted 1 year, 5 months ago

NNN

1. VM2 can't resolve v1.contoso.com to 10.1.10.10 because, there is a manual dns entry for vm1 points to 10.1.10.9 which over writes the automatic entry. So the answer is "NO"
2. Deleting a VM will delete only the automatic dns entry. Since we have a manual entry for vm1, that wouldn't be deleted when deleting the vm1. So the answer is "NO"
3. Manually changing the IP address of VM will not update the dns record. Auto DNS will only work if the VM gets ip via DHCP. So the answer is "NO":

upvoted 30 times

👤 **ESAJRR** Most Recent 2 months, 4 weeks ago

Answer is correct, N,N,N, lab tested too.

upvoted 1 times

👤 **AzureLearner01** 3 months, 2 weeks ago

Lab tested - NNY

You can't add 2 entries with the same name in the zone. So this record would be set to auto registered NO. Due to this it would not be deleted by deleting the vm. The according DNS record would be deleted, yes but only if auto registered is yes.

upvoted 3 times

👤 **Madball** 4 months, 3 weeks ago

By testing in my lab I get No, No and Yes. When you change the IP address of the VM, the VM will automatically reboot, in private DNS the A record disappears and reappears with the new IP address.

upvoted 5 times

👤 **Rajan395** 4 months, 3 weeks ago

Answer is No, NO and YES

upvoted 3 times

👤 **zukako** 5 months, 3 weeks ago

I think q3 is Yes because for VM, azure manage the DNS record automatically

upvoted 3 times

👤 **Kevmeister** 7 months ago

I would definitely answer N,N,Y As per the MS site: <https://learn.microsoft.com/en-us/azure/dns/private-dns-overview>

It clearly states: To resolve the records of a private DNS zone from your virtual network, you must link the virtual network with the zone. Linked virtual networks have full access and can resolve all DNS records published in the private zone. You can also enable autoregistration on a virtual network link. When you enable autoregistration on a virtual network link, the DNS records for the virtual machines in that virtual network are

registered in the private zone. When autoregistration gets enabled, Azure DNS will update the zone record whenever a virtual machine gets created, changes its' IP address, or gets deleted.

The only way to change the IP address is to set it to static within the portal as changing it on the VM itself is a BIG no no. So as per the documentation this proves that the answer is Y for Box 3.

upvoted 6 times

✉ **Kevmeister** 7 months ago

A few people also tested this in their LAB. The scenario provided in the FAQ page shown in the answer page I'm confident is an example of when a person sets a static IP at the OS level rather than from within the portal ipconfig. As tkcito mentioned, if you update in the portal and set an IP it should also then update the DNS record.

upvoted 2 times

✉ **HasanHHH** 8 months, 2 weeks ago

- 1.NO-overwrite the automatically registered DNS records with a manually created DNS record in the zone
- 2.NO-due VM1 record Created manually here -The private zone's records are populated by the Azure DHCP service, if deallocated, the autoregistered DNS records are removed.
- 3.NO-Manually changing the IP address of VM will not update the dns record. The private zone's records are populated by the Azure DHCP service.

upvoted 1 times

✉ **asbaleha** 8 months, 2 weeks ago

3 is yes if you change the IP address of the VM the machine will automatically restart , and the DNS will grab the new IP

upvoted 1 times

✉ **asbaleha** 8 months, 2 weeks ago

hi so i the correct answer is N N Y

- 1- N : in the manual configuration you will remove the auto-registration because u are overriding the DNS record
  - 2- N : VM1 has manual configuration so the entry in the record will be static unless the whole DNS private zone is removed
  - 3- Y : i changed the VM ip address from dynamic to static in the VNIC section , after the VM restarted , when the VM boot up the DNS record update the IP address to the new one
- you can do the lab is easy just create resource group , 1 vnet , 2 subnet and 3 VM

upvoted 3 times

✉ **jellybiscuit** 8 months, 3 weeks ago

N, N, Y

The description supporting #3 is wrong, as are some of the discussions.

You don't updated IPs inside of a VM. You can, but it's the incorrect method. MS wouldn't asked you a question based on incorrect operations. If you change an IP correctly, meaning on the network interface, it will update in private DNS with auto registration enabled. It doesn't matter if you're changing it from dynamic to static, or changing the IP address from one static address to another.

upvoted 7 times

✉ **sapien45** 9 months ago

NNN

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

I've reconfigured the OS in my virtual machine to have a new host name or static IP address. Why don't I see that change reflected in the private zone?

The private zone's records are populated by the Azure DHCP service; client registration messages are ignored. If you have disabled DHCP client support in the VM by configuring a static IP address, changes to the host name or static IP in the VM aren't reflected in the zone.

upvoted 1 times

✉ **tkcito** 9 months ago

for q3, changing ip from dynamic to static via ipconfig1 in Azure portal will update the dns record but if you change the ip inside the VM WILL NOT update the dns record.

upvoted 1 times

✉ **fun\_and\_games** 9 months, 2 weeks ago

Answer N,N,Y

tested VM3 in Lab, if you change the IP through the azure portal to a static assigned IP the DNS will update.

upvoted 5 times

✉ **RollinDeep** 9 months, 1 week ago

Also tested this and confirmed its N,N,Y

upvoted 3 times

✉ **DerekKey** 9 months, 3 weeks ago

NNN

the last question refers to changing IP (assuming manually like in Azure FAQ page)

"I've reconfigured the OS in my virtual machine to have a new host name or static IP address. Why don't I see that change reflected in the private zone? "

upvoted 1 times

✉ **Houssemonline** 10 months ago

IN EXAM 18/08

upvoted 2 times

 **WickedMJ** 10 months ago

What is the correct answer then?

upvoted 1 times

 **leonidagolfe** 9 months, 1 week ago

You can't know if your answers were correct at the end of the exam!

upvoted 1 times

 **Jamesat** 10 months, 2 weeks ago

Correct

1) Manual DNS records take precedent over the automatically registered record.

2) Deleting the VM will remove only an automatically created DNS record. As it is manual it will stay.

3) Changing the IP via normal means won't change the auto-registered record as only DHCP IP addresses are auto-registered.

upvoted 1 times

**HOTSPOT -**

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

You create an IPv6 address range to Vnet1 by using a CIDR suffix of /48. You need to enable the virtual machines on Subnet1 to communicate with each other by using IPv6 addresses assigned by the company. The solution must minimize the number of additional IPv4 addresses.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Create an IPv6 subnet that uses a CIDR suffix of:

/20	▼
/24	▼
/48	▼
/64	▼

For each virtual machine, create an additional:

IP configuration	▼
NIC	▼
Public IPv6 address	▼

**Answer Area**

Create an IPv6 subnet that uses a CIDR suffix of:

/20	▼
/24	▼
/48	▼
/64	▼

Correct Answer:

IP configuration	▼
NIC	▼
Public IPv6 address	▼

Reference:

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

  **Wesgo**  1 year, 7 months ago

1) Correct: /64

Explanation: The subnets for IPv6 must be exactly /64 in size. This ensures future compatibility should you decide to enable routing of the subnet to an on-premises network since some routers can only accept /64 IPv6 routes.

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

2) Correct: Public IPv6 Address

Explanation: Add IPv6 configuration to NIC. "Configure all of the VM NICs with an IPv6 address using Add-AzNetworkInterfaceIpConfig"

Source: <https://docs.microsoft.com/en-us/azure/load-balancer/ipv6-add-to-existing-vnet-powershell>

upvoted 23 times

  **ian2387** 1 year, 2 months ago

I didnt understand.

how can public ipv6 be correct.

It is IP configuration as per your explanation as well

upvoted 3 times

👤 **Windows98** 1 year, 7 months ago

Your IPV6 address is already public.

The powershell config for this has separate IPV4 and IPV6 config blocks and I think examtopics is correct in this instance.

upvoted 7 times

👤 **sleekdunga** 1 year, 4 months ago

The correct answer was even embedded in his powershell script "Add-AzNetworkInterfaceConfig" Implying IP Configurations at the NIC level.

upvoted 5 times

👤 **jelley** Highly Voted 1 year, 7 months ago

Even based on the stated it should make sense:

And regarding the total VNET uses /48, thus it can never be lower and considering the probable need for another subnet at a later point /64 is the most likely.

You can add multiple IP configurations to a NIC thus NIC is incorrect (1x ipv4 and an ipv6 to 1 NIC). It can't be public IP's because we are talking about internal transfers thus IP Configuration is correct

upvoted 11 times

👤 **Ayokun** Most Recent 4 months ago

Wouldn't be better give a new NIC dedicated with the IPv6???

i think the correct answer is:

/64

NIC since you can't do it on the already existing one that uses the old subnet

upvoted 1 times

👤 **LeonTH** 4 months ago

maledetti

upvoted 3 times

👤 **liono** 5 months ago

Given answers are correct!

upvoted 1 times

👤 **yamapan** 6 months, 1 week ago

URL is outdated;

this is latest

<https://learn.microsoft.com/en-US/azure/load-balancer/ipv6-add-to-existing-vnet-powershell>

upvoted 2 times

👤 **HasanHHH** 8 months, 2 weeks ago

Answer: /64 - IP configuration

#Add IPv6 prefix to the VNET

\$vnet.addressspace.addressprefixes.add("fd00:db8:deca::/48")

#Add IPv6 prefix to the Subnet (smaller than addressspace)

\$subnet.addressprefix.add("fd00:db8:deca::/64")

<https://learn.microsoft.com/en-us/azure/load-balancer/ipv6-add-to-existing-vnet-powershell>

A single service instance can connect with both IPv4 and IPv6, IPv6-only are not supported, each NIC must include at least one IPv4 IP configuration.

upvoted 3 times

👤 **Pradh** 9 months ago

100% CORRECT ANSWER : /64 & IP Configuration .

upvoted 3 times

👤 **sapien45** 9 months ago

100% unhelpful comment

upvoted 15 times

👤 **hogs** 10 months ago

Appeared on exam Aug2022

upvoted 3 times

👤 **1particle** 10 months, 3 weeks ago

Correct. /64 and IP configuration

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

<https://docs.microsoft.com/en-us/answers/questions/442977/unable-to-add-ipv6-address-to-existing-azure-netwo.html>

upvoted 4 times

👤 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam 6/28/22

upvoted 2 times

 **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 2 times

 **Edward1** 1 year, 2 months ago

Answer: /64 - IP configuration

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

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

upvoted 2 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

 **sleekdunga** 1 year, 4 months ago

/64 & IP configurations. I have done this countless times in production environment.

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

upvoted 5 times

 **KranthiChaitanya** 1 year, 4 months ago

Came on exam 28/Jan/22

upvoted 1 times

**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	

Correct Answer:

**Answer Area**

Virtual WAN type:

Basic	▼
Standard	

Number of scale units:

2	▼
4	
6	
8	

Reference:

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

  **Bharat** Highly Voted 1 year, 8 months ago

8 Gig Express Route. 2 GB per ER scale unit. Therefore number of scale units = 8/2 = 4

<https://www.wwt.com/article/microsoft-azure-virtual-wan-cloud-networking-architecture>

upvoted 40 times

  **Mirek** 1 year, 8 months ago

<https://www.azure.cn/en-us/pricing/details/virtual-wan/>

upvoted 6 times

  **walkwolf3** Highly Voted 1 year, 7 months ago

Answer is correct.

Basic virtual WAN supports Site-to-site VPN only

Standard virtual WAN supports  
ExpressRoute  
User VPN (P2S)  
VPN (site-to-site)  
Inter-hub and VNet-to-VNet transiting through the virtual hub  
Azure Firewall  
NVA in a virtual WAN

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

-----

8G/2G = 4

Express Route Scale Units and Connectivity: Similar in concept to VPN scale units, customers seeking to deploy Express Route connectivity into their Virtual WAN Hubs will incur costs for the scale units provisioned in that hub, with options ranging from 1 to 10 with each representing 2Gbps of ER throughput.

<https://www.wwt.com/article/microsoft-azure-virtual-wan-cloud-networking-architecture>  
upvoted 27 times

✉️👤 **sapien45** 9 months ago

Great link !

upvoted 2 times

✉️👤 **bakamon** [Most Recent] 3 weeks ago

Correct Answer :

:: Standard

:: 4

upvoted 1 times

✉️👤 **DeepMoon** 6 months ago

I don't see any reference on Azure Documentation ([learn.microsoft.com](https://learn.microsoft.com)) talking about 4 Scale Units give 8GB.

When I look for Virtual WAN Scale Units, all I find is this doc:

<https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#for-user-vpn-point-to-site--how-many-clients-are-supported>  
According to this chart 4 scale units is wrong.

So can someone explain; where did my thinking go wrong.

upvoted 1 times

✉️👤 **khanda** 2 months, 1 week ago

Each scale unit represents 500Mbps of VPN throughput.

upvoted 1 times

✉️👤 **HasanHHH** 8 months, 2 weeks ago

Standard-Available configurations: ExpressRoute, Site-to-Site VPN

Basic-Available configurations: Site-to-site VPN only

1 scale unit of ExpressRoute = 2 Gbps. So, 4 scale unit \* 2 Gbps = 8Gbps

upvoted 1 times

✉️👤 **iwikneerg** 10 months, 2 weeks ago

What are Virtual WAN gateway scale units?

A scale unit is a unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps. 1 scale unit of ExpressRoute = 2 Gbps. Example: 10 scale unit of VPN would imply 500 Mbps \* 10 = 5 Gbps.

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units>

upvoted 2 times

✉️👤 **1particle** 10 months, 3 weeks ago

Standard and 4

Hub Type Standard:

Standard ExpressRoute

User VPN (P2S)

VPN (site-to-site)

Inter-hub and VNet-to-VNet transiting through the virtual hub

Azure Firewall

NVA in a virtual WAN

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

Gateway Scale Units:

A scale unit is a unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps. 1 scale unit of ExpressRoute = 2 Gbps

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units>

upvoted 1 times

✉️👤 **derrrp** 11 months ago

Microsoft tryna trick us talking about Site-to-Site which ya'll know is BASIC but then they say ExpressRoute in the next section which we know makes it Standard.

upvoted 6 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

 **KranthiChaitanya** 1 year, 4 months ago

Came on exam 28/Jan/22

upvoted 1 times

 **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022

upvoted 1 times

 **Pravda** 1 year, 5 months ago

Not on exam 1/6/2022

upvoted 2 times

 **Pravda** 1 year, 6 months ago

Questions exam 11/2021

upvoted 2 times

 **Acrophat** 1 year, 7 months ago

ExpressRoute gateways are provisioned in units of 2 Gbps. 1 scale unit = 2 Gbps with support up to 10 scale units = 20 Gbps.

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-expressroute-portal#hub>

upvoted 4 times

 **Wesgo** 1 year, 7 months ago

1) Of course Standard. Basic does not support ExpressRoute.

2) ExpressRoute Scale Unit3 \$0.42/hour 2 Gbps per Scale Unit

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

upvoted 6 times

 **WorkHardBeProud** 1 year, 8 months ago

What are Virtual WAN gateway scale units?

A scale unit is a unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps. 1 scale unit of ExpressRoute = 2 Gbps. Example: 10 scale unit of VPN would imply 500 Mbps \* 10 = 5 Gbps

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq#what-are-virtual-wan-gateway-scale-units>

upvoted 5 times

 **\_fvt** 2 months, 2 weeks ago

Yes the first answer is indeed Standard as it needs to support Express route.

But for the Scale unit I don't think we are talking about ExpressRoute but Azure WAN, then it should be 8 to support 8gbps.

Link where you can find AzWan Scale Units / Traffic: <https://learn.microsoft.com/en-us/azure/virtual-wan/hub-settings>

upvoted 1 times

DRAG DROP -

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

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

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

Basic **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

**IPv4 address space**

10.3.0.0/16 10.3.0.0 - 10.3.255.255 (65536 addresses)



Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet ⌂ Remove subnet

Subnet name Subnet address range NAT gateway

Subnet1 10.3.0.0/16

**i** Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#)

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

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

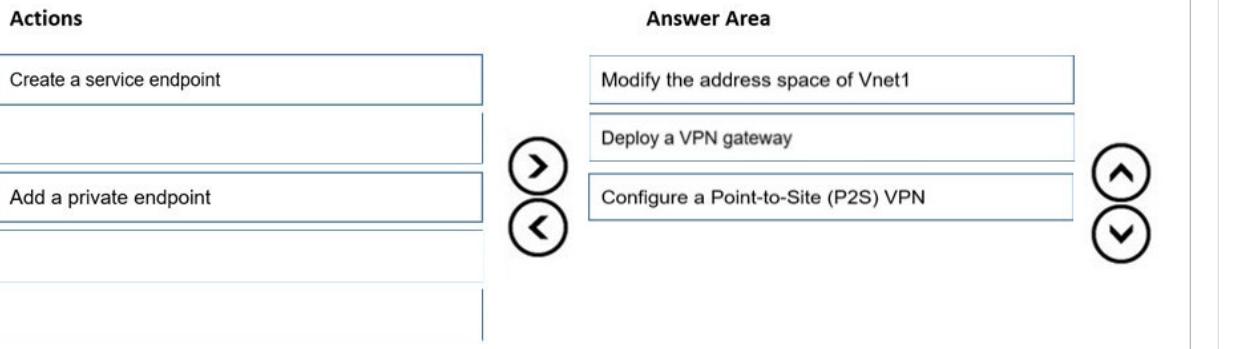
Select and Place:

**Actions**

- Create a service endpoint
- Deploy a VPN gateway
- Add a private endpoint
- Modify the address space of Vnet1
- Configure a Point-to-Site (P2S) VPN

**Answer Area**



**Correct Answer:**

Reference:

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

✉ **tkoutanis** Highly Voted 1 year, 8 months ago

Given answer is correct. Existing subnet space spans the entire address space of vnet, so it needs to be modified. Cross region vnet integration requires a vpn gateway and a point to site vpn connection. So you need to add the gateway, then configure the p2s to add address space.  
<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integration>

upvoted 49 times

✉ **walkwolf3** Highly Voted 1 year, 7 months ago

Answer is correct, it talks about cross region vent integration.

Service endpoint is for regional or same region virtual network integration.

Private endpoint is to use private DNS integration.

upvoted 14 times

✉ **tester2023** Most Recent 4 months, 3 weeks ago

I tested in the lab, and when attempting to add vNet integration to the App Service, the Portal menu allows same region automatically, but it shows "Other regions (requires a Virtual Network Gateway configured with Point to Site VPN)."

upvoted 2 times

✉ **AdityaGupta** 9 months ago

The virtual network integration feature has two variations:

1) Since you need to deploy a VNET Gateway, address space need to be modified, currently subnet is consuming entire address space.

2) You must a deploy a VPN Gateway, since Web App and VNet are in different regions.

a. Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

b. Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

3) Requires a virtual network route-based gateway configured with an SSTP point-to-site VPN before it can be connected to an app.

upvoted 3 times

✉ **1particle** 10 months, 3 weeks ago

Correct

Gateway-required virtual network integration supports connecting to a virtual network in another region or to a classic virtual network. Gateway-required virtual network integration: Requires a virtual network route-based gateway configured with an SSTP point-to-site VPN before it can be connected to an app.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-virtual-network-integration>

upvoted 2 times

✉ **Takloy** 11 months ago

If you look at the resources locations, both of them are on a different region. So Service and Private is out of the picture. Must prioritize VPN connectivity first.

upvoted 2 times

✉ **derrrp** 11 months ago

Remember:

Modify the VNET so you can add the VPN.

Add the VPN.

Then configure it.

upvoted 4 times

✉ **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam 6/28/22

upvoted 1 times

✉ **ash21** 1 year ago

The mentioned answer is correct, <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>.

upvoted 1 times

✉ **Stanley3427** 1 year ago

the answer is 413, this question will not use vpn services

upvoted 2 times

✉ **petermogaka91** 1 year, 1 month ago

Answers are correct. Check the link below

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

upvoted 1 times

✉ **Edward1** 1 year, 2 months ago

The answers are correct.

Virtual network integration doesn't enable your apps to be accessed privately.

upvoted 1 times

✉ **Pravda** 1 year, 5 months ago

on exam 1/6/2022

upvoted 3 times

✉ **Pravda** 1 year, 6 months ago

Questions exam 11/2021

upvoted 3 times

✉ **WorkHardBeProud** 1 year, 8 months ago

Requires a virtual network route-based gateway configured with an SSTP point-to-site VPN before it can be connected to an app.<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integration>

upvoted 1 times

✉ **RandomUser** 1 year, 8 months ago

Correct. Vnet integration and PLink are out of question due to different regions. Leaves us only vpn but this needs a new subnet but there is no space left currently.

upvoted 6 times

✉ **5iB** 1 year, 8 months ago

The answer on the engine seems back to front to me. Surely the answer is to create the service endpoint and then the private endpoint so the vnet in a different region can contact the web app in another region?

upvoted 1 times

✉ **5iB** 1 year, 8 months ago

I have now realised that private endpoint must be in the same region as the vnet, as such I agree that the only other alternative is VPN and subnet change.

upvoted 1 times

**DRAG DROP -**

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

You are implementing peering between Hub1 and Spoke1.

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

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

NOTE: Each correct selection is worth one point.

Select and Place:

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

**Correct Answer:**

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

**Reference:**

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

✉  **Bharat**  1 year, 8 months ago

The answer is correct. However, this is a better reference: <https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-ps>  
upvoted 26 times

✉  **jeepTango123456** 10 months, 1 week ago

From the link the example, the answer here seems to be reversed.

# Peer hub to spoke

Add-AzVirtualNetworkPeering -Name HubtoSpoke -VirtualNetwork \$VNetHub -RemoteVirtualNetworkId \$VNetSpoke.Id -AllowGatewayTransit

# Peer spoke to hub

Add-AzVirtualNetworkPeering -Name SpoketoHub -VirtualNetwork \$VNetSpoke -RemoteVirtualNetworkId \$VNetHub.Id -AllowForwardedTraffic -UseRemoteGateways

upvoted 7 times

✉  **MrBlueSky** 2 months, 3 weeks ago

No, Bharat is correct. Not sure why you said that the answers are reversed because even in your example the peering performed on the hub network is set to AllowGatewayTransit and the peering set on the Spoke network is 'UseRemoteGateways'  
upvoted 1 times

✉  **walkwolf3**  1 year, 7 months ago

Answer is correct

-AllowGatewayTransit

Select Use this virtual network's gateway or Route Server:

- If you have a virtual network gateway attached to this virtual network and want to allow traffic from the peered virtual network to flow through the gateway.

-UserremoteGateways

Select Use the remote virtual network gateway or Route Server:

- If you want to allow traffic from this virtual network to flow through a virtual network gateway attached to the virtual network you're peering with.

Box1: Hub told spoke to use hub's VPN gateway to reach on-premise network

Box2: Spoke told hub to use hub's VPN gateway to reach on-premise network

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

upvoted 18 times

✉ **MikeSA** Most Recent 6 days, 9 hours ago

Confusing because the second part could be either allowforwarded or useremotegateways. Seems to be missing one of the options.

# Peer spoke to hub

Add-AzVirtualNetworkPeering -Name SpoketoHub -VirtualNetwork \$VNetSpoke -RemoteVirtualNetworkId \$VNetHub.Id -AllowForwardedTraffic -UseRemoteGateways

upvoted 1 times

✉ **Himank20** 1 month, 3 weeks ago

Given answer is correct.

In the hub, we need to enable AllowGatewayTransit and in the spoke we need to enable UseRemoteGateway

upvoted 1 times

✉ **mauchi** 4 months, 2 weeks ago

I think the answer should be reversed, as per the docu <https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#virtual-network-peering%20%20%20Previous%20QuestionsNext%20Questions>

- Configure the peering connection in the hub to allow gateway transit.

- Configure the peering connection in each spoke to use remote gateways.

upvoted 2 times

✉ **sshera** 5 months, 2 weeks ago

In exam 04jan23

upvoted 2 times

✉ **sapien45** 8 months, 2 weeks ago

Make sure to set AllowGatewayTransit when peering VNet-Hub to VNet-Spoke and UseRemoteGateways when peering VNet-Spoke to VNet-Hub.

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-hybrid-ps>

upvoted 3 times

✉ **sapien45** 9 months ago

Allow forwarded traffic does not apply here, Allow forwarded traffic is so you can have a network appliance (NVA) in the hub that routes traffic between two spokes. When the NVA goes to forward the traffic from spoke 1 into spoke 2, this setting needs to be enabled or else Azure SDN will drop the traffic.

Details on <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke#spoke-connectivity>

upvoted 1 times

✉ **derrp** 11 months ago

It will help to remember that the hub needs to know the remote networks available from on-prem (-UseRemoteGateways) whereas a spoke network which will be connected to the hub is where you'll need to worry about making it transitive so that traffic can route through (-AllowGatewayTransit)

-AllowForwardedTraffic does not get used at all but let's move FORWARD onto the next question now that we've got this one memorized.

upvoted 2 times

✉ **Edward1** 1 year, 2 months ago

The answers are correct.

upvoted 1 times

✉ **jj22222** 1 year, 2 months ago

on test April 10 2022

upvoted 1 times

✉ **Joshalom** 1 year, 4 months ago

on exam 6/2/2022

upvoted 1 times

✉ **Joshalom** 1 year, 4 months ago

on exam 28/1/2022

upvoted 1 times

✉ **Takloy** 1 year, 5 months ago

Seems correct...

I find the article below better.

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

upvoted 2 times

- ✉  **Pravda** 1 year, 5 months ago  
on exam 1/6/2022  
upvoted 3 times
- ✉  **Pamban** 1 year, 6 months ago  
appeared on exam 5th Dec 2021  
upvoted 3 times
- ✉  **Pravda** 1 year, 6 months ago  
Not on the updated exam 11/23/2021.  
upvoted 2 times

**DRAG DROP -**

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

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

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

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

Select and Place:

**Actions**

Download the VPN configuration file from VWAN1

In a Hub1, create a VPN gateway

In a Hub1, create a VPN site

In a Hub1, create a connection to the VPN site

Configure the VPN device

**Answer Area****Correct Answer:****Actions**

In a Hub1, create a VPN gateway

**Answer Area**

In a Hub1, create a VPN site

In a Hub1, create a connection to the VPN site

Download the VPN configuration file from VWAN1

Configure the VPN device

**Reference:**

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

✉ srikanth1987 Highly Voted 1 year, 7 months ago

Answer is correct. As already two VPN S2S are formed, means that, VGW is there.

upvoted 36 times

✉ jeffangel28 10 months, 2 weeks ago

Right!

upvoted 1 times

✉ Takloy 11 months ago

You're right.

upvoted 1 times

✉ derrrp Highly Voted 11 months ago

To help remember, visualize:

You've already got the VPN infrastructure setup in Azure so you need to create the Site, Create the connection to the site, Download the stuff, then setup the on-prem side.

Make the site, connect to site, download the thing, config the on-prem.

upvoted 26 times

✉ Stevy\_nash 5 months ago

your way of explaining stuff is so funny but I it thx (^\_^\n

upvoted 1 times

- ✉  **Rajan395** Most Recent ⓘ 4 months, 3 weeks ago  
Correct Answer  
upvoted 1 times
- ✉  **sujay1982** 9 months, 2 weeks ago  
Right Answer  
upvoted 2 times
- ✉  **GGbis** 11 months, 2 weeks ago  
Answer is correct. <https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal#vnet>  
upvoted 1 times
- ✉  **bmulvIT** 1 year, 3 months ago  
On exam 3/3/2022  
upvoted 4 times
- ✉  **rockethack** 1 year, 3 months ago  
This question was on the exam on 18th Feb 2022.  
upvoted 4 times
- ✉  **Kimimoto** 1 year, 4 months ago  
Appeared in exam on 11/Feb/2022  
upvoted 3 times
- ✉  **KranthiChaitanya** 1 year, 4 months ago  
Came on exam 28/Jan/22  
upvoted 2 times
- ✉  **Pravda** 1 year, 5 months ago  
on exam 1/6/2022  
upvoted 3 times
- ✉  **AidenYoukhana** 1 year, 5 months ago  
CORRECT ANSWER.  
upvoted 2 times
- ✉  **JoMa** 1 year, 6 months ago  
Correct answer  
upvoted 4 times

**HOTSPOT -**

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area****Virtual Networks:**

1
2
3
4

**Subnets:**

1
2
3
4

**Answer Area****Virtual Networks:**

1
2
3
4

**Correct Answer:**

1
2
3
4

Reference:

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

  **Pravda** Highly Voted 1 year, 6 months ago

Question was on exam 11/2021

I believe the answer to be 1 and 4.

Web page given in answer, and below states App Service Environment requires a dedicated subnet.

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services#services-that-can-be-deployed-into-a-virtual-network>  
upvoted 33 times

  **prepper666** Highly Voted 1 year, 7 months ago

Correct answer is 1 Vnet. 3 Subnets are needed.

Gateway subnet for VPN Gateway.

Default subnet for VM

Dedicated subnet for SQL Managed instance.

<https://azure.microsoft.com/en-gb/resources/templates/sql-managed-instance-azure-environment/>

No subnet is needed for App Service. Build it and dont just believe the answers written here as many answers are wrong.

upvoted 12 times

✉ **leonmflai4exam** 1 year, 3 months ago

For Azure WebApp, we need to add webapp-integration subnet. <https://docs.microsoft.com/en-us/azure/app-service/networking/nat-gateway-integration>

upvoted 6 times

✉ **AjdIfasudfo0** 6 months, 3 weeks ago

you better get some experience before shouting so loud lol

upvoted 1 times

✉ **HasanHHH** 8 months, 2 weeks ago

Wrong. An app service needs its own dedicated subnet.

Web API Management-Dedicated Subnet-Yes

Web Apps-Dedicated Subnet-Yes

App Service Environment-Dedicated Subnet-Yes

Azure Logic Apps-Dedicated Subnet-Yes

upvoted 1 times

✉ **AnonymousJhb** 1 year, 3 months ago

wrong. an app service needs it's own dedicated subnet.

"Nothing else can be in the subnet but the App Service Environment. Be sure to choose an address space that allows for future growth. You can't change this setting later. We recommend a size of /24 with 256 addresses."

upvoted 8 times

✉ **rac\_sp** 11 months, 1 week ago

that is correct, because in the question it says: App Service and SQL Managed Instance will be delegated to create resources in virtual networks.

upvoted 4 times

✉ **AzureLearner01** [Most Recent] 3 months ago

Provided answer is correct. You need a subnet for the vm, a dedicated for the gateway, app service (vnet integration) and sql managed instance.

upvoted 2 times

✉ **Libaax01** 3 months, 1 week ago

The provided answer is correct and can be confirmed by the original linked shared.

1 Virtual Network (Vnet)

4 Subnets ( Default subnet where the VMs will reside, Dedicated subnet for APP Services, Dedicated subnet for Virtual Network Gateway, and finally dedicated subnet for SQL Managed services)

upvoted 1 times

✉ **Rajan395** 4 months, 3 weeks ago

Given answer is correct.

upvoted 1 times

✉ **sapien45** 8 months, 2 weeks ago

The solution must minimize costs to transfer data between virtual networks.

Meaning App service Gateway-required virtual network integration is not an option.

The regional virtual network integration feature enables you to place the back end of your app in a subnet in a Resource Manager virtual network in the same region as your app. This feature isn't available from an App Service Environment, which is already in a virtual network.

<https://learn.microsoft.com/en-us/azure/app-service/networking-features>

4 it is

upvoted 3 times

✉ **Jamesat** 10 months ago

This was on my exam on 22/08/2022

The correct answer did indeed seem to be 1 and 4.

A subnet for the VPN Gateway

Subnet for VMs

Subnet for App Service VNET integration (as delegated)

Subnet for SQL Managed Instance (as delegated)

upvoted 6 times

✉ **1particle** 10 months, 3 weeks ago

1 and 4

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/connectivity-architecture-overview?view=azuresql#high-level-connectivity-architecture>

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

VPN gateway of course needs a VPN subnet  
VM will be in the 4th

upvoted 1 times

✉ **Payday123** 11 months, 3 weeks ago

"App Service and SQL Managed Instance will be delegated to create resources in virtual networks" so App service requires delegates subnet for integration!

upvoted 2 times

✉ **Whatsamattr81** 1 year ago

Correct is 4. 2 subnets for the VPN gateway, the app service and vm can be on the same one, and Azure SQL Managed Instance must be deployed within an Azure virtual network and the subnet dedicated for managed instances only.

upvoted 1 times

✉ **Madball** 1 year, 2 months ago

I believe the given answer is correct, my reasoning for this is as follows.

1. Azure SQL Managed Instance requires its own subnet.
2. A Virtual Network Gateway requires its own subnet.
3. An app service by default does not connect to a virtual network and is accessible by its public frontend. It is my understanding that if you want an app service to integrate with a virtual network you need to enable VNET integration, which requires its own subnet.
4. The VM can share subnets, however in this question there are 4 resources and three of them require their own subnet, meaning the VM will require its own subnet in this instance.

upvoted 8 times

✉ **bmulvIT** 1 year, 3 months ago

On exam today 3/3/2022

upvoted 1 times

✉ **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

✉ **Beitran** 1 year, 3 months ago

"Virtual network integration depends on a dedicated subnet. "

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integration>

So yes, 4 subnets is correct

upvoted 1 times

✉ **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

✉ **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022

upvoted 2 times

✉ **TonytheTiger** 1 year, 5 months ago

On the Exam 01/14/2022

upvoted 3 times

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

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

You have two Azure virtual networks named Vnet1 and Vnet2.

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

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

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You download and reinstall the VPN client configuration.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

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

Reference:

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

*Community vote distribution*

A (100%)

✉  **d0bermannn** Highly Voted 1 year, 4 months ago

**Selected Answer: A**

A.The VPN client must be downloaded again if any changes are made to VNet peering or the network topology  
upvoted 9 times

✉  **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023  
upvoted 1 times

✉  **Rajan395** 4 months, 3 weeks ago

Given answer is correct  
upvoted 1 times

✉  **ypts** 8 months, 3 weeks ago

Does Windows10 work with IKEv2 P2S VPN?  
upvoted 1 times

✉  **jilguens** 9 months, 2 weeks ago

**Selected Answer: A**

right a  
upvoted 1 times

✉  **AckeyGraham** 1 year, 4 months ago

Questions in wrong order - you get the answer on earlier pages, but again with no context. Doesn't tell you that the client was downloaded prior to any changes being made to an existing network, then peering setup...then the client has an issue - not sure if that will be told in the actual exam - i'd hope so.  
upvoted 2 times

✉  **Joshalom** 1 year, 4 months ago

correct....on exam 28/1/2022  
upvoted 1 times

✉  **AidenYoukhana** 1 year, 5 months ago

CORRECT ANSWER.  
upvoted 1 times

✉  **Pravda** 1 year, 5 months ago

On exam. 11/2021  
upvoted 2 times

✉  **Cova16** 1 year, 7 months ago

correct  
upvoted 1 times

 **prepper666** 1 year, 7 months ago  
Agreed. Initial config was downloaded before vNet1 and vNet2 were peered.  
upvoted 1 times

 **Sbgani** 1 year, 8 months ago  
correct  
upvoted 4 times

You have an Azure virtual network named Vnet1 that hosts an Azure firewall named FW1 and 150 virtual machines. Vnet1 is linked to a private DNS zone named contoso.com. All the virtual machines have their name registered in the contoso.com zone. Vnet1 connects to an on-premises datacenter by using ExpressRoute. You need to ensure that on-premises DNS servers can resolve the names in the contoso.com zone. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Modify the DNS server settings of Vnet1.
- B. For FW1, configure custom DNS server.
- C. For FW1, enable DNS proxy.
- D. On the on-premises DNS servers, configure forwarders that point to the frontend IP address of FW1.
- E. On the on-premises DNS servers, configure forwarders that point to the Azure provided DNS service at 168.63.129.16.

**Correct Answer:** CD

Reference:

<https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns#on-premises-workloads-using-a-dns-forwarder>

<https://azure.microsoft.com/en-gb/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>

*Community vote distribution*

CD (100%)

✉️  **Whatsamattr81**  1 year ago

C and D... whilst E looks correct, it isn't a viable answer. Currently that IP address resolves to ns1-02.azure-dns.com - on which your custom domain may not even sit. If the on-premise DNS was bind, it would probably skip the DNS proxy stuff and just put forwarders in, but the question and possible answers don't mention that scenario.

upvoted 9 times

✉️  **MrBlueSky** 2 months, 3 weeks ago

Put more simply, the reason why E is wrong is because an Azure Private DNS Zone cannot be used by on-premises resources. For that they would need to use Azure DNS Private Resolver. It's a specific resource for this exact scenario described in the question:  
<https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-overview>

upvoted 1 times

✉️  **erima21**  9 months, 2 weeks ago

Requests sent to Azure DNS Private Zones go to the platform address of 168.63.129.16 that is only reachable from inside of Azure. Therefore, if the DNS request originates from on-premises (outside of Azure), there is a requirement to proxy the DNS request via a service inside of a Virtual Network.

With this general availability announcement, Azure Firewall DNS proxy is an option to meet this DNS forwarding requirement, applicable with a hub-and-spoke model. To do this, configure your on-premises DNS server to conditionally forward requests to Azure Firewall for the required zone name.

upvoted 7 times

✉️  **AzureLearner01**  3 months ago

Correct Answer, you need conditional forwarding for the on-prem DNS to the Azure Firewall. In the firewall policy enable DNS Proxy.

upvoted 1 times

✉️  **sapien45** 9 months ago

**Selected Answer: CD**

Azure Firewall DNS proxy is an option to meet this DNS forwarding requirement, applicable with a hub-and-spoke model. To do this, configure your on-premises DNS server to conditionally forward requests to Azure Firewall for the required zone name. Ensure that your private DNS zone is linked to the Virtual Network within which the Azure Firewall resides. Configure Azure Firewall to use the default Azure DNS for lookups, and enable DNS proxy in Azure Firewall DNS settings.

<https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>

upvoted 5 times

✉️  **AdityaGupta** 9 months ago

**Selected Answer: CD**

Explanation provided by "Erima21" is best. There are two ways to do it.

1) Create DNS Proxy on Azure Firewall in Hub VNET to forward all external DNS requests (from On-prem) to Azure DNS (168.63.129.16) and configure your on-prem DNS server with forwarder to Azure Firewall DNS Proxy. In this case you can still use Azure DNS in VNETs or configure them with Azure Firewall DNS Proxy IP (Custom DNS server)

1) Provision a VM as custom DNS Server in Hub VNET and configure all your private zones requests and external DNS requests to be forwarded to Azure DNS (168.63.129.16) and configuire your on-prem DNS server with forwarder to Azure DNS VM.

upvoted 4 times

✉ **Takloy** 11 months ago

Can someone explain why the answers are CD?

I thought E would be one of the answers.

upvoted 1 times

✉ **john6732** 11 months ago

Technically you would need to perform both B and C, but enable DNS proxy is the best exam answer. You need to add the custom server and then turn on Proxy so that the AFW sends DNS to said server.

DNS proxy listens for requests on TCP port 53 and forwards them to Azure DNS or the custom DNS specified.

upvoted 2 times

✉ **unclegrandfather** 11 months, 3 weeks ago

A version of this question appeared on the exam. Make sure you know WHY these are correct

upvoted 2 times

✉ **kinder2** 1 year ago

**Selected Answer: CD**

DNS proxy configuration requires three steps:

Enable DNS proxy in Azure Firewall DNS settings.

Optionally configure your custom DNS server or use the provided default.

Finally, you must configure the Azure Firewall's private IP address as a custom DNS server in your virtual network DNS server settings. This ensures DNS traffic is directed to Azure Firewall.

upvoted 7 times

✉ **milan92stankovic** 1 year ago

**Selected Answer: CD**

C and D are correct.

upvoted 4 times

✉ **mdnick** 1 year, 1 month ago

Provided answers are correct. This is similar to private link resolution.

<https://github.com/adstuart/azure-privatelink-dns-azurefirewall>

upvoted 4 times

✉ **madsa** 1 year, 1 month ago

So it would be A and C, not E as per the link, I would much appreciate it if someone can clarify this question for me, what is the actual answer and why?

upvoted 1 times

✉ **RVR** 1 year, 1 month ago

A & E would be better options?

upvoted 2 times

✉ **jkklim** 1 year, 1 month ago

ae - the answer

upvoted 1 times

✉ **jamelia1303** 1 year, 2 months ago

better explanation : <https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>

upvoted 2 times

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. internal load balancers
- B. storage account
- C. Azure Virtual Networks NAT
- D. service endpoint policies

**Correct Answer: A**

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

*Community vote distribution*

A (100%)

 **SOMINAZURE** 3 months, 1 week ago

**Selected Answer: A**

yes correct

upvoted 2 times

 **JennyHuang36** 3 months, 3 weeks ago

In exam Feb,2023

upvoted 2 times

 **sellamibassem** 3 months, 4 weeks ago

A is correct

upvoted 1 times

 **Rajan395** 4 months, 3 weeks ago

A is correct for sure

upvoted 1 times

 **degiro** 7 months, 3 weeks ago

**Selected Answer: A**

Answer is correct.

upvoted 1 times

 **Prutser2** 8 months, 1 week ago

**Selected Answer: A**

for sure

upvoted 1 times

 **Jawad1462** 8 months, 3 weeks ago

**Selected Answer: A**

Answer is correct A

upvoted 1 times

 **Alessandro365** 9 months ago

**Selected Answer: A**

A, correct answer

upvoted 1 times

 **AdityaGupta** 9 months ago

**Selected Answer: A**

Undoubtly A, Internal Load Balancer.

upvoted 1 times

 **naidu** 9 months, 3 weeks ago

Yes Correct answer

upvoted 2 times

 **Villaran** 9 months, 3 weeks ago

**Selected Answer: A**

A. internal load balancers  
upvoted 2 times

**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

Correct 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

Reference:

✉ **AdityaGupta** Highly Voted 9 months ago

VWAN Type Hub type Available configurations

Basic Basic Site-to-site VPN only

Standard Standard ExpressRoute

User VPN (P2S)

VPN (site-to-site)

Inter-hub and VNet-to-VNet transiting through the virtual hub

Azure Firewall

NVA in a virtual WAN

upvoted 9 times

✉ **omgMerrick** Most Recent 4 months ago

Given answer is correct.

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

upvoted 1 times

✉ **Rajan395** 4 months, 3 weeks ago

Answer is correct. Basic sku supports Site-to-Site only

upvoted 2 times

✉ **Jawad1462** 8 months, 3 weeks ago

That's correct

upvoted 3 times

✉ **fun\_and\_games** 9 months, 1 week ago

Vitual WAN

Basic

Site-to-site Only

Standard

ExpressRoute

User VPN (P2S)

VPN (site-to-site)

Inter-hub and VNet-to-VNet transiting through the virtual hub

Azure Firewall

NVA in a virtual WAN

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

upvoted 4 times

✉ **Cristoicach91** 9 months, 3 weeks ago

This is correct.

upvoted 3 times

**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.

The screenshot shows the Azure DNS Zone configuration for the domain fabrikam.com. The interface includes a header with 'DNS' and 'fabrikam.com' (DNS zone), and a toolbar with 'Record set', 'Child zone', 'Move', 'Delete zone', and 'Refresh' buttons. A 'JSON View' link is also present. Below the toolbar, there's a section titled 'Essentials' containing resource group, subscription, and name server information. A note indicates that more record sets can be loaded by scrolling. A search bar for 'Search record sets' is at the bottom of this section. The main table lists the following records:

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.



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)	:	<a href="#">Click here to add tags</a>

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

 Search record sets

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.co... Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
			Subscription (change) : Subscription1	
			Subscription ID : 169d1bba-ba4c-471c-b513-092eb7063265	
			Tags (change) : <a href="#">Click here to add tags</a>	

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

 Search record sets

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

 Fabrikam.com | Virtual network links ... ×

Private DNS zone

+ Add     Refresh

 Search virtual network links

Link Name	Link status	Virtual network	Auto-Registration	...
vnet1_link	Completed	Vnet1	Disabled	...

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"/>

Correct 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"/>

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.

  AdityaGupta Highly Voted 9 months ago

The given answers and explanations are correct, please pay attention to following details if you are confused.

- 1) Public DNS Zones are created for Internet Dns requests.
- 2) Private DNS Zones are created to cater internal DNS requests.
- 3) Private DNS Zones must be linked (private links) to VNETs to ensure that resources inside that VNET can make use of private dns zone. In this case it "VNET1\_Link" created but no "VNET2\_Link" is created.

upvoted 22 times

 **wsrudmen** Highly Voted 1 year, 1 month ago

CORRECT!!

upvoted 11 times

 **\_fvt** Most Recent 2 months, 2 weeks ago

They say : "You register a Public DNS zone" but not "and you delegate your domain from your registrar to the Public DNS zone" so this step is missing. The wording for the Private DNS is "You have" so this is different here they don't mention any step. I think the difference is important and the fact that they choose this for the Public DNS is probably because the delegate step is missing.  
<https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

Should be NNN (for the last one VNet2 is not linked to private DNS so cannot resolve names in the private DNS)

upvoted 1 times

 **Rajan395** 4 months, 3 weeks ago

absolutely correct.

upvoted 1 times

 **DeepMoon** 5 months, 1 week ago

Public dns zone doesn't have cname record for www. So how can internet queries for www resolve to 131.107.1.1?  
Box 1 should be NO.

Box 2 should be NO - there is no server1 record on public dns.

Box 3 No. vnet 2 is not linked to the private dns zone.

upvoted 2 times

 **Skankhunt** 4 months, 2 weeks ago

Look carefully there's a host-A record for appservice1 in Public DNS Zone.

upvoted 4 times

 **sshera** 5 months, 2 weeks ago

In exam 04Jan23

upvoted 2 times

 **Prutser2** 8 months, 1 week ago

correct,

upvoted 1 times

 **jeffangel28** 10 months, 2 weeks ago

Given answer and explanation is correct

upvoted 2 times

**HOTSPOT -**

You have two Azure virtual networks named VNet1 and VNet2 in an Azure region that has three availability zones.

You deploy 12 virtual machines to each virtual network, deploying four virtual machines per zone. The virtual machines in VNet1 host an app named App1. The virtual machines in VNet2 host an app named App2.

You plan to use Azure Virtual Network NAT to implement outbound connectivity for App1 and App2.

You need to identify the minimum number of subnets and Virtual Network NAT instances required to meet the following requirements:

- ⇒ A failure of two zones must NOT affect the availability of either App1 or App2.
- ⇒ A failure of two zones must NOT affect the outbound connectivity of either App1 or App2.

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Minimum number of subnets:

1
2
6
12

Minimum number of Virtual Network NAT instances:

1
2
6
12

**Correct Answer:**

**Answer Area**

Minimum number of subnets:

1
2
6
12

Minimum number of Virtual Network NAT instances:

1
2
6
12

Reference:

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

  **pinchocr** Highly Voted  1 year ago

You cannot assign more than one nat gw to a subnet. 6 subnets are required (3 in vnet1 and 3 in vnet2). Then assign zonal nat gateways to each subnet

upvoted 25 times

✉️  **Komy** 12 months ago

Not right. Even though you can not assign multiple NAT GW to the same subnet - however - Multiple subnets within the same virtual network can use the same NAT gateway. so we can create 2 Subnets(1 per each VNET) and 2 NAT GW (1 per each Vnet/subnet).. and because NAT GW is zonal, we will have to multiply that by 3 = 6 NAT GW

2 subnets/ 6 NAT GW

upvoted 6 times

✉️  **Komy** 11 months, 4 weeks ago

Correction: Reviewing the below architecture, answer should be: 6 Subnets / 6 NAT GW

<https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway>

upvoted 13 times

✉️  **john6732** 11 months ago

This is correct:

Availability zone isolation cannot be provided, unless each subnet only has resources within a specific zone. Instead, deploy a subnet for each of the availability zones where VMs are deployed, align the zonal VMs with matching zonal NAT gateways, and build separate zonal stacks. For example, a virtual machine in availability zone 1 is on a subnet with other resources that are also only in availability zone 1. A NAT gateway is configured in availability zone 1 to serve that subnet.

upvoted 7 times

✉️  **sapien45** 9 months ago

I concur, but best is to prove your point with official Azure Litteraure

<https://learn.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway>

upvoted 3 times

✉️  **Jorex**  1 year, 1 month ago

I would say 2 subnets, because the subnets are regional resources, hence they exists in all zones and 6 NAT gateways (Virtual NAT refers to virtual NAT gateway: <https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview>), because the NAT gateway is zonal, so you have to deploy a NAT gateway in each zone to have the full redundancy. ([https://docs.microsoft.com/en-us/azure/virtual-network/nat-overview#virtual-network-nat-basics](https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#virtual-network-nat-basics))

upvoted 19 times

✉️  **khanda** 2 months, 1 week ago

You cant attach multiple NAT gateways to a single subnet.

upvoted 1 times

✉️  **Goofier** 5 months, 1 week ago

See - <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones#zonal-nat-gateway-resource-for-each-zone-in-a-region-to-create-zone-resiliency>

upvoted 1 times

✉️  **Sanaz90** 9 months, 1 week ago

Multiple NAT gateways can't be attached to a single subnet.

upvoted 3 times

✉️  **Arkadeep** 12 months ago

1 subnet can have only 1 nat gateway, so 6 subnets are required for 6 nat gateway.

upvoted 9 times

✉️  **roshingrg**  1 day, 3 hours ago

The minimum number of subnets required is 6, and the minimum number of Virtual Network NAT instances required is 3.

Here is the reasoning:

To meet the requirement that a failure of two zones must not affect the availability of either App1 or App2, we need to place the virtual machines for each app in at least two different zones. This means that we need a total of 6 zones, 3 for each app.

To meet the requirement that a failure of two zones must not affect the outbound connectivity of either App1 or App2, we need to place a Virtual Network NAT instance in each zone. This means that we need a total of 3 NAT instances.

Therefore, the minimum number of subnets required is 6, and the minimum number of Virtual Network NAT instances required is 3.

Answer:

Minimum number of subnets: 6

Minimum number of Virtual Network NAT instances: 3

upvoted 1 times

✉️  **roshingrg** 1 day, 3 hours ago

The number of NAT instances that can be deployed in a single region is 1, 2, 6, or 12. Therefore, the minimum number of NAT instances required in this case is 2.

The answer would then be:

Minimum number of subnets: 6

Minimum number of Virtual Network NAT instances: 2

I apologize for the error in my previous response.

upvoted 1 times

✉ **occupatissimo** 1 month, 3 weeks ago

NAT GW is a zonal resource  
To have complete availability configure 6+6  
upvoted 2 times

✉ **michealnghe** 2 months, 3 weeks ago

Correct answer must be  
6 subnets  
6 NAT Gateways  
<https://azure.microsoft.com/en-us/blog/ensure-zone-resilient-outbound-connectivity-with-nat-gateway/>  
upvoted 5 times

✉ **MightyMonarch74** 2 months, 3 weeks ago

Correct answer should be 6 subnets with 6 NAT GW, using a zonal NAT gateway resource for each zone in a region as per  
<https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway>  
upvoted 3 times

✉ **AzureLearner01** 3 months ago

NAT gateway resources are highly available in one availability zone and span multiple fault domains. NAT gateway can be deployed to "no zone" in which Azure automatically selects a zone to place NAT gateway. NAT gateway can also be isolated to a specific zone by a user.  
Availability zone isolation cannot be provided, unless each subnet only has resources within a specific zone. Instead, deploy a subnet for each of the availability zones where VMs are deployed, align the zonal VMs with matching zonal NAT gateways, and build separate zonal stacks. For example, a virtual machine in availability zone 1 is on a subnet with other resources that are also only in availability zone 1. A NAT gateway is configured in availability zone 1 to serve that subnet.

See the diagram at  
<https://learn.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway>  
upvoted 1 times

✉ **stack120566** 3 months ago

One subnet in each zone for each Vnet =6 subnets  
need to Nat gateways in each zone .Nat gateways can not be associated with subnets from different vnets .. only 1 Nat gateway per subnet. = 6  
Nat gateways  
upvoted 1 times

✉ **zukako** 3 months, 2 weeks ago

NAT gateway cannot associate subnet across VNets->2  
Azure subnet can has vms in multi-Az->2  
upvoted 1 times

✉ **omgMerrick** 3 months, 3 weeks ago

6 and 6.

The minimum number of subnets required is six, one for each zone in each virtual network. This way, you can associate a NAT gateway resource to each subnet and provide outbound connectivity for all compute resources in that subnet2.

The minimum number of Virtual Network NAT instances required is six, one for each subnet. This way, you can ensure that a failure of two zones will not affect the availability or outbound connectivity of either App1 or App2.

upvoted 3 times

✉ **Madball** 4 months, 3 weeks ago

I personally believe the answer should be 6 and 6, the reason for this is as follows, you have 24 VMs in total with 12 deployed to each VNET. To help with availability you will deploy 4 VMs to each availability zone.  
The first question is how many subnets are required (minimum), and this is the part that will trick people into the wrong answer if they are unsure on how NAT gateway is deployed. Technically at this point you would only need two subnets because VNets do not care about zones, however you cannot deploy two or more NAT gateways to the same subnet and NAT gateways are zonal.  
This means that to cover 3 availability zones, you will need 3 NAT gateways, which then in turn means you need to link each NAT gateway to a separate subnet (3 subnets) giving a total of 6 NAT gateways and 6 subnets across the two VNets.

upvoted 6 times

✉ **sandydh** 4 months, 3 weeks ago

Zonal NAT gateway resource for each zone in a region to create zone-resiliency. <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones>.  
Exact scenario is given in simpler form.

Since, it is expected to provide protection against 2 zone failures, hence, 3 subnets per vNET is needed and 4 VM's per Zone making it 12.

Answer should be 6 Subnets and 6 NAT

upvoted 3 times

✉ **Stevy\_nash** 5 months ago

6 subnets and 2 NAT  
Multiple subnets within the same virtual network can either use different NAT gateways or the same NAT gateway.  
upvoted 1 times

✉ **Wis10** 5 months, 1 week ago

Correct answer:

- Minimum snets = 6 (3 for each vnet, 1 for each region)
- Minimum NAT GWs = 6 (each subnet must have its own NAT GW)

Tested on my lab, and explained here:

<https://learn.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway#reliability>

upvoted 5 times

✉️ **Goofer** 5 months, 1 week ago

Zonal NAT gateway resource for each zone in a region to create zone-resiliency

1 vNet1 (App1)

3 Availability Zones

3 subnets (4 servers per availability zone,  $3 \times 4 = 12$ )

3 zonal Nat gateways (1 per availability zone)

1 vNet2 (App2)

3 Availability Zones

3 subnets (4 servers per availability zone,  $3 \times 4 = 12$ )

3 zonal Nat gateways (1 per availability zone)

Total of 6 subnets and 6 NAT gateways

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones#zonal-nat-gateway-resource-for-each-zone-in-a-region-to-create-zone-resiliency>

upvoted 4 times

✉️ **sshera** 5 months, 2 weeks ago

In exam 04jan23

upvoted 1 times

✉️ **Takloy** 7 months, 2 weeks ago

6 Subnets and 6 NAT GWs.

See this article: <https://learn.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-network-address-translation-gateway#reliability>

upvoted 3 times

HOTSPOT -

You have the Azure resources shown in the following table.

Name	Type	Location
Vnet1	Virtual network	East US
Vnet1\Subnet1	Subnet	East US
Vnet1\GatewaySubnet	Subnet	East US
Vnet2	Virtual network	West US
Vnet2\Subnet1	Subnet	West US
Vnet2\GatewaySubnet	Subnet	West US
WebApp1	Azure App Service web app	East US

WebApp1 uses the Standard pricing tier.

You need to ensure that WebApp1 can access the virtual machines deployed to Vnet1\Subnet1 and Vnet2\Subnet1. The solution must minimize costs.

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

Hot Area:

**Answer Area:**

Vnet1:

- |                      |
|----------------------|
| An additional subnet |
| A peering connection |
| A private endpoint   |
| A VPN gateway        |

Vnet2:

- |                      |
|----------------------|
| An additional subnet |
| A peering connection |
| A private endpoint   |
| A VPN gateway        |

Correct Answer:

**Answer Area:**

Vnet1:

- |                      |
|----------------------|
| An additional subnet |
| A peering connection |
| A private endpoint   |
| A VPN gateway        |

Vnet2:

- |                      |
|----------------------|
| An additional subnet |
| A peering connection |
| A private endpoint   |
| A VPN gateway        |

Box 1: An additional subnet -

Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

Box 2: A VPN gateway -

Gateway-required virtual network integration: When you connect directly to virtual networks in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

Note: If your app is in an App Service Environment, it's already in a virtual network and doesn't require use of the VNet integration feature to reach resources in the same virtual network.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

 **Cristoicach91** Highly Voted 9 months, 3 weeks ago

Answer is correct. You need to create for VNET1 a subnet, because you can do Regional VNET integration since the web app and the VNET1 are in the same region. VNET2 is in a different region so you would need a VPN gate and a P2S ( consider that in VNET2 you already have a GatewaySubnet which doesn't necessarily mean you have a VPN gate created, it just means you created a subnet called GatewaySubnet ).

upvoted 23 times

 **Flacky\_Penguin32** 6 months, 2 weeks ago

not to mention "minimize costs"; peering is free.

upvoted 3 times

 **sapien45** 9 months ago

Thanks Cristoicach91 !

upvoted 2 times

 **leaviu1** Highly Voted 5 months, 1 week ago

Answer given is not correct.

Correct answer: Vnet1 - an additional subnet

Correct answer: Vnet2 - a peering connection

From same attached documentation:

<https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

Using regional virtual network integration enables your app to access:

Resources in the virtual network you're integrated with.

Resources in virtual networks peered to the virtual network your app is integrated with including global peering connections.  
(you could use a gateway if you wanted to connect directly, but it is not a requirement here. Cost is.)

upvoted 10 times

 **aklas** 2 months ago

This is the answer as it says minimizing costs and the public doc says integration allows access to include global peering connections.

upvoted 1 times

 **AzureLearner01** Most Recent 3 months, 2 weeks ago

I think there are multiple right answers to this. After evaluating in my lab i would go for private endpoint. Why? Because it establishes a connection between the PaaS Service WebApp and your VM. Private endpoints are typically less expensive than VPN Gateways, so i would go for it. VNet peering seems also a way but, the App is not in a Vnet and the question is what are you creating in each VNet, so I would go for Private Endpoint. Let me know what you think about this.

upvoted 2 times

 **AzureLearner01** 3 months ago

Correct myself. Private endpoint is only used for incoming traffic to your app. Outgoing traffic won't use this private endpoint. You can inject outgoing traffic to your network in a different subnet through the virtual network integration feature. So i would go for subnet in the same region an VNet peering

upvoted 1 times

 **Skankhut** 4 months, 3 weeks ago

Answer is correct. There is no need to have connectivity between Vnet1 and Vnet2 (might actually not be allowed).. The requirements only states App Service needs connection to Vnet1 and Vnet2

upvoted 1 times

 **MrBlueSky** 2 months ago

It mentions minimizing cost. The most cost effective way to achieve the goal is to use a new subnet (for app integration) + peering  
upvoted 1 times

 **Rajan395** 4 months, 3 weeks ago

exam topic answer seem to be correct

upvoted 1 times

 **TJ001** 5 months ago

because there are 2 VNets involved and now VNET integration supports global peering connections .. I will go with vnet peering for second question..first is correct

upvoted 1 times

✉️ **TJ001** 5 months ago

If it is single VNET scenario where App Service and VNET are in different region then the only option for direct integration is set up VPN gateway and SSTP P2S VPN

upvoted 1 times

✉️ **DerekKey** 5 months, 2 weeks ago

Answer:

An additional subnet -----> Regional virtual network integration: When you connect to virtual networks in ---> the same region <--- , you must have a dedicated subnet in the virtual network you're integrating with.

A VPN gateway -----> Gateway-required virtual network integration: When you connect directly to virtual networks in ---> other regions <--- or to a classic virtual network in the same region, you need an Azure Virtual Network gateway created in the target virtual network.

upvoted 1 times

✉️ **Tightbot** 6 months, 1 week ago

Ans: Additional subnet and Peering connection

Explanation:

Using regional virtual network integration enables your app to access:

1)Resources in the virtual network you're integrated with.

2)Resources in virtual networks peered to the virtual network your app is integrated with including global peering connections.

<https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual-network-integration>

upvoted 3 times

✉️ **Flacky\_Penguin32** 6 months, 2 weeks ago

I feel since these are both connected by the Azure global network and if these are both in the same tenant and owned by the same owner, if you have a vnet in US East and a vnet is US West, then in my mind Answer 1 is 'vnet peering' and Answer 2 is 'vnet peering'.

upvoted 1 times

✉️ **Flacky\_Penguin32** 6 months, 2 weeks ago

having the gateway subnet is irrelevant, its meant to confuse.

upvoted 1 times

✉️ **Flacky\_Penguin32** 6 months, 2 weeks ago

not to mention "minimize costs"; peering is free.

upvoted 1 times

✉️ **jellybiscuit** 8 months, 3 weeks ago

I agree that the first option is an additional subnet for vnet integration.

For the second option, I would personally create a peering (between vnet1 and vnet2)

- it works

- it requires no additional steps

- cost difference is hard to know without knowing the traffic details

VPN: pay for 2 gateways and egress traffic

Peering: pay for ingress/egress traffic

Problems with the VPN choice

- it does not work without also creating a VPN gateway in vnet 1

- Does the existence of gateway subnets imply that I can use them? Or that they are in use? I have no way of knowing.

- Not addressed in the question, but it limits my bandwidth.

upvoted 4 times

✉️ **wooyourdaddy** 3 months, 1 week ago

Think the flaw in the logic is that VNET1 and VNET2 have to have connectivity. App Service plans can't have more than two virtual network integrations per App Service plan. Multiple apps in the same App Service plan can use the same virtual network integration. Currently you can only configure the first integration through Azure portal. The second integration must be created using Azure Resource Manager templates or Azure CLI commands.

The suggested answer assumes you use the VNET integration model to connect to VNET1, and the Gateway required VNET integration model to connect to VNET2. No interconnectivity between VNET1 and VNET2.

The documentation is not clear on if these 2 models can exist together. I would go with peering myself for the 2nd answer.

upvoted 1 times

✉️ **wooyourdaddy** 3 months, 1 week ago

So found some additional information that provides the correct context for this question.

The question states 'WebApp1 uses the Standard pricing tier.' Not sure what it was at the time of the question months ago, but when you create an App Service Plan, only the Windows Operating System option has a Standard pricing tier.

When I create a standard Windows App Service Plan and go to the Networking section under settings and then click on 'Click here to manage', I am brought to the VNET Integration management page where it states:

Regional VNET Integrations 0/2  
Gateway required VNET Integrations 0/5

This confirms that the 2 models can exist together. So the correct answer is an additional subnet in VNET1 and a virtual network gateway in VNET2.

upvoted 2 times

✉️  **Aanandan** 8 months, 2 weeks ago

your right... Same question raised for me... if enabled peering between Vnet-1 and vnet-2 ,it will be less cost and easy to manage the connectivity... But if we used VPN gateway need more configuration for enable the connectivity

upvoted 1 times

✉️  **AdityaGupta** 9 months ago

correct.

upvoted 3 times

✉️  **sapien45** 9 months ago

So helpful, truly appreciate your valuable contributions

upvoted 9 times

HOTSPOT -

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

The screenshot shows the Azure App Service blade for an application named 'as12'. The top navigation bar includes 'Browse', 'Stop', 'Swap', 'Restart', 'Delete', 'Refresh', 'Get publish profile', and a 'JSON View' button. A message box at the top says 'Click here to access our Quickstart guide for deploying code to your app →'. The main content area is titled 'Essentials' and displays the following configuration details:

Resource group (change) RG1	URL <a href="https://as12.azurewebsites.net">https://as12.azurewebsites.net</a>
Status Running	Health Check Not configured
Location North Europe	App Service Plan ASP1 (P1v2:1)
Subscription (change) Visual Studio Premium with MSDN	FTP/deployment user set No FTP/deployment user set
Subscription ID 8372f433-2dcf-4361-b5ef-5b188fed87d0	FTP hostname <a href="ftp://waws-prod-db3-085.ftp.azurewebsites.windows.net...">ftp://waws-prod-db3-085.ftp.azurewebsites.windows.net...</a>
	FTPS hostname <a href="ftps://waws-prod-db3-085.ftp.azurewebsites.windows.net...">ftps://waws-prod-db3-085.ftp.azurewebsites.windows.net...</a>
Tags (change) Click here to add tags	

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

The screenshot shows the VNet Integration blade for the 'as12' application. It features a 'VNet Configuration' section with a link to 'Securely access resources available in or through your Azure VNet. [Learn more](#)'. Below this, there are sections for 'VNet Details', 'VNet Address Space', 'Subnet Details', and 'Subnet Address Space'.

VNet Details	
VNet NAME	Vnet1
LOCATION	North Europe

VNet Address Space	
Start Address	End Address
10.100.0.0	10.100.255.255

Subnet Details	
Subnet NAME	Subnet2

Subnet Address Space	
Start Address	End Address
10.100.2.0	10.100.2.255

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

## Private Endpoint connections

[Add](#) [Refresh](#) | [Approve](#) [Reject](#) [Remove](#)

## Private Endpoint connections

Private access to services hosted on the Azure platform, keeping your data on the Microsoft network [Learn more](#)

Filter by name or description [All connection states](#)

Connection name ↑↓ Connection state ↑↓ Private endpoint ↑↓ Description

No results.

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

Subnet2 can contain only App Service apps in the ASP1 App Service plan

As12 will use an IP address from Subnet2 for network communications

Computers in Vnet1 will connect to a private IP address when they connect to as12

Correct Answer:

### Answer Area

#### Statements

Yes      No

Subnet2 can contain only App Service apps in the ASP1 App Service plan

As12 will use an IP address from Subnet2 for network communications

Computers in Vnet1 will connect to a private IP address when they connect to as12

Box 1: Yes -

The integration subnet can be used by only one App Service plan.

Box 2: No -

No Private Endpoint connections defined.

When regional virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app. However, if your outbound call is to a virtual machine or private endpoint in the integration virtual network or peered virtual network, the outbound address will be an address from the integration subnet.

Box 3: Yes -

Apps in App Service are hosted on worker roles. Regional virtual network integration works by mounting virtual interfaces to the worker roles with addresses in the delegated subnet. Because the from address is in your virtual network, it can access most things in or through your virtual network like a VM in your virtual network would.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

 **zenithcsa1** Highly Voted 9 months, 2 weeks ago

YYN

Y / <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#limitations>

Y / VNet integrated App Service uses IP from dedicated subnet to communicate resources in the VNet. ( vNet integration : outbound / private endpoint : inbound )

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional-virtual-network-integration-works>

N / There's no private endpoint.

upvoted 27 times

 **AdityaGupta** Highly Voted 9 months ago

Correct Answer is: YYN

1) Subnet2 is delegated to ASP.

2) Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network. Private site access refers to making an app accessible only from a private network, such as from within an Azure virtual network. Virtual network integration is used only to make outbound calls from your app into your virtual network.

<https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration#gateway-required-vnet-integration>  
~:text=Virtual%20network%20integration%20gives%20your%20app%20access%20to%20resources%20in,make%20outbound%20calls%20from%20your%20app%20into%20your%20virtual%20network.

3) There is no Private Endpoint configured and again VNET integration only allows outbound network communication, no inbound communication is allowed.

upvoted 14 times

 **khanda** Most Recent 2 months, 1 week ago

YYN are the correct answers. App will use private IP from the vnet-intergration subnet for outbound calls.

upvoted 1 times

 **mrgreat** 2 months, 3 weeks ago

YYN is the correct

upvoted 1 times

 **ruirosamendes** 3 months ago

Y - Subnet2 is delegated to ASP

N - Network communication (IN/OUT). Only Out is possible!

Y - APP goes out, and presents to VMs or ourthes devcs on the network with the "From IP". An IP from the delegated subnet. So VM connects back to the IP in private IP of the subnet

upvoted 1 times

 **AzureLearner01** 3 months, 2 weeks ago

YNN, a Subnet is delegated to an App service plan. without PE it wouldn't use the internal IPs from the VNet.

upvoted 1 times

 **AzureLearner01** 3 months ago

Have to correct myself. YYN

When virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app. However, if your outbound call is to a virtual machine or private endpoint in the integration virtual network or peered virtual network, the outbound address is an address from the integration subnet.

upvoted 1 times

 **Ayokun** 4 months ago

YYN

1,2)Uses ip from the subnet only for outbound connectivity

3 Uses ip from the subnet only for outbound connectivity

upvoted 2 times

 **mm2** 5 months ago

YYN

1) it's one subnet one app sp

2) AP service will use IP from integration vnet for communication but just for outbound connection (and responses back, but traffic have to be initiated by App service)

3) N - because if you need inbound traffic - so clients would like to reach app service first - then you need private endpoint which has not been configured in our example

upvoted 3 times

 **Tightbot** 6 months, 1 week ago

3)Ans: N

Explanation: Private Endpoint is only used for incoming flows to your Web App. Outgoing flows won't use this Private Endpoint. You can inject outgoing flows to your network in a different subnet through the virtual network integration feature.

Since there is no private endpoint configured for the app service, the VMs in the same vnet cannot reach the app service.

So, the correct statement would be; Computers in Vnet1 will connect to a private IP address when they connect to as12 "when there is a private endpoint for the app created on Vnet1"

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

upvoted 2 times

 **kimalto452** 9 months, 2 weeks ago

YNN

The inbound rules don't apply because>>> you can't use virtual network integration to provide inbound access to your app.

upvoted 5 times

✉️  **Cristoicach91** 9 months, 3 weeks ago

YNN. You can have only 1 subnet per APP service plan. You don't have a PE defined. You don't have a PE defined.  
upvoted 1 times

✉️  **Cristoicach91** 9 months, 3 weeks ago

Correction. The Private Endpoint uses an IP from the Subnet and it will be used for an WEB APP service. In the image it doesn't show one configured, because there might not exist a WEB APP service yet, so answer is YYYY.  
upvoted 1 times

✉️  **jellybiscuit** 8 months, 3 weeks ago

You were right the first time. There is no PE configured.  
upvoted 1 times

You have a hub-and-spoke topology. The topology includes multiple on-premises locations that connect to a hub virtual network in Azure via ExpressRoute circuits.

You have an Azure Application Gateway named GW1 that provides a single point of ingress from the internet.

You plan to migrate the hub-and-spoke topology to Azure Virtual WAN.

You need to identify which changes must be applied to the existing topology. The solution must ensure that you maintain a single point of ingress from the internet.

Which three changes should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add user-defined routes.
- B. Add virtual network peerings.
- C. Replace the user-defined routes used by the current topology.
- D. Create virtual network connections.
- E. Remove the existing virtual network peerings.
- F. Redeploy GW1.

**Correct Answer:** CDE

Transition connectivity to virtual WAN hub:

Step 1. (E) Delete the existing peering connections from Spoke virtual networks to the old customer-managed hub. Access to applications in spoke virtual networks is unavailable until steps 1-3 are complete.

Step 2. (D) Connect the spoke virtual networks to the Virtual WAN hub via VNet connections.

Step 3. (C) Remove any user-defined routes (UDR) previously used within spoke virtual networks for spoke-to-spoke communications. This path is now enabled by dynamic routing available within the Virtual WAN hub.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology>

*Community vote distribution*

CDE (100%)

✉️  **AdityaGupta**  9 months ago

**Selected Answer:** CDE

The given answers are correct and in correct sequence.

First you need to remove existing VNET peering (E) then add VNET connections from VWAN Hub to same spoke VNETs (D) and later removed any existing UDRs you defined earlier. (C).

There is no need to replay App Gateway. Since it is VWAN there will be Vnet connection, no VNET peering.

upvoted 9 times

✉️  **AdityaGupta** 9 months ago

There is no new UDRs required as it will be replaced by VWAN Hub Dynamic Routing.

upvoted 3 times

✉️  **flurgen248**  3 months, 4 weeks ago

**Selected Answer:** CDE

The answers are correct. They're specifically listed order on this page: <https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology#step-5-transition-connectivity-to-virtual-wan-hub>

- a. Delete the existing peering connections from Spoke virtual networks to the old customer-managed hub. Access to applications in spoke virtual networks is unavailable until steps a-c are complete.
- b. Connect the spoke virtual networks to the Virtual WAN hub via VNet connections.
- c. Remove any user-defined routes (UDR) previously used within spoke virtual networks for spoke-to-spoke communications. This path is now enabled by dynamic routing available within the Virtual WAN hub.

upvoted 4 times

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: A**

Azure Application Gateway is limited to 100 active listeners that are routing traffic. Active listeners = total number of listeners - listeners not active.

If a default configuration inside a routing rule is set to route traffic (for example, it has a listener, a backend pool, and HTTP settings) then that also counts as a listener.

Note: Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. This type of routing is known as application layer (OSI layer 7) load balancing.

Incorrect:

Not B: Floating IP. Some application scenarios prefer or require the same port to be used by multiple application instances on a single VM in the backend pool.

Common examples of port reuse include:

clustering for high availability

network virtual appliances

exposing multiple TLS endpoints without re-encryption.

Not D: Multiple site hosting enables you to configure more than one web application on the same port of application gateways using public-facing listeners. It allows you to configure a more efficient topology for your deployments by adding up to 100+ websites to one application gateway. Each website can be directed to its own backend pool.

Reference:

<https://github.com/MicrosoftDocs/azure-docs/blob/main/includes/application-gateway-limits.md>

*Community vote distribution*

C (100%)

✉️  **Cristoicach91** Highly Voted 9 months, 3 weeks ago

**Selected Answer: C**

C. Azure Standard Load Balancer that has high availability (HA) ports enabled

App1 is installed on 10 VMs which can be put in a Backend pool. The req is to minimize the number of load balancing rules. If you select HA it will allow you to have 1 rule for TCP and UDP ports, if you don't select HA you will need to have a minimum of 2 rules for TCP and UDP with a \* range.

upvoted 15 times

✉️  **sshera** Highly Voted 5 months, 2 weeks ago

In exam 04Jan23

upvoted 7 times

✉️  **vigklk** 1 month ago

what was the anwser?

upvoted 1 times

✉️  **Ben\_88** Most Recent 1 week, 2 days ago

**Selected Answer: C**

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

Load balance a large number of ports

You can also use HA ports for applications that require load balancing of large numbers of ports. You can simplify these scenarios by using an internal standard load balancer with HA ports. A single load-balancing rule replaces multiple individual load-balancing rules, one for each port.

upvoted 1 times

✉️  **Oklama** 4 weeks ago

**Selected Answer: C**

C is correct  
upvoted 1 times

 **tomtom2022** 1 month, 3 weeks ago

**Selected Answer: C**

C is correct  
upvoted 1 times

 **mrgreat** 2 months, 3 weeks ago

C is correct  
When you enable high availability (HA) ports on the load balancer, it creates a single rule for all the ports of the virtual machines in the back-end pool.  
upvoted 1 times

 **jellybiscuit** 8 months, 3 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview>  
upvoted 1 times

 **sapien45** 8 months, 4 weeks ago

**Selected Answer: C**

Load balance a large number of ports  
You can also use HA ports for applications that require load balancing of large numbers of ports. You can simplify these scenarios by using an internal standard load balancer with HA ports. A single load-balancing rule replaces multiple individual load-balancing rules, one for each port.  
<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-ha-ports-overview>  
upvoted 2 times

 **AdityaGupta** 9 months ago

**Selected Answer: C**

Here the requirement is on TCP and UDP ports, not HTTP or HTTPS, hence application gateway is ruled out.

Incorrect Answer B: Some application scenarios prefer or require the same port to be used by multiple application instances on a single VM in the backend pool. Common examples of port reuse include:

clustering for high availability  
network virtual appliances  
exposing multiple TLS endpoints without re-encryption.

If you want to reuse the backend port across multiple rules, you must enable Floating IP in the rule definition.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-floating-ip>

Correct Answer is C: - The HA ports load-balancing rules are configured when you set the front-end and back-end ports to 0 and the protocol to All. The internal load balancer resource then balances all TCP and UDP flows, regardless of port number

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

upvoted 6 times

 **Alessandro365** 9 months ago

**Selected Answer: C**

C is correct  
upvoted 1 times

 **Alessandro365** 9 months ago

**Selected Answer: C**

C is correct  
upvoted 2 times

 **Sayden** 9 months, 2 weeks ago

C. <https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq>. UDP is layer 4. Application gateway is layer 7.  
upvoted 1 times

 **zenithcsa1** 9 months, 2 weeks ago

**Selected Answer: C**

Application gateway does not support UDP protocol.  
In order to minimize the number of load-balancing rules, HA ports load-balancing rule should be used.  
upvoted 4 times

**DRAG DROP -**

You register a DNS domain with a third-party registrar.

You need to host the DNS zone on Azure.

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

Select and Place:

**Actions**

Identify the FQDNs of the name servers.

Create a public DNS zone.

Identify the IP addresses of the name servers.

Modify the SOA records for the domain.

Modify the NS records for the domain.

**Answer Area****Correct Answer:****Actions**

Identify the IP addresses of the name servers.

Modify the SOA records for the domain.

**Answer Area**

Step 1: Create a public DNS zone.

Create a DNS zone -

1. Go to the Azure portal to create a DNS zone. Search for and select DNS zones.

2. Select Create DNS zone.

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

Step 2: Identify the FQDNs of the name servers.

Retrieve name servers.

Before you can delegate your DNS zone to Azure DNS, you need to know the name servers for your zone. Azure DNS gives name servers from a pool each time a zone is created.

With the DNS zone created, in the Azure portal Favorites pane, select All resources. On the All resources page, select your DNS zone. If the subscription you've selected already has several resources in it, you can enter your domain name in the Filter by name box to easily access the application gateway.

Retrieve the name servers from the DNS zone page. In this example, the zone contoso.net has been assigned name servers ns1-01.azure-dns.com, ns2-

01.azure-dns.net, \*ns3-01.azure-dns.org, and ns4-01.azure-dns.info:



Search (Ctrl+I)

Record set Move Delete zone Refresh

Resource group (change)

contosorg

Subscription (change)

Microsoft Azure Internal Consumption

Subscription ID

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Name server 1  
ns1-08.azure-dns.com.  
Name server 2  
ns2-08.azure-dns.net.  
Name server 3  
ns3-08.azure-dns.org.  
Name server 4  
ns4-08.azure-dns.info.

Tags (change)

Click here to add tags

## SETTINGS

Properties

Locks

Automation script

## MONITORING

Metrics (Preview)

Alerts

## SUPPORT + TROUBLESHOOTING

New support request

Search record sets

NAME	TYPE	TTL	VALUE
@	NS	172800	ns1-08.azure-dns.com. ns2-08.azure-dns.net. ns3-08.azure-dns.org. ns4-08.azure-dns.info.
@	SOA	3600	Email: azuredns-hostmaster.microsoft.com Host: ns1-08.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1

Azure DNS automatically creates authoritative NS records in your zone for the assigned name servers.

Step 3: Modify the NS records for the domain.

## Delegate the domain -

Once the DNS zone gets created and you have the name servers, you'll need to update the parent domain with the Azure DNS name servers.

Each registrar has its own DNS management tools to change the name server records for a domain.

- In the registrar's DNS management page, edit the NS records and replace the NS records with the Azure DNS name servers.
- When you delegate a domain to Azure DNS, you must use the name servers that Azure DNS provides. Use all four name servers, regardless of the name of your domain. Domain delegation doesn't require a name server to use the same top-level domain as your domain.

Reference:

<https://docs.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

omgMerrick 3 months, 3 weeks ago

The answer is correct.

Source:

<https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

upvoted 3 times

Rajan395 4 months, 3 weeks ago

correct answers

upvoted 1 times

TJ001 5 months ago

correct answers

upvoted 1 times

Jawad1462 8 months, 3 weeks ago

Correct

upvoted 1 times

[Removed] 9 months ago

Correct..

upvoted 1 times

AdityaGupta 9 months ago

Correct : - <https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns>

upvoted 4 times

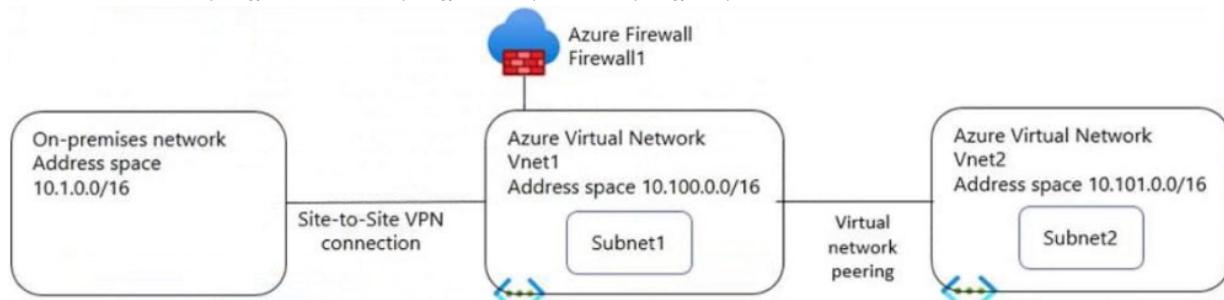
 **Cristoicach91** 9 months, 3 weeks ago

correct

upvoted 2 times

HOTSPOT -

You have the network topology shown in the Topology exhibit. (Click the Topology tab.)



You have the Azure firewall shown in the Firewall1 exhibit. (Click the Firewall1 tab.)

All services > Firewalls >

**Firewall1** ✎ ...

Firewall

» [Delete](#) [Lock](#)

[Visit Azure Firewall Manager to configure and manage this firewall.](#) →

[JSON View](#)

**Essentials**

Resource group (change) RG2	Firewall sku Standard
Location North Europe	Firewall subnet AzureFirewallSubnet
Subscription (change) Visual Studio Premium with MSDN	Firewall public IP Firewall1-IP1
Subscription ID 8372f433-2dcd-4361-b5ef-5b188fed87d0	Firewall private IP 10.100.253.4
Virtual network Vnet1	Management subnet -
Firewall policy FirewallPolicy	Management public IP -
Provisioning state Succeeded	Private IP Ranges Managed by Firewall Policy
Tags (change) <a href="#">Click here to add tags</a>	

You have the route table shown in the RouteTable1 exhibit. (Click the RouteTable1 tab.)

**RouteTable1**

Route table

Move Delete Refresh Give feedback

Essentials

Resource group (change) RG1 Associations 1 subnet associations

Location North Europe

Subscription (change) Visual Studio Premium with MSDN

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

Tags (change) Click here to add tags

Routes

Search routes					
Name	Address prefix	Next hop type	Next hop IP address		
Route1	10.1.0.0/16	Virtual network gateway	-	***	
Route2	0.0.0.0/0	Virtual appliance	10.100.253.4	***	

Subnets

Search subnets					
Name	Address range	Virtual network	Security group		
Subnet1	10.100.1.0/24	Vnet1	-	***	

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 Subnet1 can connect to the internet through Firewall1.	<input type="radio"/>	<input type="radio"/>
The resources in Subnet1 can connect to the resources in Vnet2.	<input type="radio"/>	<input type="radio"/>
The resources in Subnet2 can connect to the internet through Firewall1.	<input type="radio"/>	<input type="radio"/>

**Correct Answer:**

**Answer Area**

Statements	Yes	No
The resources in Subnet1 can connect to the internet through Firewall1.	<input checked="" type="radio"/>	<input type="radio"/>
The resources in Subnet1 can connect to the resources in Vnet2.	<input checked="" type="radio"/>	<input type="radio"/>
The resources in Subnet2 can connect to the internet through Firewall1.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

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

Box 2: Yes -

Yes, with network network peering.

Box 3: No -

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

Reference:

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

✉ **Sheriboy** [Highly Voted] 9 months, 2 weeks ago

Answer seems correct,  
Y - it will go through VA which is firewall  
Y - there is a peering, so subnet and subnet2 can communicate  
N - there is no route for subnet 2 through VA/firewall  
upvoted 14 times

✉ **AdityaGupta** 9 months ago

Look at the exhibits again, the route table is associated to only subnet1 and not to subnet2.

Even though there is peering enabled, since route table is not associated with subnet2, it can't connect to Internet using Route Table.

It is worth noting that there is no mention of gateway transit in VNET peering, as explained in given answers "gateway transit for virtual network peering has not been configured."

Routes to the gateway-connected virtual networks or on-premises networks will propagate to the routing tables for the peered virtual networks using gateway transit. You can disable the automatic route propagation from the VPN gateway. Create a routing table with the "Disable BGP route propagation" option, and associate the routing table to the subnets to prevent the route distribution to those subnets.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit#:~:text=Routes%20to%20the,to%20those%20subnets>.

upvoted 2 times

✉ **charlesr1700** [Highly Voted] 9 months ago

I would say correct:  
Y: Traffic will flow through the FW because of the 0.0.0.0/0 rule  
Y: Traffic will flow through the FW then onto vNet 2 through the peer.  
N: No route for subnet 2 through the FW so it will use Azure default to connect to the web  
upvoted 8 times

✉ **Qunlay** [Most Recent] 1 month, 3 weeks ago

Transit gateway or remote gateway must be enable for resources in Vnet1 to talk to Vnet2. Therefore Subnet1 and subnet2 cannot communicate.  
Answer is Y,N,N  
upvoted 2 times

✉ **Qunlay** 1 month, 3 weeks ago

Correct answer is Y,N,N  
upvoted 2 times

✉ **\_fvt** 2 months, 2 weeks ago

I would have put YYN.  
Y - the firewall has a public IP and Route Table applied to Subnet 1 is correct and making traffic to internet go through FW.  
Y - But maybe with asymmetric routing ? User-Defined routes takes precedence over Default routes (<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>), so the traffic from Subnet 1 to Subnet 2 will go through Firewall, then through the peering to Subnet 2. Subnet 2 however don't have UDR assigned so then answer will go through default route, not the Firewall. If the traffic was initiated from Subnet 2 the answer from Subnet 1 to Subnet 2 will go through azure FW and likely be dropped as no first packet (SYN) was found (not gone through FW from Subnet 2 to 1). So communication from Subnet 1 to Sunbet 2 => YES, but from Subnet 2 to Subnet 1 would have not been possible.  
N - Not UDR applied to Subnet 2 so it will use default routes and not go through Firewall.  
upvoted 1 times

✉ **Accounts** 2 months, 3 weeks ago

YNN  
Y- Will go throuth FW - 0.0.0.0 rout  
N- subnet2 doesnt have RT  
N- No route through FW  
upvoted 3 times

✉ **Rajan395** 4 months, 3 weeks ago

Answers seems to be correct  
upvoted 1 times

✉ **TJ001** 5 months ago

YYN  
Second yes, because peering route take precedence over UDR  
upvoted 1 times

✉ **DerekKey** 5 months, 1 week ago

YYN  
Second YES - explanation

Traffic between directly peered VNets is routed directly even if a UDR points to Azure Firewall as the default gateway. To send subnet-to-subnet traffic to the firewall in this scenario, a UDR must contain the target subnet network prefix explicitly on both subnets.

upvoted 1 times

 **zukako** 5 months, 2 weeks ago

Y

Y

N- explanation is wrong. The reason is udr is not attached to subnet2

upvoted 1 times

 **sapien45** 8 months, 4 weeks ago

YNN

Route for 0.0.0.0/0 would direct any flow going to VNET2 to go through the Firewall, and therefore going nowhere.

There are no routes for peering VNET1-VNET2

upvoted 6 times

 **sapien45** 8 months, 2 weeks ago

YYN. I stand corrected.

The screenshot just shows the detail on ONE route table.

the resulting routes in EFFECTIVE routes is not shown there, since the two VNETS are peered, VNET peering CIDR range takes priority

upvoted 5 times

 **Cristoicach91** 9 months, 3 weeks ago

YNN. The default for subnet one is NH to FW NVA. The effective routes doesn't show that you are aware of the VNET2 address space ( no route ).  
There is no Subnet2 associated to the RT1.

upvoted 2 times

 **zenithcsa1** 9 months, 2 weeks ago

There's peering between Vnet1 and Vnet2. Effective routes can be seen in Network Interface menu, not Route Table.

upvoted 2 times

 **[Removed]** 9 months ago

Peering is there just to connect. If no route configured, will use system route but here in subnet 1, there is route, says 0.0.0.0/0 to NVA...  
traffic will go via FW only. answer is YNN

upvoted 1 times

 **hom3sick** 8 months, 4 weeks ago

YYN

The question is asking if Subnet1 can connect to the resources in Vnet2, not about how it is connecting to Vnet2.

So yes, Subnet1 can connect to Vnet2 via Firewall1

upvoted 3 times

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 resize the gateway of Vnet1 to a larger SKU.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

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

Reference:

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

*Community vote distribution*

B (100%)

 **Stevy\_nash** 5 months ago

"You resize the gateway of Vnet1 to a larger SKU"

Bro why whould u do that ? are u okay ?

upvoted 4 times

 **AdityaGupta** 9 months ago

You need to download VPN client again, since there are topology changes.

upvoted 2 times

 **jilguens** 9 months, 2 weeks ago

**Selected Answer: B**

correct

upvoted 2 times

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

Name	In resource group	Location
Vnet1	RG1	West US
Vnet2	RG1	Central US
Vnet3	RG2	Central US
Vnet4	RG2	West US
Vnet5	RG3	East US

You plan to deploy an Azure firewall named AF1 to RG1 in the West US Azure region.

To which virtual networks can you deploy AF1?

- A. Vnet1 and Vnet4 only
- B. Vnet1, Vnet2, Vnet3, and Vnet4
- C. Vnet1 only
- D. Vnet1 and Vnet2 only
- E. Vnet1, Vnet2, and Vnet4 only

**Correct Answer: C**

Azure Firewall operates in a single VNET.

Azure Firewall is a regional service.

Yes. Vnet1: Same VNET and same region.

No. Vnet2: Same Resource Group but different VNET and different region. Must be in the same region.

No. Vnet3: Different VNET, different region. Must be in the same region.

No. Vnet4: Different VNET, same region.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-framework-azure-firewall>

*Community vote distribution*

C (88%) 12%

✉ **jellybiscuit** Highly Voted 8 months, 2 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>  
upvoted 18 times

✉ **IvanMtz** Highly Voted 8 months, 3 weeks ago

**Selected Answer: C**

The answer correct is C. I created a Lab with specification and i tried to select the vnet in rg2 when i received the message "Azure firewall cannot be used with a from a different resource group". The lab was created from Azure Portal.  
upvoted 15 times

✉ **Ben\_88** Most Recent 1 week, 2 days ago

**Selected Answer: C**

Firewall and VNET must be from the same RG  
<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>  
upvoted 1 times

✉ **xamkiller** 1 month, 2 weeks ago

**Selected Answer: C**

Azure firewall cannot be used with a from a different resource group  
upvoted 2 times

✉ **somenick** 3 months, 1 week ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>  
upvoted 3 times

✉ **Rajan395** 4 months, 3 weeks ago

Correct Answer : C

upvoted 2 times

✉ **TJ001** 5 months ago

>VNET, PIP, FW all in same region and resource group  
>Firewall subnet should be names AzureFirewallSubnet

upvoted 3 times

✉ **Akodo\_Shado** 5 months, 1 week ago

**Selected Answer: C**

The firewall, VNet, and the public IP address all must be in the same resource group.

upvoted 3 times

✉ **sshera** 5 months, 2 weeks ago

In exam 04jan23

upvoted 3 times

✉ **abdulmoiz** 6 months, 1 week ago

Should be only Vnet with RG-1

upvoted 1 times

✉ **Takloy** 6 months, 2 weeks ago

Are there any firewall resource group restrictions? Yes. The firewall, VNet, and the public IP address all must be in the same resource group.

So, answer here is just VNET 1.

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>

upvoted 3 times

✉ **Andre369** 6 months, 2 weeks ago

**Selected Answer: C**

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>

upvoted 1 times

✉ **Azuriste** 8 months, 3 weeks ago

Correct

upvoted 1 times

✉ **JerT** 8 months, 3 weeks ago

The firewall, VNet, and the public IP address all must be in the same resource group.

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

upvoted 3 times

✉ **BlackZeros** 8 months, 3 weeks ago

**Selected Answer: C**

vnet 1 only

upvoted 1 times

✉ **MII1975** 8 months, 3 weeks ago

**Selected Answer: C**

We are talking about deployment only. Once deployed how you configure it is another question.

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#are-there-any-firewall-resource-group-restrictions>

upvoted 1 times

✉ **Pradh** 8 months, 3 weeks ago

VNET-1 ONLY !!!!!!! is the right answer . If Azure Firewall is in RG1 , thn it can be associated with VNET's residing in RG1 only . And also VNETs should be allocated with the same location as Firewalls

upvoted 2 times

**HOTSPOT**

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

Name	Web app URLs
As1.contoso.com	<a href="https://app1.contoso.com/">https://app1.contoso.com/</a> <a href="https://app2.contoso.com/">https://app2.contoso.com/</a>
As2.contoso.com	<a href="https://app3.contoso.com/">https://app3.contoso.com/</a> <a href="https://app4.contoso.com/">https://app4.contoso.com/</a>

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 Area**

Listeners:

0
1
2
3
4

Correct Answer:

Routing rules:

0
1
2
3
4

✉️  **TJ001** Highly Voted  5 months ago

Answer seems correct

- 1) 1 Multi site Listener mapping each backend app service (total 2)
  - 2) 1 routing rule mapping per listener/backend pool with Multi site option (total 2)
- upvoted 10 times

✉️  **JohnAvlakiotis** 3 weeks, 6 days ago

I also went to the portal to deploy it, and there seems to be the only way to do that. Even if the listener is a wildcard listener you will not be able to split it to 2 different back end pools from the same listener IMHO

upvoted 1 times

✉️  **TJ001** 5 months ago

pls note if the no of site per app Service is 1 in that case also total no of routing rule will be 2. because the front end listeners are different and it is scenario of creating Basic site listener still requiring rule mapping per listener

upvoted 1 times

✉️  **TJ001** 5 months ago

small correction...in this case as well ...Multi site listener will be created and there is a sub option ... single site/multiple site within the Multi site selection..so both the case Multi site listener is created but there could be 1 or more sites within that selection

upvoted 1 times

✉️  **WMG** Most Recent  2 months ago

Answer is wrong, created this setup in our lab environment. Read: <https://learn.microsoft.com/en-us/azure/application-gateway/multiple-site-overview#wildcard-host-names-in-listener>

upvoted 1 times

✉️  **Zeppoonstream** 2 months ago

what is meant by "You deploy an Azure 2" ??

upvoted 4 times

✉️  **henryhung** 2 months, 1 week ago

From ChatGPT Plus(GPT-4)

You can use a multi-site listener to consolidate your configuration. A multi-site listener allows you to host multiple web apps on a single application gateway, routing requests based on the host header. In this case, you can create just one multi-site listener and configure the necessary routing rules.

Listener:

Create a single multi-site listener with the wildcard hostname configuration:

Multi-site Listener: Hostname: \*.contoso.com

Routing rules:

Create 4 routing rules to route requests to the respective backend pools based on the host header:

Rule 1: Hostname: app1.contoso.com -> Backend pool (as1.contoso.com)

Rule 2: Hostname: app2.contoso.com -> Backend pool (as1.contoso.com)

Rule 3: Hostname: app3.contoso.com -> Backend pool (as2.contoso.com)

Rule 4: Hostname: app4.contoso.com -> Backend pool (as2.contoso.com)

By using a multi-site listener, you can minimize the number of listeners you need to configure:

1 multi-site listener

4 routing rules

upvoted 1 times

✉️  **MrBlueSky** 2 months ago

You posting these ChatGPT answers is not helpful dude.

upvoted 9 times

✉️  **drprepper\_** 3 months, 2 weeks ago

You only need 1 multi-site listener I think? <https://learn.microsoft.com/en-us/azure/application-gateway/multiple-site-overview#wildcard-host-names-in-listener> You can wildcard the start of the FQDN then just two routing rule 1 for each pool? So 1 and 2?

upvoted 4 times

✉️  **wooyourdaddy** 3 months, 1 week ago

I agree that it is 1 multi-site listener using either wildcard or up to 5 hostnames as per the link you cited. Then it would be a routing rule for each backend, so 2 in total.

upvoted 2 times

✉️  **flurgen248** 3 months, 4 weeks ago

Answer is correct: <https://learn.microsoft.com/en-us/azure/application-gateway/application-gateway-components#types-of-listeners>

Create a multi-site listener for each Azure App Service, and each listener needs one rule.

upvoted 1 times

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**

*Community vote distribution*

C (100%)

 **Goofer**  5 months, 1 week ago

Answer C

The VPN gateway is not the problem, Branch2, 3, 4 are still working

Reset the connection

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

upvoted 11 times

 **Oklama**  3 weeks, 6 days ago

**Selected Answer: C**

The Correct answer is C

upvoted 1 times

 **sunsetblvdfightclub** 3 months, 1 week ago

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

upvoted 1 times

 **Rajan395** 4 months, 3 weeks ago

C is correct

upvoted 1 times

 **DerekKey** 5 months, 1 week ago

Answer D

Problem: After you configure a site-to-site VPN connection between an on-premises network and an Azure virtual network, the VPN connection suddenly stops working and cannot be reconnected.

Solution: To resolve the problem, >>first try to reset the Azure VPN gateway<< and reset the tunnel from the on-premises VPN device.

upvoted 1 times

 **fz2021** 5 months, 1 week ago

GW1 is common for multiple connections and it shall incresaee the downtime  
upvoted 2 times

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

Answer Area
<p><b>Correct Answer:</b> Vnet1: A private endpoint</p> <p>Vnet2: A peering link</p>

**Wis10** Highly Voted 5 months, 1 week ago

Correct Answer:

- Vnet1 = Standard Load Balancer
- Vnet2 = Private Endpoint

Justification:

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

upvoted 21 times

**DavidSapery** Highly Voted 5 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview> indicates that a Load Balancer is needed on the SQL side (vnet1) and a Private Endpoint on the VM side (vnet2).

upvoted 16 times

**AzureLearner01** Most Recent 3 months, 2 weeks ago

To establish the private link service you need a load balancer in VNet 1 and for sure the private link service resource. In the partner company tenant you need an private endpoint that connects to this private link service. To answer the question correctly we might answer to create standard load balancer and private link service in vnet1 an pe in vnet2.

upvoted 3 times

✉ Ayokun 3 months, 3 weeks ago

Load balancer  
Private Link  
<https://learn.microsoft.com/it-it/azure/private-link/private-link-overview>  
upvoted 1 times

✉ Ayokun 3 months, 3 weeks ago

Sorry i correct "You need to provide VM1 with access to SQL1 by using an Azure Private Link service" hence it is required the last part of the config which is a private endpoint on VM1  
LB  
Private Endpoint  
upvoted 1 times

✉ tester2023 4 months, 3 weeks ago

VNET1: Peering Link  
VNET2: Peering Link

The question notes a Private Endpoint is already configured on the SQL Server (PaaS) resource. As such, vNet peering will allow the VM on vNet 2 to reach the database on vNet 1.

A private endpoint is part of the Private Link Service (<https://learn.microsoft.com/en-us/azure/private-link/private-link-faq#what-is-azure-private-endpoint-and-azure-private-link-service->)

For those selecting Load Balancer, you are correct it requires a Private Link Service (PLS), but that isn't one of the available answers. Also, a PLS requires a VM or VM Scale Set Load Balancer backend pool (see <https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview>). Testing revealed I couldn't use the private IP address of the SQL PaaS server private endpoint for the PLS.

upvoted 2 times

✉ flurgen248 3 months, 3 weeks ago

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

A private link service requires a load balancer.  
VNET1: Load Balancer  
VNET2: Private Endpoint

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

upvoted 3 times

✉ lingxian 3 months, 1 week ago

I would agree with this. How to use an LB with the Azure SQL database as a backend? We have already the private endpoint in VNet1, setting up peering should be enough for VMs in VNet2 talking to the SQL service.

upvoted 1 times

✉ 4729 4 months, 3 weeks ago

VNET1: Private Link  
VNET2: Private Endpoint  
upvoted 3 times

✉ amt2022 5 months ago

Correct answer  
- VNET1 = Standard LB  
- VNET2 = Private EndPoint  
Check this sample from MS.  
<https://learn.microsoft.com/en-us/azure/private-link/create-private-link-service-powershell>  
upvoted 7 times

✉ DerekKey 5 months, 1 week ago

VNet 1: Load Balancer  
VNet 2: Private Endpoint  
Microsoft docs: <https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview>  
upvoted 5 times

✉ chatlisi 5 months, 1 week ago

VNET1 - Azure Load Balancer - your existing service must be behind a load balancer  
VNET2 - Private link  
upvoted 1 times

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

Name	Type	Description
Vnet1	Virtual network	<i>None</i>
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: B**

*Community vote distribution*

C (56%)

B (41%)

✉  **amt2022**  5 months ago

Correct Answer : 4

1. GatewaySubnet
2. Subnet 2
3. Subnet 1 with Basic SKU for Public IP
4. NAT Gateway requires in VNET 1 and hence 4. Otherwise you could have used Subnet2 to avoid creating 4th Subnet. Requirement is to create NAT GW in VNET1 so you need 4th Subnet.

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

Check out - NAT gateway and basic SKU resources section

upvoted 12 times

✉  **MrBlueSky** 2 months, 2 weeks ago

Why could you not just deploy the NAT Gateway into the GatewaySubnet?

upvoted 1 times

✉  **JohnnyChimp0** 1 week, 5 days ago

GatewaySubnet has nothing to do with NAT Gateway resources. GatewaySubnet is the azure naming convention for subnet used with Virtual Network Gateways

upvoted 1 times

✉  **jarz** 1 month, 4 weeks ago

according to this page <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview> NAT GW cannot be deployed into a GW Subnet.

upvoted 2 times

✉  **tester2023** 4 months, 3 weeks ago

Another reason this makes sense is the requirement for the two VMs to continue using their own Public IPs instead of the NAT Gateway. As soon as a NAT Gateway is associated with a vNet, it overrides the instance-level IPs (see <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#connect-to-the-internet-with-nat-gateway> ).

upvoted 3 times

👤 **MrBlueSky** 2 months, 2 weeks ago

Wrong. It only applies to within the same subnet.

So if you use the GatewaySubnet to deploy the NAT Gateway (I don't see why you wouldn't), then the answer is 3.

upvoted 1 times

👤 **MrBlueSky** 2 months ago

Correction: NATGateway cannot be associated to GatewaySubnet

However, NATGateway doesn't need its own subnet and is instead associated to subnets.

Answer is still 3

upvoted 1 times

👤 **jarz** 1 month, 4 weeks ago

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

The order of operations for outbound connectivity follows this order of precedence: Virtual appliance UDR / ExpressRoute >> NAT gateway >> Instance-level public IP addresses on virtual machines >> Load balancer outbound rules >> default system

upvoted 2 times

👤 **wooyourdaddy** Highly Voted 3 months, 1 week ago

Selected Answer: C

The correct answer is 4.

1. The Gateway Subnet must exist on its own.

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

Basic resources, such as basic load balancer or basic public IPs aren't compatible with Virtual Network NAT. Basic resources must be placed on a subnet not associated to a NAT gateway.

3. The question also states that VM1 and VM2 will access the internet by using their respective public IP address. From the same link above we have the statement:

NAT gateway takes precedence over other outbound scenarios (including Load balancer and instance-level public IP addresses) and replaces the default Internet destination of a subnet.

So to meet that requirement, we would need a 4th subnet where the NAT gateway is deployed.

upvoted 10 times

👤 **\_NoobMaster69** 3 months ago

Agree +1

upvoted 1 times

👤 **Zika69** Most Recent 1 week, 2 days ago

Selected Answer: B

Question is asking only to deploy. You can deploy to vnet and not associate with any subnet. So there is no need to create any new subnet.

upvoted 1 times

👤 **roshingr** 2 weeks ago

C. 4

Here's an explanation:

GatewaySubnet: This subnet is required to host the NAT gateway (Gateway1). It is dedicated to the NAT gateway and its associated resources.

Subnet1: This subnet is needed for VM1 to connect to Vnet1. It allows VM1 to access the internet using its public IP address.

Subnet2: This subnet is required for VM2 to connect to Vnet1. It enables VM2 to access the internet using its public IP address.

Subnet3: This subnet is necessary for internal resources or other virtual machines that do not require direct internet access. It allows for segmentation and organization within the virtual network.

Therefore, with these four subnets (GatewaySubnet, Subnet1, Subnet2, Subnet3), you can deploy Gateway1 to Vnet1 while ensuring that VM1 and VM2 can access the internet via their public IP addresses, and also minimizing administrative effort.

upvoted 1 times

👤 **Kipper\_2022** 1 month ago

Selected Answer: C

Agree with amt2022

upvoted 1 times

👤 **xamkiller** 1 month, 2 weeks ago

Selected Answer: C

NAT gateway takes precedence over public IP if it was attached to a subnet 1 or subnet 2, so an additional subnet is required. In total four subnets are required.

upvoted 2 times

👤 **hal01** 1 month, 3 weeks ago

**Selected Answer: C**

4 subnets

upvoted 1 times

 **ckyap** 2 months, 1 week ago

Tested in lab, the condition for VM2 to use its own public ip address can still be achieved if I disassociate the Standard SKU public IP address, then go to NATGateway, change the outbound IP to that public ip address. In this way, we dont need the fourth Subnet. However the question said Administrative effort must be minimized, so I supposed creating a new subnet will be effortless. Subnet 1 cannot be added because of the Basic SKU public IP address. GatewaySubnet cannot be selected in the Subnet association. Thus the answer should be 4.

upvoted 1 times

 **\_fvt** 2 months, 2 weeks ago

**Selected Answer: B**

You have Subnet 1 with VM1 and Subnet 2 with VM2.

You want to deploy a NAT Gateway which will not interact/handle the traffic of VM1 and VM2, so Subnet 1 and Subnet 2.

=> Just create a 3rd Subnet and deploy a Zonal gateway to this Subnet 3 (<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones>)

upvoted 1 times

 **TAJAN** 2 months, 3 weeks ago

**Selected Answer: B**

B is the answer. Nat gateway does not deploy in vNet, it can be associated with subnets in a vnet.

upvoted 2 times

 **mrgreat** 2 months, 3 weeks ago

B. 3

To deploy a NAT gateway in a virtual network, you must have at least three subnets in the virtual network:

GatewaySubnet: This subnet is used by the NAT gateway to perform network address translation. The size of the subnet must be /27 or larger.

VMSubnet1: This subnet contains VM1, which needs to access the internet using its public IP address.

VMSubnet2: This subnet contains VM2, which needs to access the internet using its public IP address.

Therefore, the minimum number of subnets required on Vnet1 is 3.

Option A (2 subnets) is incorrect because it does not meet the minimum requirement for deploying a NAT gateway.

Option C (4 subnets) and Option D (5 subnets) are incorrect as they are more than the minimum number of subnets required for deploying a NAT gateway.

upvoted 2 times

 **AzureLearner01** 3 months ago

My answer would be 3 or 4, depending on the scenario and what Microsoft understands with least administrative effort. Scenario 1 The requirement is, that both VM need to use their own public ip. So those two subnets are not available in this case. Counter = 2 Subnets. The Gateway Subnet should only be for VPN Gateways and you cant bind the Subnet to the NAT Gateway. Counter = 3 Subnets. So we would need another Subnet where we can bind the NAT Gateway. So it would be 4.

Scenario 2

We migrate the public standard ip from VM2 to NAT Gateway and associate the NAT Gateway to Subnet 2. VM2 would use this IP Address but its associated with the gateway. VM1 is not affected from this and would use its own public ip. Migrating steps are very easy only disassociate ip from vm and associate it to the NAT Gateway. Connect NAT Gateway to Subnet 2. In this case we would need 3 subnets. For me this scenario would make a little bit more sense, because why would we deploy a NAT Gateway if we don't use it? All in all this question is very confusing.

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

upvoted 1 times

 **samir111** 3 months, 3 weeks ago

**Selected Answer: B**

Correct Answer: B

upvoted 2 times

 **flurgen248** 3 months, 3 weeks ago

**Selected Answer: B**

Correct Answer: 3

Since VM1 has a Basic IP address, it can't interact with a NAT Gateway.

That alone gives you two subnets.

A NAT gateway resource can be associated to a subnet and can be used by all compute resources in that subnet.

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

That means that a NAT gateway can be deployed in the same subnet as a VM, so you can put it in Subnet 2 with VM2.

Gateway Subnet

Subnet1

Subnet2

upvoted 3 times

 **flurgen248** 1 month, 3 weeks ago

I was wrong. It's 4.

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview#outbound-connectivity>  
"NAT gateway takes precedence over other outbound scenarios (including Load balancer and instance-level public IP addresses)"

So associating the NAT gateway with Subnet 2 would prevent VM2 from connecting using its own IP, and the prompt specifically says VM2 must use its own IP.

upvoted 2 times

 **Kasurot** 3 months, 3 weeks ago

The question states that you must deploy it to Vnet1, so this is not an option.

upvoted 1 times

 **Kasurot** 3 months, 3 weeks ago

Disregard this comment, it does not state that subnet2 is in a different vnet.

upvoted 2 times

 **flurgen248** 3 months, 3 weeks ago

Plus, putting the NAT Gateway in the same subnet as VM2 would also minimize administrative overhead, which is also listed as a requirement.

upvoted 2 times

 **Studies** 4 months ago

**Selected Answer: B**

To deploy Azure Virtual Network NAT gateway named Gateway1 to Vnet1 while meeting the given requirements, the minimum number of subnets required on Vnet1 is three.

The three subnets required are:

Subnet1: This subnet will be used to host VM1, which has a basic SKU public IP address.

Subnet2: This subnet will be used to host VM2, which has a standard SKU public IP address.

GatewaySubnet: This subnet will be used to host the Azure Virtual Network NAT gateway named Gateway1.

By creating the GatewaySubnet, the Azure Portal will automatically deploy the required resources, such as the Virtual Machine Scale Set (VMSS), NAT Gateway IP addresses, and the necessary routing. Once Gateway1 is deployed, the VMs can be configured to use the NAT gateway for internet access, and no additional administrative effort is required.

upvoted 1 times

 **Studies** 4 months ago

**Selected Answer: C**

To deploy Azure Virtual Network NAT gateway named Gateway1 to Vnet1 while meeting the given requirements, the minimum number of subnets required on Vnet1 is three.

The three subnets required are:

Subnet1: This subnet will be used to host VM1, which has a basic SKU public IP address.

Subnet2: This subnet will be used to host VM2, which has a standard SKU public IP address.

GatewaySubnet: This subnet will be used to host the Azure Virtual Network NAT gateway named Gateway1.

By creating the GatewaySubnet, the Azure Portal will automatically deploy the required resources, such as the Virtual Machine Scale Set (VMSS), NAT Gateway IP addresses, and the necessary routing. Once Gateway1 is deployed, the VMs can be configured to use the NAT gateway for internet access, and no additional administrative effort is required.

upvoted 1 times

 **energie** 4 months, 2 weeks ago

**Selected Answer: B**

Answer is 3(B): GatewaySubnet, Subnet1 and Subnet2. NAT GW doesn't need a separate subnet, it can be associated with Subnet1 or Subnet2 or both.

upvoted 3 times

 **mVic** 4 months ago

I agree.

We have 3 subnets from start in VNet1 - GatewaySubnet, Subnet1 and Subnet2.

You can deploy NAT GW without associating it to any Subnet. NAT GW is an Azure Service, it doesn't need a dedicated subnet.

The requirements are that VM1 and VM2 connect to internet using their existing Public IPs. Associating NAT GW with any Subnet will make the outbound traffic to flow through it only.

NAT GW isn't compatible with Basic SKU resources (PIP or LB).

upvoted 1 times

## 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.)

Home > Private DNS zones > fabrikam.com

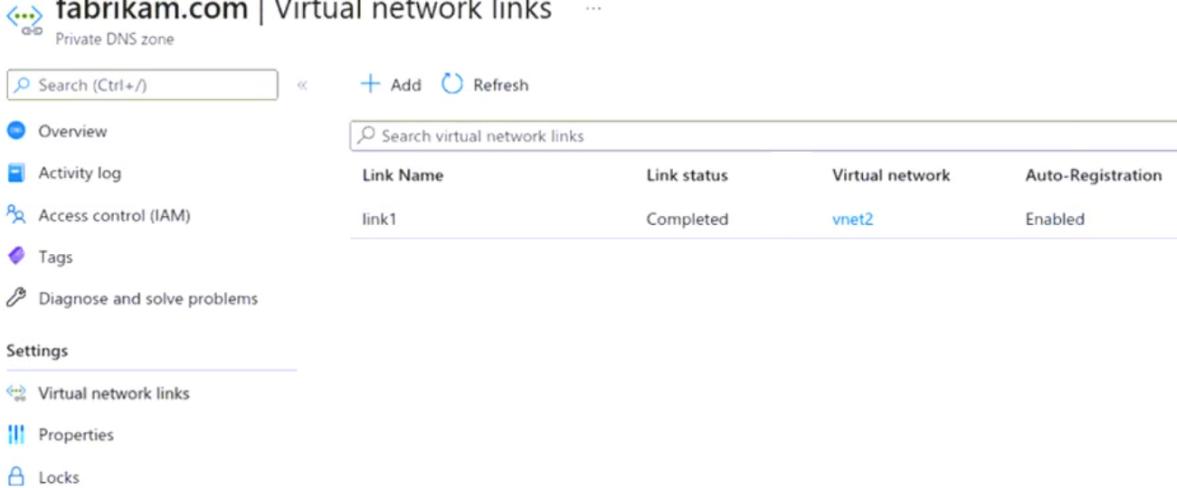
 Private DNS zone

Search (Ctrl+/) << + Add Refresh

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

Overview     Activity log     Access control (IAM)     Tags     Diagnose and solve problems

Virtual network links     Properties     Locks



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.	<input type="radio"/>	<input type="radio"/>
Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	<input type="radio"/>	<input type="radio"/>
Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	<input type="radio"/>	<input type="radio"/>

**Correct Answer:**

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.	<input checked="" type="radio"/>	<input type="radio"/>
Enabling a virtual network link for Vnet3 in the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	<input checked="" type="radio"/>	<input type="radio"/>
Adding an A record for app1.fabrikam.com to the fabrikam.com DNS zone will enable VM5 to resolve app1.fabrikam.com.	<input type="radio"/>	<input checked="" type="radio"/>

✉ **Madball** Highly Voted 4 months, 2 weeks ago

NYN

VM5 is in VNET3 and VNET3 isn't linked to the fabrikam.com private DNS zone. This means it won't be able to resolve anything in that private DNZ zone until it is linked.

upvoted 18 times

✉ **Gabaky** Highly Voted 4 months, 1 week ago

NYN

10.4.0.2 and 10.4.0.5 are within same subnet that was initially not resolving

upvoted 13 times

✉ **Aziza\_Adam** Most Recent 4 months, 2 weeks ago

No

Yes

No

upvoted 5 times

✉ **bobg** 4 months, 2 weeks ago

n/y/n . There is no mention of 10.4.0.2 and what it is in the question.

upvoted 5 times

✉ **Madball** 4 months, 1 week ago

10.4.0.2 is the DNS servers for that IP address space, but since there is no private DNS zone linked to the VNET it won't resolve the load balancer FQDN.

upvoted 6 times

Your company has five offices. Each office has a firewall device and a local internet connection. The offices connect to a third-party SD-WAN.

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains a virtual network gateway named Gateway1. Each office connects to Gateway1 by using a Site-to-Site VPN connection.

You need to replace the third-party SD-WAN with an Azure Virtual WAN.

What should you include in the solution?

- A. Delete Gateway1.
- B. Create new Point-to-Site (P2S) VPN connections on the firewall devices.
- C. Create an Azure Traffic Manager profile.
- D. Enable active-active mode on Gateway1.

**Correct Answer: B**

*Community vote distribution*

A (100%)

 **flurgen248** Highly Voted ⓘ 3 months, 3 weeks ago

**Selected Answer: A**

Virtual Wan requires a Wan Hub Gateway, so Gateway1 should be deleted (after the new gateway is connected).

<https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology#step-5-transition-connectivity-to-virtual-wan-hub>  
upvoted 7 times

 **WaleedSaleh** Most Recent ⓘ 1 day, 1 hour ago

**Selected Answer: A**

Correct

upvoted 1 times

 **tomtom2022** 1 month, 3 weeks ago

**Selected Answer: A**

A is correct

upvoted 1 times

 **ayoubneo** 3 months, 1 week ago

**Selected Answer: A**

Correct

upvoted 1 times

 **AP78** 3 months, 2 weeks ago

**Selected Answer: A**

Correct

upvoted 1 times

 **omgMerrick** 3 months, 3 weeks ago

**Selected Answer: A**

A. Delete Gateway1

A hub gateway isn't the same as a virtual network gateway that you use for ExpressRoute and VPN Gateway. For example, when using Virtual WAN, you don't create a site-to-site connection from your on-premises site directly to your VNet. Instead, you create a site-to-site connection to the hub. The traffic always goes through the hub gateway.

\*\*\* This means that your VNets don't need their own virtual network gateway. Virtual WAN lets your VNets take advantage of scaling easily through the virtual hub and the virtual hub gateway.

Source:

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

upvoted 3 times

 **Ayokun** 4 months ago

Enable active - active and then delete.

upvoted 1 times

✉️ **drprepper\_** 3 months, 2 weeks ago

Are u ok bro?

upvoted 4 times

✉️ **samir111** 4 months ago

**Selected Answer: A**

delete Gateway1

upvoted 2 times

✉️ **certacc** 4 months, 1 week ago

I believe the answer is A. The vWAN migration doc states you would create new VPN connections to the HUB (making sure the existing route is still prioritised), then test the new connection with a test VNet attached to the HUB, and then when ready delete the old connections and gateway to failover.

upvoted 4 times

✉️ **Bbb78** 4 months, 2 weeks ago

Why p2s ? I would delete GW first!

upvoted 3 times

✉️ **Ayboum** 4 months, 1 week ago

Don't think so, i say active active mode on gateway to be able to create a connection to the Virtual WAN  
<https://learn.microsoft.com/en-us/azure/virtual-wan/connect-virtual-network-gateway-vwan>

upvoted 5 times

✉️ **wooyourdaddy** 3 months, 1 week ago

I agree after reading that link, where it states "Creating a connection from a VPN Gateway (virtual network gateway) to a Virtual WAN (VPN gateway) is similar to setting up connectivity to a virtual WAN from branch VPN sites."

The answer should be D, to enable active-active mode on Gateway1 as per step 1 in the link.

upvoted 1 times

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. internal load balancers
- B. Azure DDoS Protection for virtual networks
- C. service endpoint policies
- D. service endpoints

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **WaleedSaleh** 1 day, 1 hour ago

**Selected Answer: A**

A. Internal Load Balancers  
upvoted 1 times

 **omgMerrick** 3 months, 3 weeks ago

**Selected Answer: A**

A. Internal Load Balancers

Internal load balancers require IP addresses in the subnets because they distribute network traffic among resources that are located in a private network.

You do not need IP addresses for Azure DDoS Protection for virtual networks because it is a service that protects your resources from distributed denial-of-service (DDoS) attacks.

You do not need IP addresses for service endpoint policies because they are used to filter network traffic from a subnet to an Azure service.

You do not need IP addresses for service endpoints because they are logical connections from a virtual network subnet to an Azure service.

Source:

<https://learn.microsoft.com/en-us/training/modules/design-ip-addressing-for-azure/>

upvoted 2 times

 **flurgen248** 3 months, 3 weeks ago

**Selected Answer: A**

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

An internal (or private) load balancer is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network.

upvoted 2 times

 **JennyHuang36** 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 1 times

 **mVic** 4 months ago

**Selected Answer: A**

Internal Load Balancers is the right option.

upvoted 3 times

 **Ayboum** 4 months, 1 week ago

Correct

upvoted 2 times

 **harshit101** 4 months, 1 week ago

ok sir, very good, god bless.

upvoted 1 times

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

You plan to deploy a hub and spoke topology by using virtual network peering.

You need to configure VNet1 as the hub network. The solution must meet the following requirements:

- Support transitive routing between spokes.
- Maximize network throughput.

What should you include in the solution?

- A. Azure VPN Gateway
- B. Azure Route Server
- C. Azure Private Link
- D. Azure Firewall

**Correct Answer: A**

*Community vote distribution*

D (100%)

 **Ayboum** Highly Voted 4 months, 1 week ago

**Selected Answer: D**

Azure Firewall is the best response  
Communication through an NVA

If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.

You can also use a VPN gateway to route traffic between spokes, although this choice affects latency and throughput. For configuration details, see Configure VPN gateway transit for virtual network peering.

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>  
upvoted 10 times

 **mammoot** 4 months ago

I agree with this, especially since they say to maximise throughput.  
VPN Gateways have less throughput in comparison

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

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#how-can-i-increase-my-firewall-throughput>  
upvoted 1 times

 **mVic** 4 months ago

Agree with firewall.  
VPN Gateways might even not be required since it's not specified the VNets are in a different region. And it specifies you use peerings.  
upvoted 1 times

 **omgMerrick** Highly Voted 4 months ago

**Selected Answer: D**

Forgot to vote. Wish you could edit your posts...

Source:

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

upvoted 5 times

 **MrBlueSky** Most Recent 2 months, 2 weeks ago

This is a trick question as you'd never use Azure Firewall to accomplish this unless you need the other features of it. The question doesn't mention any of these additional features of Azure Firewall as a requirement.

However, there are no other suitable answers so clearly what they are testing on here is your knowledge of if Azure Firewalls can be used at all.

Answer is D

upvoted 2 times

✉ **omgMerrick** 4 months ago

D. Azure Firewall

There are two main ways to allow spoke virtual networks to communicate with each other:

Communication via an NVA like a firewall and router. This method incurs a hop between the two spokes.

Communication by using virtual network peering or Virtual Network Manager direct connectivity between spokes. This approach doesn't cause a hop between the two spokes and is recommended for minimizing latency.

Communication through an NVA

If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.

Source:

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

upvoted 4 times

✉ **Ayboum** 4 months, 1 week ago

Azure Firewall is the best response

Communication through an NVA

If you need connectivity between spokes, consider deploying Azure Firewall or another NVA in the hub. Then create routes to forward traffic from a spoke to the firewall or NVA, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.

You can also use a VPN gateway to route traffic between spokes, although this choice affects latency and throughput. For configuration details, see Configure VPN gateway transit for virtual network peering.

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

upvoted 3 times

✉ **Bbb78** 4 months, 2 weeks ago

b.Azure Router Service is probably a better answer than VPN GW

upvoted 3 times

✉ **Kafura** 2 months ago

Use Azure Route Server to enable dynamic routing between your network appliances and gateways in Azure, instead of using static routing.

Azure Route Server provides Border Gateway Protocol (BGP) endpoints using standard routing protocol to exchange routes.

upvoted 1 times

✉ **\_fvt** 2 months, 2 weeks ago

You need an NVA/FW for ARS, it's just to facilitate the routing setup not handle it: <https://learn.microsoft.com/fr-fr/azure/route-server/overview>

upvoted 1 times

## HOTSPOT

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

Name	Location
RG1	East US
RG2	East US
RG3	UK West

You have the virtual networks shown in the following table.

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

You have the subnets shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Vnet1 can be moved to RG3.	<input type="radio"/>	<input type="radio"/>
Three hundred virtual machines can be deployed to the East US Azure region.	<input type="radio"/>	<input type="radio"/>
A new virtual network named Vnet2 can be created in RG2 in the East US Azure region.	<input type="radio"/>	<input type="radio"/>

Statements	Yes	No
Vnet1 can be moved to RG3.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>Correct Answer:</b> Three hundred virtual machines can be deployed to the East US Azure region.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
A new virtual network named Vnet2 can be created in RG2 in the East US Azure region.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

 **Madball** Highly Voted 4 months, 1 week ago  
YNN

You can move VNET1 to RG3.

You cannot deploy 300 VMs to East US Azure region because the subnet in VNET1 is a /24 which isn't large enough.

You cannot create a new VNET called VNET2 in RG2 because there is already a VNET with that name in the resource group.  
upvoted 12 times

 **ubdubdoo** 1 month ago  
you're wrong. you can deploy two vnets in the same RG, as long as they are in different regions.  
upvoted 1 times

 **jarz** 1 month, 4 weeks ago  
I'd say YYY they talk of the region, not the subnet. And yes the Subnet is a /24, but the VNET is a /16. Or am I splitting hairs here?  
upvoted 2 times

 **oakl** 1 month, 1 week ago

Yes, you could add a new subnet to fit the total of 300 machines but you are supposed to evaluate the situation as described in the question. Only the /24 subnet is mentioned which has 251 free IP addresses. Hence it should be YNN

upvoted 1 times

✉️  **staffo** Highly Voted  4 months, 1 week ago

I thought it was NNN but just tested and you can move VNET1 to RG3. They are in different locations so its fine. So Answer is YNN.

upvoted 8 times

✉️  **xamkiller** 1 month, 2 weeks ago

Even if both are in the same location you can create however with a different name. Basically, you can create everything same but with a different name for the VNET.

upvoted 1 times

✉️  **Himank20** Most Recent  1 month, 3 weeks ago

I think it should be NYN

- A. Both Vnets have same range so Vnet1 can't be moved
- B. If we consider the /16 range of Vnet, 500 VMs can be deployed
- C. Two Vnets can have same name if they are in different region

Correct me if I'm wrong

upvoted 3 times

✉️  **crypto700** 1 month, 4 weeks ago

NNN

- you cannot move Vnet to RG3. because they have the same subnet.
- you cannot deploy 300 VMs, Because the subnet size is /24.

upvoted 1 times

✉️  **oakl** 1 month, 1 week ago

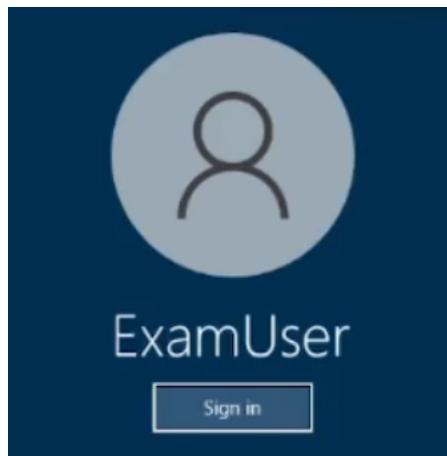
You can move the vnet to RG3. Just because they are in the same resource group doesn't mean there is any interaction between these networks. You could deploy as many vnets as you like with the same address range within this resource groups as long as the names are different. What you won't be able to do is to setup peering between these networks because their address ranges overlap.

upvoted 3 times

✉️  **crypto700** 1 month, 1 week ago

You are right... just tested in the Lab  
YNN

upvoted 2 times

**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: xxxxxxxxxxx

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 all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address. The solution must minimize administrative effort when adding hosts to the subnet.

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

**Correct Answer:**

NAT gateway provides outbound internet connectivity for one or more subnets of a virtual network. Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet. NAT gateway specifies which static IP addresses virtual machines use when creating outbound flows.

Plan:

Stage 1: Create a NAT gateway

Stage 2: Edit subnet subnet3-2 and link it to the NAT gateway

Stage 1: Create a NAT gateway

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter NAT gateway. Select NAT gateways in the search results.

Step 3: Select + Create.

Step 4: In Create network address translation (NAT) gateway, enter or select this information in the Basics tab:

\* NAT gateway name: Enter myNATgateway

Step 5: Select the Outbound IP tab, or select the Next: Outbound IP button at the bottom of the page.

Step 6: In the Outbound IP tab, enter or select the following information:

Public IP addresses - Select Create a new public IP address.

In Name, enter myPublicIP.

Select OK.

Step 7: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 8: Select Create.

Stage 2: Edit subnet subnet3-2 and link it to the NAT gateway

Change subnet settings

Step 1: Go to the Azure portal to view your virtual networks. Search for and select Virtual networks.

Step 2: Select the name of the virtual network containing the subnet you want to change.

Step 3: From Settings, select Subnets.

Step 4: In the list of subnets, select the subnet you want to change settings for. Here choose subnet3-2 connect.

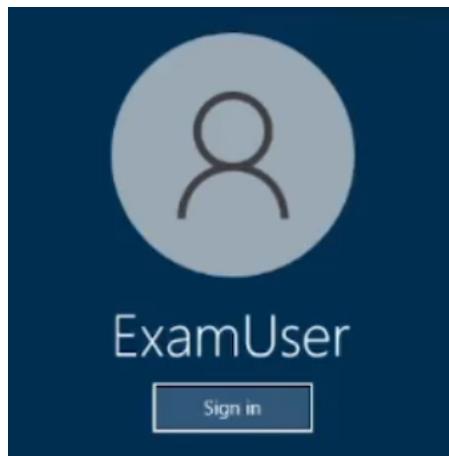
Step 5: In the subnet page, change the NAT Gateway to myNATgateway (the one we created in Stage 1).

Step 6: Select Save.

Reference:

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

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

**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: xxxxxxxxxxx

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 subnet 4-3 can accommodate 507 hosts.

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

**Correct Answer:**

Change subnet settings

Step 1: Go to the Azure portal to view your virtual networks. Search for and select Virtual networks.

Step 2: Select the name of the virtual network containing the subnet you want to change.

Step 3: From Settings, select Subnets.

Step 4: In the list of subnets, select the subnet you want to change settings for. We select subnet 4-3.

Step 5: In the subnet page, change the Subnet address range setting:

For 507 hosts we need a 9-bit address range or larger, that is /23.

Change to address to /23. For example: 10.0.0.0/23 will work fine.

Note: For example, in a virtual network with address space 10.0.0.0/16, you might define a subnet address space of 10.0.0.0/22. The smallest range you can specify is /29, which provides eight IP addresses for the subnet. Azure reserves the first and last address in each subnet for protocol conformance. Three more addresses are reserved for Azure service usage. As a result, defining a subnet with a /29 address range results in three usable IP addresses in the subnet.

Step 6: Select Save.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet>

Question #37

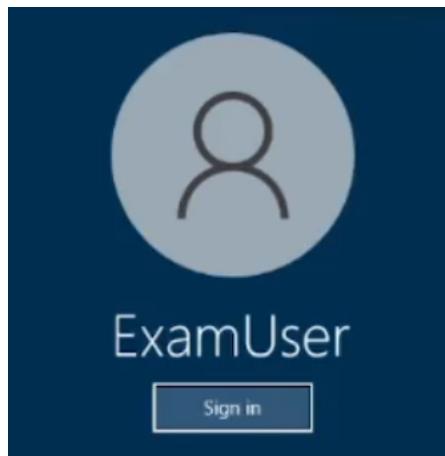
*Topic 2*

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. internal load balancers
- B. Azure DDoS Protection for virtual networks
- C. service endpoint policies
- D. service endpoints

**Correct Answer: A**

**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: xxxxxxxxx

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 virtual machines on VNET1 and VNET2 are included automatically in a DNS zone named contosoazure. The solution must ensure that the virtual machines on VNET1 and VNET2 can resolve the names of the virtual machines on either virtual network.

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

What is the auto registration feature in Azure DNS private zones?

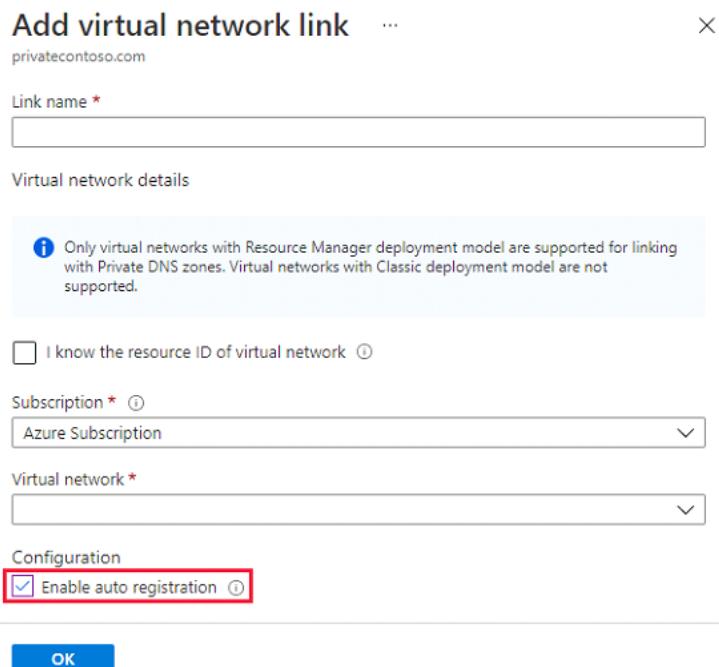
The Azure DNS private zones auto registration feature manages DNS records for virtual machines deployed in a virtual network. When you link a virtual network with a private DNS zone with this setting enabled, a DNS record gets created for each virtual machine deployed in the virtual network.

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

Step 1: Locate the DNS zone contosoazure

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

Step 3: Select Add.



Step 4: Type myLink for the Link name.

Step 5: For Virtual network, select VNET1.

Step 6: Select the Enable auto registration check box.

To enable auto registration, select the checkbox for "Enable auto registration" when you create the virtual network link.

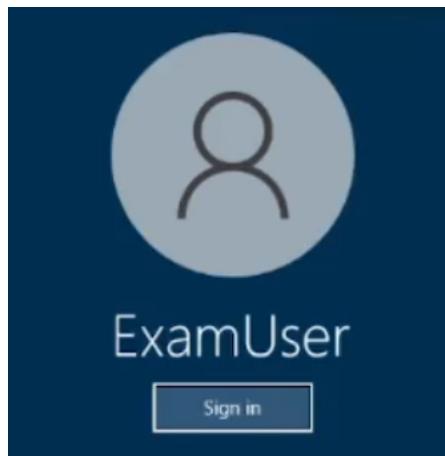
Step 7: Select OK.

Step 8: Repeat procedure for VNET2.

Reference:

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

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

**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: xxxxxxxxxxx

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 you can deploy Azure virtual machines to the France Central Azure region. The solution must ensure that virtual machines in the France Central region are in a network segment that has an IP address range of 10.5.1.0/24.

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



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

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

Network interfaces  
IP addresses  
Virtual network and subnets

Create a virtual network

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

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

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

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

**Create virtual network** ... X

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

**Project details**

Subscription \*  ▼

Resource group \*  ▼  
[Create new](#)

**Instance details**

Name \*  ✓

Region \*  ▼

[Review + create](#) [< Previous](#) [Next : IP Addresses >](#) [Download a template for automation](#)

**Correct Answer:**

Step 5: Enter Region: France Central

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

[Home](#) > [Create a resource](#) > [Marketplace](#) > [Virtual network](#) >

**Create virtual network** ...

[Basics](#) [IP Addresses](#) [Security](#) [Tags](#) [Review + create](#)

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

**IPv4 address space**

✓

Add IPv6 address space ○

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

**Add subnet** Remove subnet

Subnet name	Subnet address range	NAT gateway
<input type="text" value="MySubnet"/>	10.1.0.0/24	-

**Info** Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#) ○

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

Step 8: Click Add subnet

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

Step 10: Finish the wizard.

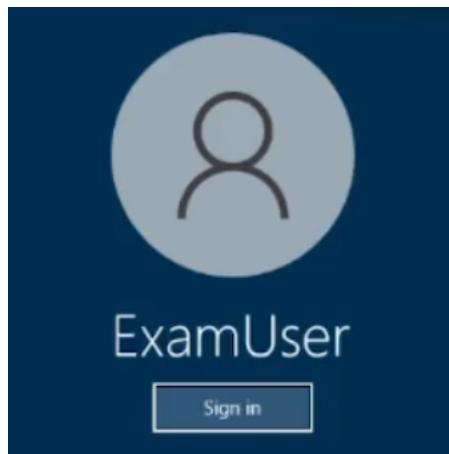
Reference:

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

✉️  **Crazysaffer** 3 weeks, 5 days ago

Remember to select the right location. (France Central Azure region)

upvoted 1 times

**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: xxxxxxxxx

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 VNET1 and VNET2 can communicate. The solution must minimize latency between the virtual networks.

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

**Correct Answer:**

## Peer virtual networks

Step 1: In the search box at the top of the Azure portal, look for VNet1. When VNET1 appears in the search results, select it.

The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains the text "myVirtualNetwork1". Below the search bar, the "Virtual networks" result is highlighted with a red box. The left sidebar includes links for Home, Dashboard, All services, Favorites, Resource groups, All resources, Recent, App Services, Virtual machines (classic), Virtual machines, and SQL databases. The main content area displays search results for "Virtual networks" and "Virtual network gateway", with "myVirtualNetwork1" selected. The bottom of the screen shows a resource group named "myresourcegroup".

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

The screenshot shows the "myVirtualNetwork1 | Peerings" page in the Azure portal. The left sidebar lists various settings: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Address space, Connected devices, Subnets, DDoS protection, Firewall, Security, DNS servers, Peerings (highlighted with a red box), and Service endpoints. The main content area displays a table for managing peerings, with a red box highlighting the "+ Add" button in the top right corner of the table header. The table has columns for Name, Peering status, Peer, and Gateway transit.

Step 3: Enter or select the following information, accept the defaults for the remaining settings, and then select Add.

\* ..

\* Virtual network

Select VNET2 for the name of the remote virtual network. The remote virtual network can be in the same region of VNET1 or in a different region.

Home > myVirtualNetwork1 >

### Add peering

myVirtualNetwork1

For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.

This virtual network

Peering link name \*

myVirtualNetwork1-myVirtualNetwork2

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

Virtual network deployment model  Resource manager  Classic

I know my resource ID

Subscription

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**

**Step 4: Click Add**

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

Home > myVirtualNetwork1

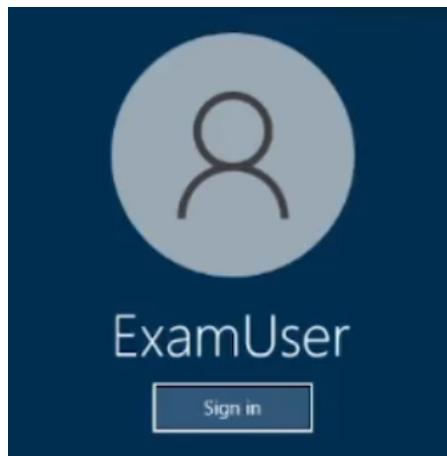
 **myVirtualNetwork1 | Peerings**

Virtual network

<input type="text" value="Search (Ctrl+ /)"/>	<input type="button" value="Add"/>	<input type="button" value="Refresh"/>									
<input type="text" value="Filter by name..."/> <table border="1"> <thead> <tr> <th>Name ↑↓</th><th>Peering status ↑↓</th><th>Peer ↑↓</th><th>Gateway transit ↑↓</th></tr> </thead> <tbody> <tr> <td>myVirtualNetwork1-myVirtualNetwork2</td><td>Connected</td><td>myVirtualNetwork2</td><td>Disabled</td></tr> </tbody> </table>			Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓	myVirtualNetwork1-myVirtualNetwork2	Connected	myVirtualNetwork2	Disabled	
Name ↑↓	Peering status ↑↓	Peer ↑↓	Gateway transit ↑↓								
myVirtualNetwork1-myVirtualNetwork2	Connected	myVirtualNetwork2	Disabled								

**Reference:**

<https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal>

**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: xxxxxxxxxxx

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 the owner of VNET3 receives an alert if an administrative operation is performed in the virtual network.

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

**Correct Answer:**

## Monitoring Azure virtual network

### Alerts

Azure Monitor alerts proactively notify you when important conditions are found in your monitoring data. They allow you to identify and address issues in your system before your customers notice them. You can set alerts on metrics, logs, and the activity log.

Create a new alert rule in the Azure portal

Step 1: In the portal, select Monitor > Alerts.

Step 2: Open the + Create menu and select Alert rule.

The screenshot shows the Azure Monitor Alerts interface. On the left, there's a navigation pane with various monitoring services like Home, Dashboard, All services, Favorites, All resources, Resource groups, App Services, Function App, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor (highlighted with a red box and number 1), Advisor, Microsoft Defender for Cloud, Cost Management + Billing, and Help + support. Under the Monitor section, there are sub-options: Overview, Activity log (highlighted with a red box and number 2), Alerts (highlighted with a red box and number 3), Metrics, Logs, Service Health, Workbooks, Insights, Applications, Virtual Machines, Storage accounts, Containers, Networks, SQL (preview), Azure Cosmos DB, Key Vaults, Azure Cache for Redis, and Azure Data Explorer Clusters. The main area shows an 'Alert rule' card with a count of 3. Below it is an 'Alert processing rule' section with counts: Error (273), Warning (199), Informational (0), and Verbose (7). A table lists 18 alert rules, each with a checkbox, name, severity (Error or Critical), alert condition (Fired), and user response (New). The table has columns for Name, Severity, Alert condition, and User response.

Step 3: On the Select a resource pane, set the scope for your alert rule. You can filter by subscription, resource type, or resource location. We select Virtual Network.

The Available signal types for your selected resources are at the bottom right of the pane.

Step 4: Select Include all future resources to include any future resources added to the selected scope.

Step 5: Select Done.

Step 6: Select Next: Condition at the bottom of the page.

Step 7: On the Select a signal pane, filter the list of signals by using the signal type and monitor service:

\* Signal type: The type of alert rule you're creating.  
We select Activity log

\* Monitor service: The service sending the signal. This list is pre-populated based on the type of alert rule you selected.

We select Activity log – Administrative (The service that provides the Administrative activity log events)

Step 8: On the Actions tab, select to create the required action group.

The screenshot shows the 'Actions' tab of the alert rule configuration. At the top, there are tabs: Scope, Condition, Actions (selected), Details, Tags, and Review + create. Below the tabs, a note says 'An action group is a set of actions that can be applied to an alert rule. [Learn more](#)'. There are two buttons: '+ Add action groups' and '+ Create action group'. A table below has columns for 'Action group name' and 'Contains actions'. A message at the bottom says 'No action group selected yet'.

### Step 9: Configure basic action group settings

Home > Alerts > Manage actions >

## Create action group

[Basics](#) [Notifications](#) [Actions](#) [Tags](#) [Review + create](#)

An action group invokes a defined set of notifications and actions when an alert is triggered. Learn more

**Project details**

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

Subscription \* [Contoso](#)

Resource group \* [Contoso-RG](#) [Create new](#)

**Instance details**

Action group name \* [Sample action group](#)

Display name \* [Sample ag](#)  
This display name is limited to 12 characters

[Review + create](#) [Previous](#) [Next: Notifications >](#)

Step 10: Configure notifications. To open the Notifications tab, select Next: Notifications.  
Alternately, at the top of the page, select the Notifications tab.

Step 11: Define a list of notifications to send when an alert is triggered.

Notification: Email Azure Resource Manager Role  
Name: Notify Owner

Home > Alerts > Manage actions >

## Create action group

[Basics](#) [Notifications](#) [Actions](#) [Tags](#) [Review + create](#)

**Notifications**

Configure the method in which users will be notified when the action group triggers. Select notification types, provide receiver details and add a unique description. This step is optional.

Notification type	Name	Selected
<a href="#">Email/SMS message/Push/Voice</a>	<a href="#">Notify on-call team</a>	Email
<a href="#">Email/Azure Resource Manager Role</a>	<a href="#">Notify subscription owners</a>	Owner

**Email/SMS message/Push/Voice**  
Add or edit an Email/SMS/Push/Voice action

Email  
Email: on-call@contoso.com

SMS (Carrier charges may apply)  
Country code: 1

Azure app Push Notifications  
Azure account email:

Voice  
Country code: 1

Enable the common alert schema. Learn more  
[Yes](#) [No](#)

**OK**

[Review + create](#) [Previous](#) [Next: Actions >](#)

Step 12: Select OK.

Step 13: Finish the remaining steps in the wizard.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network/monitor-virtual-network>  
<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule?tabs=metric#create-a-new-alert-rule-in-the-azure-portal>

 **ABLYGK** 2 weeks, 3 days ago

1. Monitor □ Alerts □ Alert Rule
  2. Alert Rule
- Scope > Select VNet3 > Apply
  - Condition > See all signals > Activity Log > All Administrative Operation > Apply

• Actions > Create Action Group

Basic Tab

Notification > Email/SMS-message/Push Voice > Put the email > Name

Actions > Not required for this scenario just notification is enough

Tags > You can assign a necessary tag for the action group

Review+Create

• Details

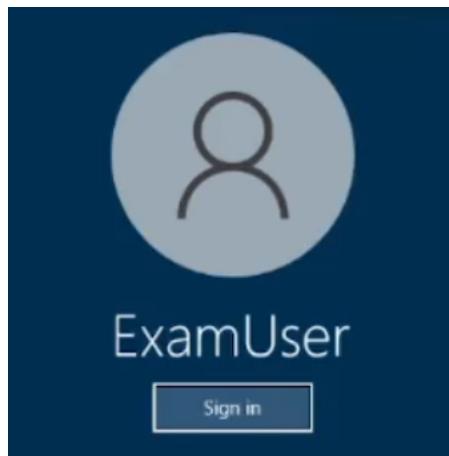
Alert Rule Name > VNET3 Notification

Description > Notify the admin for any changes on VNET3

• Tags > Put any tag that represent the Alert Rule

• Review+Create

upvoted 2 times

**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: xxxxxxxxx

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 archive all the metrics of VNET1 to an existing storage account.

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



Monitoring Azure virtual network  
Azure virtual network uses Azure Monitor.

#### Data platform

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

#### Retention of metrics

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

#### Send to Azure Storage

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

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

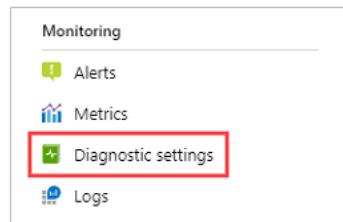
Archiving logs and metrics to a Storage account is useful for audit, static analysis, or backup. Compared to using Azure Monitor Logs or a Log Analytics workspace, Storage is less expensive, and logs can be kept there indefinitely.

#### Create diagnostic settings

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

Step 1: Select the Virtual Network VNET1.

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



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

The screenshot shows the 'Diagnostics settings' blade. It has filters for Subscription (Contoso IT - demo), Resource group (ContosoMonitor), Resource type (Kubernetes services), and Resource (ContosoMonitor1). Below the filters, it says 'No diagnostic settings defined' and has a button '+ Add diagnostic setting' highlighted with a red box.

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

The screenshot shows the 'Diagnostic settings' blade for a Logic app named 'simpletest2'. It has filters for Subscription (Azure Monitor Demo), Resource group (ContosoLoanApp1), Resource type (Logic apps), and Resource (simpletest2). The table lists two rows: 'logstoStorage' (Storage account: loanapptestsa) and 'send to EH for alerts' (Event hub namespace: RootManageSharedAccessKey). Both rows have an 'Edit setting' button highlighted with a red box. At the bottom, there is a '+ Add diagnostic setting' button highlighted with a red box.

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

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

[Home](#) > [Monitor](#) >

**Diagnostic setting** ...

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name \*

Logs

Category groups ⓘ

audit

allLogs

Categories

AuditEvent

AzurePolicyEvaluationDetails

Destination details

Send to Log Analytics workspace

Archive to a storage account

Stream to an event hub

Send to partner solution

Metrics

AllMetrics

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

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

Category details

log

WorkflowRuntime

Retention (days)

0

metric

AllMetrics

Retention (days)

0

**Info** Retention only applies to storage account. Retention policy ranges from 1 to 365 days. If you do not want to apply any retention policy and retain data forever, set retention (days) to 0.

Destination details

Send to Log Analytics

Archive to a storage account

**Info** Showing all storage accounts including classic storage accounts

Location

West US

Subscription

AI - SRT- Dev ...

Storage account \*

azmonitorbidev

Stream to an event hub

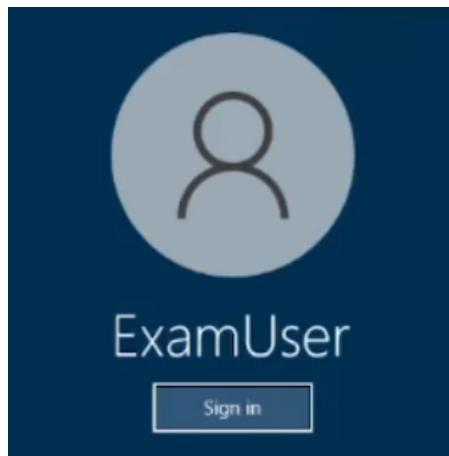
Step 8: Select Save.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings>

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

## 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: xxxxxxxxx

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 plan to deploy 100 virtual machines to subnet-1. The virtual machines will NOT be assigned a public IP address. The virtual machines will call the same API which is hosted by a third party. The virtual machines will make more than 10,000 calls per minute to the API.

You need to minimize the risk of SNAT port exhaustion. The solution must minimize administrative effort.

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

SNAT exhaustion occurs when a backend instance runs out of given SNAT Ports. A load balancer can still have unused SNAT ports. If a backend instance's used SNAT ports exceed its given SNAT ports, it will be unable to establish new outbound connections.

Use a NAT gateway for outbound connectivity to the Internet. Virtual network NAT gateway is a highly resilient and scalable Azure service that provides outbound connectivity to the internet from your virtual network. A NAT gateway's unique method of consuming SNAT ports helps resolve common SNAT exhaustion and connection issues.

(Basic load balancers and basic public IP addresses aren't compatible with NAT.)

Create a NAT gateway.

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter NAT gateway. Select NAT gateways in the search results.

Step 3: Select + Create.

**Correct Answer:** Step 4: In Create network address translation (NAT) gateway, enter or select this information in the Basics tab.

\* Details omitted \*

Step 5: Select the Outbound IP tab, or select the Next: Outbound IP button at the bottom of the page.

Step 6: In the Outbound IP tab, enter or select the following information:

\* Public IP addresses

Select Create a new public IP address.

In Name, enter myPublicIP.

Select OK.

Step 7: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 8: Select Create.

Reference:

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections>

<https://learn.microsoft.com/en-us/azure/load-balancer/troubleshoot-outbound-connection>

✉️  **Shimi** 2 months, 1 week ago

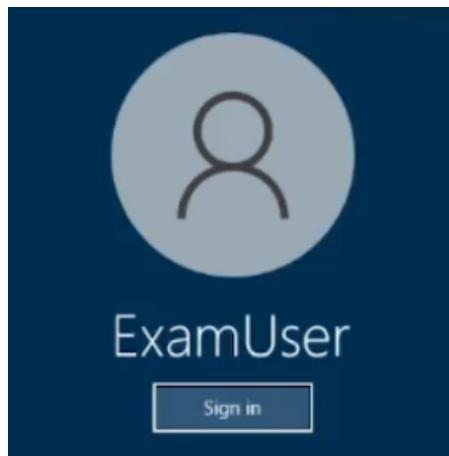
Shouldn't this be a standard load balancer?

upvoted 2 times

✉️  **MrBlueSky** 2 months ago

No. When you see SNAT Port exhaustion the answer they want you to pick is likely NAT Gateway as it specifically addresses this problem that LBs have

upvoted 5 times

**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: xxxxxxxxx

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 plan to deploy an appliance to subnet3-2. The appliance will perform packet inspection and will have an IP address of 10.3.2.100.

You need to ensure that all traffic to the internet from subnet3-1 is forwarded to the appliance for inspection.

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



**Plan:**

- Stage 1: Create a route table
- Stage 2: Create a route
- Stage 3: Associate a route table to a subnet

Stage 1: Create a route table

Step 1: On the Azure portal menu or from the Home page, select Create a resource.

Step 2: In the search box, enter Route table. When Route table appears in the search results, select it.

Step 3: In the Route table page, select Create.

Step 4: In the Create route table dialog box:

\* Details omitted\*

Step 5: Select Review + create and then Create to create your new route table.

Stage 2: Create a route

Step 6: Make sure the route table you created is selected.

Step 7: From the route table menu bar, choose Routes and then select + Add.

Step 8: Enter a unique Route name for the route within the route table.

**Add route**

myRouteTable

Route name \*

Address prefix destination \* ⓘ

Select source

Next hop type \* ⓘ

Select next hop type

Next hop address \* ⓘ

**Add**

Step 9: Enter the Address prefix, in Classless Inter-Domain Routing (CIDR) notation, that you want to route traffic to. The prefix can't be duplicated in more than one route within the route table, though the prefix can be within another prefix. For example, if you defined 10.0.0.0/16 as a prefix in one route, you can still define another route with the 10.0.0.0/22 address prefix. Azure selects a route for traffic based on longest prefix match.

Enter the following:

Address prefixes: 0.0.0.0/0

Next hop type: Internet

Next hop address: 10.3.2.100

Step 10: Click Add.

**Correct Answer:** Stage 3: Associate a route table to a subnet

Step 11: In the virtual network list, choose the virtual network that contains the subnet you want to associate a route table to.

Step 12: In the virtual network menu bar, choose Subnets.

Step 13: Select the subnet you want to associate the route table to. In our case select subnet3-1, (You need to ensure that all traffic to the internet from subnet3-1 is forwarded to the appliance for inspection.)

Step 14: In Route table, choose the route table you want to associate to the subnet. Select the one you created earlier.

**default**

VNetA

Name

Subnet address range \* ⓘ

10.0.0.0/24  
10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ  
None

Network security group  
None

Route table  
None

None

myRouteTable

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ  
0 selected

**SUBNET DELEGATION**

Delegate subnet to a service ⓘ  
None

**Save** **Cancel**

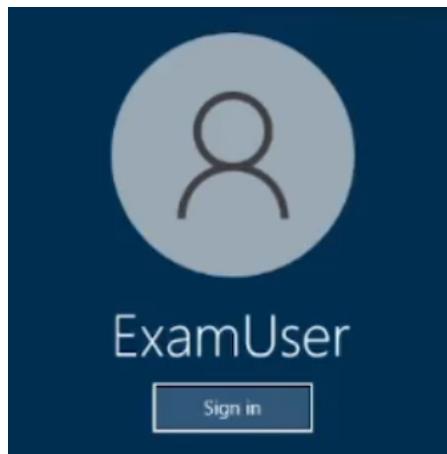
Step 15: Select Save.

Reference:  
<https://learn.microsoft.com/en-us/azure/virtual-network/manage-route-table>  
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#how-azure-selects-a-route>

✉ **khanda** Highly Voted 2 months, 1 week ago  
Next hop should not be internet if you want to send your internet traffic to an NVA. It should be "Virtual appliance"  
upvoted 8 times

✉ **occupatissimo** 1 month, 1 week ago  
you're right  
upvoted 1 times

## 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: xxxxxxxxxxx

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 plan to use VNET4 for an Azure API Management implementation.

You need to configure a policy that can be used by an Azure application gateway to protect against known web attack vectors. The policy must only allow requests that originate from IP addresses in Canada. You do NOT need to create the application gateway to complete this task.

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

**Correct Answer:**

Azure Front Door web application firewall (WAF) protects web applications from common vulnerabilities and exploits. Azure-managed rule sets provide an easy way to deploy protection against a common set of security threats.

You can restrict access to your web applications by country/region.

Plan:

Stage 1: Create a WAF policy

Stage 2: Create a custom WAF Geo location rule that blocks all traffic outside Canada

Stage 3: Create a custom WAF Geo location rule that allows traffic from Canada

First, create a basic WAF policy with a managed Default Rule Set (DRS) using the Azure portal.

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

Step 2: On Create a WAF policy page, Basics tab, enter or select the following information and accept the defaults for the remaining settings:

\* details omitted \*

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

Application Gateway: Select the application gateway, and then select Add.

HTTP Listener: Select the application gateway, select the listeners, then select Add.

Route Path: Select the application gateway, select the listener, select the routing rule, and then select Add.

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

Home > WAF policies > Create a WAF policy

## Create a WAF policy

[Basics](#) [Policy settings](#) [Managed rules](#) [Custom rules](#) [Association](#) [Tags](#) [Review + create](#)

Malicious attacks such as SQL Injection, Cross Site Scripting (XSS), and other OWASP top 10 threats could cause service outage or data loss, and pose a big threat to web application owners. Web Application Firewall (WAF) protects your web applications from common web attacks, keeps your service available and helps you meet compliance requirements.

[Learn more about WAF policy for Front Door](#)

[Learn more about WAF policy for Application Gateway](#)

**Project details**

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

Policy for \* ⓘ

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

**Instance details**

Policy name \* ⓘ  ✓

Location \* ⓘ

Policy state ⓘ  Enabled  Disabled

Stage 2: Create a custom WAF Geo location rule that blocks all traffic outside Canada

Configure WAF rules

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

Custom rules

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

Home > WAF policies > Create a WAF policy

## Create a WAF policy

[Basics](#) [Policy settings](#) [Managed rules](#) [Custom rules](#) [Association](#) [Tags](#) [Review + create](#)

Configure a policy with custom authored rules. Once a rule is matched, the corresponding action that was defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value denotes a higher priority. [Learn more](#)

[+ ADD custom rule](#)

Priority	Name
10	testRule1

**Edit custom rule**

A custom rule is made up of one or more conditions followed by an action. All custom rules for an Application Gateway WAF policy are match rules.

[Learn more about custom rules](#)

Custom rule name \*

Priority \* ⓘ

**Conditions**

Match type ⓘ

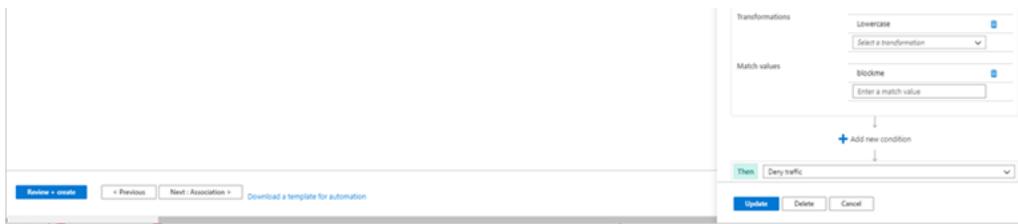
Match variables

Match variable \* ⓘ

+ Add another match variable

Operation  is  is not

Operator \*



Step 6: To create a geo-filtering custom rule in the Azure portal, simply select Geo location as the Match Type, and then select the country/region or countries/regions you want to allow/block from your application.

#### Step 7: Select Add Custom rule



A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy match rules. [Learn more about custom rules](#)

Custom rule name \*

Priority \* ⓘ

Assign priority to the rule

#### Conditions

If

Match type ⓘ

IP address

Number

String

#### Step 8: Select Geo location

Create your Custom Rule with an appropriate name and priority, then choose 'Geo location' from the Match type drop down as above. Next, you'll want to ensure you choose RemoteAddr as the match variable, and decide what logic you want to apply. By logic I mean the pattern that will fire the rule. In this example, I want all traffic except Ireland blocked. So I will choose the Operation 'Is not', then location Ireland, then Deny. If I wanted all traffic allowed and Ireland blocked, I would simply choose the Operation 'Is', I recommend figuring out your pattern then working your way through the final section of the CR.

Step 9: Set Match variable to Canada, choose IS NOT, Choose country Canada, and finally Then: Deny traffic.

#### Conditions

If

Match type ⓘ

#### Match variables



Match variable \* ⓘ

+ Add another match variable

#### Operation

Is  Is not

Country/Region \*

Then

Deny traffic

Stage 3: Create a custom WAF Geo location rule that allows traffic from Canada

Step 10: Repeat steps 5 to 9 but instead use:

Operation: IS

Country/Region: Canada

Then: Allow traffic

Step 11: Finish the creation of the policy. Click Review+Create

Reference:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-drs>

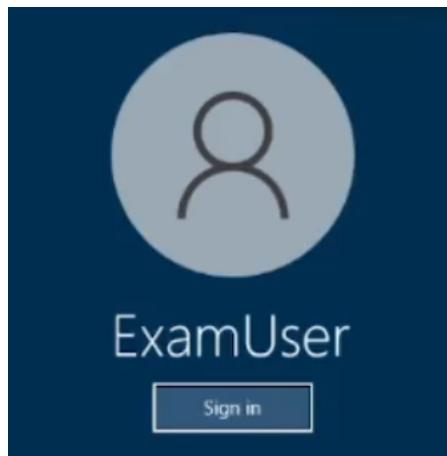
<https://wedoazure.ie/2021/08/09/how-to-enable-web-application-firewall-geomatch-custom-rules/>

<https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/create-waf-policy-ag>

 **occupatissimo** 1 month, 1 week ago

one rule blocking all that isn't from canada is enough

upvoted 2 times

**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: xxxxxxxxxxx

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 plan to deploy several virtual machines to subnet1-2.

You need to prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts on subnet1-2. The solution must minimize administrative effort.

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

**Correct Answer:**

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

## Plan

- Stage 1: Create a network security group
- Stage 2: Associate network security group to subnet
- Stage 3: Create security rule

### Stage 1: Create a network security group

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

Step 1: From the Azure portal menu, select + Create a resource > Networking > Network security group, or search for Network security group in the portal search box.

Step 2: Select Create.

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

\*Details omitted\*

Step 4: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

Step 5: Select Create.

### Stage 2: Associate network security group to subnet

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

Step 6: Search for myNsg (the name you give in stage 1) in the portal search box.

Step 7: Select Subnets from the Settings section of myNSG.

Step 8: In the Subnets page, select + Associate.

The screenshot shows the 'myNSG | Subnets' blade. At the top, there's a search bar and an 'Associate' button. Below that is a table with columns for Name, Address range, Virtual network, and Action. A message says 'No results.' To the left, a sidebar lists Overview, Activity log, Access control (IAM), Tags, and a 'Diagnose and solve problems' section. Under 'Settings', there are links for Inbound security rules, Outbound security rules, Network interfaces, Subnets (which is selected and highlighted with a red box), Properties, and Locks.

Step 9: Under Associate subnet, select myVNet (the virtual network that is available) for Virtual network.

Step 10: Select subnet1-2 for Subnet, and then select OK.

Stage 3: Create security rule

Step 11: Select Inbound security rules from the Settings section of myNSG.

Step 12: In Inbound security rules page, select + Add:

The screenshot shows the 'myNSG | Inbound security rules' blade. At the top, there's a search bar and an '+ Add' button. Below that is a table with columns for Priority, Name, Port, Protocol, Source, Destination, and Action. The table contains three rows: one allowing VNet traffic, one allowing Azure Load Balancer traffic, and one denying all inbound traffic. To the left, a sidebar lists Overview, Activity log, Access control (IAM), Tags, and a 'Diagnose and solve problems' section. Under 'Settings', there are links for Inbound security rules (which is selected and highlighted with a red box), Outbound security rules, and Network interfaces.

Step 13: Create a security rule that blocks TCP port 5585 to the network security group you created earlier. In Add inbound security rule page, enter or select this information:  
(You need to prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts on subnet1-2.)

Source: Leave the default of Any.  
Source port ranges: Leave the default of (\*).  
Destination: Select Network security group.  
Destination Network security groups: Select the network security group you created earlier.  
Service: Leave the default of Custom.  
Destination port ranges: Enter 5585  
Protocol: Select TCP.  
Action: Deny  
Priority: Leave the default of 100.  
Name: Enter something

 Add inbound security rule X

myNSG

Source (i)

Source port ranges \* (i)

Destination (i)  
  
Destination application security group \* (i)

Service (i)

Destination port ranges \* (i)

Protocol  
 Any  
 TCP  
 UDP  
 ICMP

Action  
 Allow  
 Deny

Priority \* (i)

Name \*

Description

Add Cancel

Step 14: Select Add.

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

 ABIYGK 2 weeks, 3 days ago

The lab is about creating NSG only, The NSG needs to deny traffic on port 5585 to the Subnet1-2. The image is not correct. Create an NSG with deny inbound traffic on port 5585 and associate the NSG with Subnet1-2.

Step 1: Create NSG

Upper left side of the portal Search for Network Security Group

Put > Subscription > Resource Group > Name > Region

Tags

Review+Create

Step 2: Add Inbound Security  
Source > Any  
Port Range > \*  
Destination > IP address  
Destination IP address/CIDR Range > Range of Subnet1-2  
Service > Custom  
Destination Port Range > 5585  
Protocol > Any  
Action > Deny  
Priority > 100  
Name > DenyAnyCustom8080Inbound  
Add  
Step 3: Associate the NSG with the subnet  
Go to Virtual Network  
Select the Subnet1-2  
On NSG section > select the proper name of the NSG that you create earlier  
Save  
upvoted 3 times

✉️ **ABIGK** 2 weeks, 3 days ago

The lab is about creating NSG only, The NSG needs to deny traffic on port 5585 to the Subnet1-2. The image is not correct. Create an NSG with deny inbound traffic on port 5585 and associate the NSG with Subnet1-2.

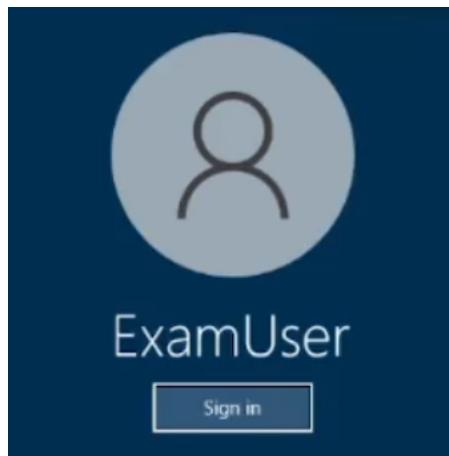
Step 1: Create NSG  
Upper left side of the portal Search for Network Security Group  
Put > Subscription > Resource Group > Name > Region  
Tags  
Review+Create  
Step 2: Add Inbound Security  
Source > Any  
Port Range > \*  
Destination > IP address  
Destination IP address/CIDR Range > Range of Subnet1-2  
Service > Custom  
Destination Port Range > 5585  
Protocol > Any  
Action > Deny  
Priority > 100  
Name > DenyAnyCustom8080Inbound  
Add  
Step 3: Associate the NSG with the subnet  
Go to Virtual Network  
Select the Subnet1-2  
On NSG section > select the proper name of the NSG that you create earlier  
Save

upvoted 2 times

✉️ **JohnAvlakiotis** 3 weeks, 5 days ago

The "Add inbound rule" image is misleading. The text above for the rule is correct.

upvoted 2 times

**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: xxxxxxxxx

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 only hosts on VNET1 can access the storage123456789 storage account. The solution must ensure that access occurs over the Azure backbone network.

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

#### Use private endpoints for Azure Storage

You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service. Network traffic between the clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposure from the public internet.

Connect to a storage account using an Azure Private Endpoint  
Create a private endpoint

Step 1: In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.

Step 2: Locate and select the Storage Account storage123456789

Step 3: Select the Networking tab or select Next: Advanced then Next: Networking.

**Correct Answer:** Step 4: In the Networking tab, under Network connectivity select Disable public access and use private access.

Step 5: In Private endpoint, select + Add private endpoint.

Step 6: In Create private endpoint enter or select the following information:  
\*Details omitted\*

\* Virtual network: Select VNET1.

Step 7: Select OK.

Step 8: Select Review.

Step 9: Select Create.

#### Reference

<https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

<https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal>

 **MrIMG** 1 month, 4 weeks ago

You can also use Service Endpoints:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?toc=%2Fazur...>

+

You need Service Endpoints Policies:

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview>  
upvoted 3 times

 **Ben\_88** 1 week, 1 day ago

The only condition is that the traffic stays in the backbone (not specifically in the vnet) so yeah service endpoint fits too  
upvoted 2 times

 **JohnAvlakiotis** 3 weeks, 5 days ago

This should be the only solution as it states that the access should happen over the Azure backbone. Service Endpoint is the correct option.  
upvoted 2 times

**HOTSPOT**

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

You create a NAT gateway named NATgateway1 as shown in the following exhibit.

## Create network address translation (NAT) gateway ...

 Validation passed

[Basics](#)   [Outbound IP](#)   [Subnet](#)   [Tags](#)   [Review + create](#)

**Basics**

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

**Outbound IP**

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

**Subnets**

Virtual network	Vnet1
Subnets	None

**Tags**

None

---

[Create](#)   [< Previous](#)   [Next >](#)   [Download a template for automation](#)

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

NOTE: Each correct selection is worth one point.

## Answer Area

NATgateway1 can be linked to [answer choice].

only GatewaySubnet
only Subnet1 or Subnet2
both Subnet1 and Subnet2
only Vnet1

NATgateway1 is assigned [answer choice].

0 IP addresses
1 IP addresses
2 IP addresses
16 IP addresses
28 IP addresses

## Answer Area

NATgateway1 can be linked to [answer choice].

only GatewaySubnet
only Subnet1 or Subnet2
both Subnet1 and Subnet2
only Vnet1

Correct Answer:

NATgateway1 is assigned [answer choice].

0 IP addresses
1 IP addresses
2 IP addresses
16 IP addresses
28 IP addresses

 **khanda** 2 months, 1 week ago

Answer is correct.

upvoted 2 times

 **ESAJRR** 2 months, 1 week ago

Same Vnet add all SubNets.  
SUBNET 1 2 4 8 [16] 32 64 128 256

HOST 256 128 64 32 [16] 8 4 2 1  
MASK /24 /25 /26 /27 [/28]/29 /30 /31 /32

upvoted 2 times

 **sunsetblvdfightclub** 2 months, 2 weeks ago

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/faq#can-nat-gateway-be-attached-to-multiple-subnets>  
upvoted 4 times

 **MrBlueSky** 2 months, 2 weeks ago

NAT Gateway can be associated to multiple subnets as long as they are in the same VNET.

The (28) indicates that the public IP prefix is a /28, which allows 16 IP addresses.

Correct answer

upvoted 4 times

**HOTSPOT**

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

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

You need to publish App1 by using AG1 and a URL of <https://app1.contoso.com>. The solution must meet the following requirements:

- TLS connections must terminate on AG1.
- Minimize the number of targets in the backend pool of AG1.
- Minimize the number of deployed copies of the SSL certificate of App1.

How many locations should you import to the certificate, and how many targets should you add to the backend pool of AG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Certificates:

1  
 2  
 3  
 4  
 5

Backend pool targets:

1  
 2  
 3  
 4

**Answer Area**

Certificates:

1  
 2  
 3  
 4  
 5

Correct Answer:

Backend pool targets:

1  
 2  
 3  
 4

 **seth\_saurabh84** Highly Voted 2 months, 2 weeks ago

why not 1 and 1? VMSS itself can be a backend target and not the 4 VM's making the VMSS. Certificate can come from Key Vault.

upvoted 19 times

 **\_fvt** 2 months, 2 weeks ago

Agrees

upvoted 3 times

✉  **crypto700** Highly Voted 1 month, 4 weeks ago

correct answer 1 & 1

upvoted 5 times

✉  **cloudselflearner** Most Recent 2 months ago

Correct answer 1-1

upvoted 4 times

**HOTSPOT**

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 has a /24 IPv4 address space.

You need to subdivide Vnet1. The solution must maximize the number of usable subnets.

What is the maximum number of IPv4 subnets you can create, and how many usable IP addresses will be available per subnet? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Usable IP addresses:

1  
3  
7

IPv4 subnets:

16  
32  
64  
128

**Answer Area**

Correct Answer:

Usable IP addresses:

1  
**3**  
7

IPv4 subnets:

16  
**32**  
64  
128

✉  **bakamon** 2 weeks, 4 days ago

Answer :

3

32

sidhi baat no bakwas

upvoted 2 times

✉  **xamkiller** 1 month, 2 weeks ago

This was on 24/04/2023

upvoted 2 times

✉  **Himank20** 1 month, 3 weeks ago

Correct.

Using a /24 will give us 256 IPs. Now, In azure we can create a minimum subnet of /29 which gives us 8 IPs per subnet. Dividing 256/8 we get 32 thus we can have 32 IPv4 subnets. Out of each these subnets 5 IP from them will be used by azure so number of usable IP in each subnet is 3.

upvoted 4 times

✉  **twaller78** 2 months ago

Correct. /24 gives you 256 ip addresses. Divide that by 32 is 8. Take off 5 ip addresses that azure reserves gives 3 usable ip's

upvoted 1 times

✉  **khanda** 2 months, 1 week ago

Answer is correct.

Azure can allow a minimum mask of /29, which gives you 6 usable IP's and Azure reserves the first 3 which leaves you with 3 IP's. You can have 32 /29 from a /24. This does require some networking subnetting skill. Hop on to --> <https://www.freecodecamp.org/news/subnet-cheat-sheet-24-subnet-mask-30-26-27-29-and-other-ip-address-cidr-network-references/>

upvoted 1 times

✉️ **Lapiduse** 2 months, 2 weeks ago

Correct !

upvoted 1 times

✉️ **seth\_saurabh84** 2 months, 2 weeks ago

Can someone explain the logic of the answer here?

upvoted 1 times

✉️ **Lapiduse** 2 months, 2 weeks ago

Azure Reserves 3 addresses for itself.

The first and last are the network address and the broadcast

Total 5 addresses. Hence the minimum mask /29. Amount of a Class C 32

upvoted 1 times

✉️ **\_fvt** 2 months, 2 weeks ago

a VNet with a /24 ip space can be splitted to multiple /29 subnets.

So it's 32 /29 subnets for a /24 VNet.

/29 have 6 Hosts IP Free, but Azure reserve the 4 first IP addresses so you have only 2 usable Addresses. That's also why you cannot split to /30 subnets (not enough IP addresses per subnet for Azure).

So the answer is 32 and 2. (<https://jodies.de/ipcalc?host=192.168.0.1&mask1=24&mask2=29>)

upvoted 1 times

✉️ **\_fvt** 2 months, 2 weeks ago

Sorry Azure reserves only firsts 3 IP Addresses (5 if you count the Network and Broadcast IP) (<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq>)

So the answer is well 32 and 30

upvoted 1 times

✉️ **\_fvt** 2 months, 2 weeks ago

32 and 3

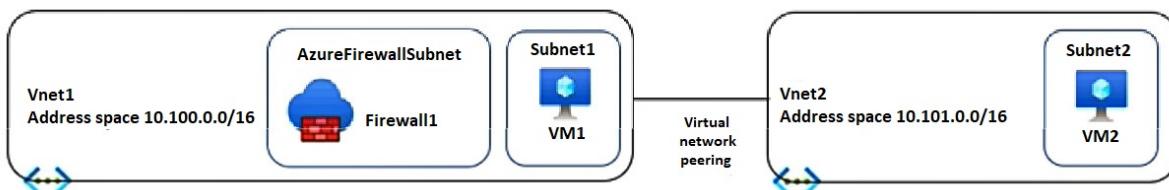
upvoted 2 times

## 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.

Setting	Value
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

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 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 checked="" type="radio"/>
Correct Answer:	The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall1.	<input checked="" type="radio"/>	<input type="radio"/>
	Firewall1 can be configured to limit access to websites by categories.	<input checked="" type="radio"/>	<input type="radio"/>

 **\_fvt**  2 months, 2 weeks ago

Should be YNY

Y - 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>)

N - The firewall is not a VPN Gateway, and we do not have any connection with On-Premises here (<https://learn.microsoft.com/en-us/answers/questions/516530/how-to-set-up-a-multi-spoke-virtual-network-in-azu>)

Y - Azure Firewall can filter by web categories (<https://learn.microsoft.com/en-us/azure/firewall/web-categories>)  
upvoted 21 times

 **TheBigMan**  2 weeks, 4 days ago

Think it should be NNN

- 1) Question is about gateway nor UDR
- 3) Firewall is standard, only premium has categories

upvoted 1 times

 **KyleHodg** 3 weeks, 1 day ago

The Firewall SKU states standard. Wouldn't Premium be required for filtering by category? Meaning YNN?

upvoted 4 times

 **Apptech** 1 week, 2 days ago

Standard SKU supports category filtering. "Azure Firewall Standard is recommended for customers looking for Layer 3–Layer 7 firewall and needs autoscaling to handle peak traffic periods of up to 30 Gbps. It supports enterprise features like threat intelligence, DNS proxy, custom DNS, and web categories." <https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku>

upvoted 2 times

 **occupatissimo** 3 weeks, 2 days ago

question ask for a routing table, not for a udr, be aware ....NNY

upvoted 2 times

 **khandा** 2 months, 1 week ago

Answer should be YNY, see @\_fvt comment.

upvoted 1 times

 **ckyap** 2 months, 1 week ago

YNN -

Yes - routing table is required- Create a routing table, add a router - next hop type select Virtual Appliance and put the firewall1 local ip (<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal#create-a-default-route>)

No - Vnet1 and Vnet2 is not used for Virtual network gateway or route server, the remote gateway setting will be greyed out if you try to configure the settings in the Peering.

No - Network rule is prioritised before application rules thus application rules like website blocking will not be enforced(<https://learn.microsoft.com/en-us/training/modules/design-implement-network-security-monitoring/6-azure-firewall#:~:text=Outbound%20connectivity%20using%20network%20rules%20and%20application%20rules>)

upvoted 1 times

 **ajinkyap** 2 months, 1 week ago

it should be YNY

upvoted 3 times

**HOTSPOT**

Your company has 40 branch offices across North America and Europe.

You have an Azure subscription that contains the following virtual networks:

- Two networks in the East US Azure region
- Three networks in the West Europe Azure region

You need to implement Azure Virtual WAN. The solution must meet the following requirements:

- Each branch office in North America must have an ExpressRoute circuit and a Site-to-Site VPN that connects to the East US region.
- Each branch office in Europe must have an ExpressRoute circuit and a Site-to-Site VPN that connects to the West Europe region.
- Transitive connections must be supported between all the branch offices and all the virtual networks.
- Costs must be minimized.

What is the minimum number of Virtual WAN resources required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Virtual WAN:

Virtual WAN:

- One Basic virtual WAN
- One Standard virtual WAN
- Two Basic virtual WANs
- Two Standard virtual WANs

Virtual WAN hub:

Virtual WAN hub:

- One virtual WAN hub
- Two virtual WAN hubs
- Four virtual WAN hubs
- Five virtual WAN hubs

Virtual network gateway:

Virtual network gateway:

- One virtual network gateway
- Two virtual network gateways
- Four virtual network gateways
- Five virtual network gateways

## Answer Area

Virtual WAN:

One Basic virtual WAN  
One Standard virtual WAN  
Two Basic virtual WANs  
**Two Standard virtual WANs**

Virtual WAN hub:

Correct Answer:

One virtual WAN hub  
Two virtual WAN hubs  
Four virtual WAN hubs  
**Five virtual WAN hubs**

Virtual network gateway:

One virtual network gateway  
**Two virtual network gateways**  
Four virtual network gateways  
Five virtual network gateways

✉ **MrBlueSky** Highly Voted 2 months ago

1 Standard VWAN (all hubs can be connected globally across regions with Standard VWAN)

2 VHUBS (one for each region)

4 Gateways (1 ER Gateway in US, 1 VPNGW in US + 1 ER Gateway in Europe + 1 VPNGW in Europe)

upvoted 10 times

✉ **xamkiller** 1 month, 2 weeks ago

Appreciate the proper explanation.

vHUB regional based

VPN and ER need separate gateways (per vHUB)

upvoted 2 times

✉ **stack12056** Highly Voted 2 months, 2 weeks ago

"When multiple hubs are enabled in a single virtual WAN, the hubs are automatically interconnected via hub-to-hub links, thus enabling global connectivity between branches and Vnets that are distributed across multiple regions."

ref: <https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-global-transit-network-architecture>

1 wan 2 hubs . 2 gateways

each gateway supporting the vpn connections to the offices

upvoted 9 times

✉ **BenyIR** 2 months, 2 weeks ago

it shouldnot be 4 gateways ? since it is said that needs Express route and VPN ? I mean 2 gateways in one hub or to configure both express route and vpn one gateway is enough ?

upvoted 5 times

✉ **\_fvt** 2 months, 2 weeks ago

Yes I agree

upvoted 1 times

✉ **bakamon** Most Recent 2 weeks, 6 days ago

: One standard virtual WAN

: 2 hubs

: 4 gateways

upvoted 2 times

✉ **Qunlay** 1 month, 3 weeks ago

1 Standard VWAN, 2 VHubs, 5 VPNGWs

upvoted 2 times

✉ **Chief\_D11** 2 months ago

To meet the requirements, you need to create a minimum of 1 Virtual WAN resource, 2 Virtual WAN hubs (one in the East US region and one in the West Europe region), and 5 virtual network gateways (one for each virtual network). Each branch office will connect to the nearest Virtual WAN hub using an ExpressRoute circuit and a Site-to-Site VPN. The Virtual WAN hubs will provide transitive connectivity between all the branch offices and all the virtual networks. The virtual network gateways will be used to connect the virtual networks to the Virtual WAN hubs. This solution minimizes costs by using a single Virtual WAN resource and by connecting each branch office to the nearest Virtual WAN hub.

upvoted 2 times

✉ **khanda** 2 months, 1 week ago

1 Standard vWAN  
2 Hubs, one for each region  
4 NGWs, which is two on each region, because ER and VPN cant coexist on one gateway.  
upvoted 3 times

 **manny72** 2 months, 1 week ago

1 Standard VWan - more hubs can coexist in a VWan - <https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-faq>

2 Hubs, one for each region.

2 GWs - Express Route and VPN GWs can coexist in a Standard VWan - <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>  
upvoted 4 times

 **silvarohit** 2 months, 1 week ago

Standard Virtual WAN - 1  
Hub - 2  
VPN GW - 4  
upvoted 4 times

 **MrBlueSky** 2 months, 2 weeks ago

It's definitely one Standard VWAN and 2 hubs.

The question is can a single VNET Gateway support both an ExpressRoute connection and a S2S connection simultaneously? While it doesn't explicitly address this, the documentation seems to suggest that they each need their own Gateway: <https://learn.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>

upvoted 5 times

**DRAG DROP**

You have a DNS domain named contoso.com that is hosted by a third-party domain name registrar.

You have an Azure subscription.

You need to ensure that all DNS queries for the contoso.com domain are resolved by using Azure DNS.

What should you create in the registrar, and what should you create in Azure? 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	Answer Area
A delegation	Registrar:
A DNS subdomain	option
A forwarder	Azure:
A primary DNS zone	option
A private DNS zone	
A public DNS zone	
A secondary DNS zone	

Answer Area	
Correct Answer:	Registrar: A delegation
	Azure: A public DNS zone

  **vigklk** 1 month ago

is it correct?

upvoted 2 times

  **khksoma** 1 month ago

Yes. Delegate, create zone and then modify NS records

upvoted 2 times

**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	<i>None</i>
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 Area****Correct Answer:**

Connection to Vnet1:

Microsoft peering  
**Private peering**  
Public peering  
Virtual network peering

Connection to SQL1:

**Microsoft peering**  
Private peering  
Public peering  
Virtual network peering

 **UR** Highly Voted 1 month, 1 week ago

The answer is correct!

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

upvoted 6 times

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. storage account
- B. internal load balancers
- C. service endpoints
- D. virtual network peering

**Correct Answer:** B

 **UR** 1 month, 1 week ago

The answer is correct.

B

upvoted 3 times

You have the on-premises networks shown in the following table.

Name	ASN	IP address space	Connection type	Description
Branch1	64551	10.50.0.0/24, 10.61.0.0/16	VPN	Is an on-premises datacenter
Branch2	64551	10.50.0.0/16, 10.61.0.0/16	VPN and ExpressRoute	AS Path has a prefix of 64551, 64551, 64551
Branch3	64551	10.50.2.0/24, 10.61.0.0/16	ExpressRoute	None

You have an Azure subscription that contains an Azure virtual WAN named VWAN1 and a virtual network named VNet1. VWAN is connected to the on-premises networks and VNet1 in a full mesh topology. The virtual hub routing preference for VWAN1 is AS Path.

You need to route traffic from VNet1 to 10.61.1.5.

Which path will be used?

- A. the VPN connection to Branch1
- B. the VPN connection to Branch2
- C. the ExpressRoute connection to Branch2
- D. the ExpressRoute connection to Branch3

**Correct Answer: B**

crypto700 Highly Voted 1 month, 1 week ago

**Selected Answer: D**

D- Branch3  
for two reasons

1- VWAN prefers ER over VPN  
2- it doesn't have BGP prepend .. Branch 2 has three AS hops so it is less preferred  
upvoted 11 times

roshingrg Most Recent 1 week, 6 days ago

B. the VPN connection to Branch2

The AS Path routing preference in the virtual hub (VWAN1) will determine the path selection. In this case, the AS Path for Branch2 includes a prefix of ExpressRoute (64551, 64551, 64551), indicating that traffic should be routed through the ExpressRoute connection to Branch2. However, the VPN connection to Branch2 has a more specific IP address space (10.50.0.0/16) than the ExpressRoute connection to Branch3 (10.50.2.0/24). Since the destination IP address (10.61.1.5) falls within the IP address space of the VPN connection to Branch2, the traffic will be routed through the VPN connection to Branch2.

Therefore, the correct path for routing traffic from VNet1 to 10.61.1.5 is the VPN connection to Branch2.

upvoted 2 times

roshingrg 1 week, 6 days ago

Apologies for the confusion in my previous response. Let's reassess the routing based on the updated information:

Given the following information:

Branch1: 64551, 10.50.0.0/24, VPN

Branch2: 64551, 10.50.0.0/16, VPN, AS Path has a prefix of ExpressRoute (64551, 64551, 64551)

Branch3: 64551, 10.50.2.0/24, 10.61.0.0/16, ExpressRoute

You need to route traffic from VNet1 to 10.61.1.5.

In this case, the AS Path for Branch2 includes a prefix of ExpressRoute, indicating that traffic can be routed through the ExpressRoute connection to Branch2. However, the destination IP address (10.61.1.5) does not fall within the IP address spaces of Branch1 or Branch2.

Branch3 has an IP address space (10.61.0.0/16) that includes the destination IP address (10.61.1.5). Although Branch3 is connected via ExpressRoute and doesn't have an AS Path, the destination IP address matches its IP address space.

Therefore, the correct path for routing traffic from VNet1 to 10.61.1.5 is:

D. the ExpressRoute connection to Branch3

upvoted 2 times

 **Kipper\_2022** 1 month ago

**Selected Answer: D**

Agree with crypto700

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure application gateway that has Azure Web Application Firewall (WAF) enabled.

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

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

```
{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
  "operationName": "ApplicationGatewayFirewall",
  "category": "ApplicationGatewayFirewallLog",
  "properties": {
    "instanceId": "appgw_0",
    "clientIp": "137.135.10.24",
    "clientPort": "",
    "requestUri": "/login",
    "ruleSetType": "OWASP_CRS",
    "ruleSetVersion": "3.0.0",
    "ruleId": "920300",
    "message": "Request Missing an Accept Header",
    "action": "Matched",
    "site": "Global",
    "details": {
      "message": "Warning. Match of \\"pm AppleWebKit Android\\" against \\"REQUEST_HEADER:User-Agent\\" required. ",
      "data": "",
      "file": "rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "appl.contoso.com",
    "transactionId": "f7546159ylhjk7wa114568if5131t68h7",
    "policyId": "default",
    "policyScope": "Global",
    "policyScopeName": "Global",
  }
}
```

You need to ensure that the URL is accessible through the application gateway from any IP address.

Solution: You configure a custom cookie and an exclusion rule.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

The log shows that WAF rule with ruleId 920300 was triggered. Instead we should disable the WAF rule that has a ruleId 920300.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot>

✉  **khanda** 2 months, 1 week ago

**Selected Answer: B**

Correct, disable the matched rule. False positive.

upvoted 1 times

✉  **Rajan395** 4 months, 3 weeks ago

correct

upvoted 1 times

✉  **sshera** 5 months, 2 weeks ago

in exam 4jan23

upvoted 3 times

✉  **fisherx001** 6 months, 3 weeks ago

correct

upvoted 1 times

✉  **Shereenassaf984** 9 months, 1 week ago

correct

upvoted 2 times

HOTSPOT -

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

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

The subscription contains the subnets shown in the following table.

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

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

Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

The subscription contains the local network gateways shown in the following table.

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

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

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
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input type="radio"/>
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input type="radio"/>
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input type="radio"/>

Correct Answer:

### Answer Area

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection	<input checked="" type="radio"/>	<input type="radio"/>

Reference:

✉️  **jellybiscuit** Highly Voted 8 months, 3 weeks ago

The answers depend on some assumptions.

Is there actually a vpn gateway sitting in that gateway subnet?

If so, is it configured for BGP? If so, then...

N - all outbound traffic from VM2 is sent to the internet

N - by default, subnets within a vnet can communicate. (I'm assuming that a NSG isn't blocking)

Y - all outbound traffic from VM1 is sent to the VPN gateway

BGP eliminates the need for a local azure route table.

upvoted 25 times

✉️  **Ajdlifasudfo** 6 months, 2 weeks ago

VPN: You can, optionally use BGP. For details, see BGP with site-to-site VPN connections.

There is no mentioning of BGP so you can't simply assume we have it set up

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

upvoted 1 times

✉️  **kimalto452** Highly Voted 9 months, 2 weeks ago

incorrect, the answer is NYY

upvoted 25 times

✉️  **aklas** 1 month ago

No you're wrong. Given answer is correct. The subnets are in the same VNet so there is a local route between them which is more specific than 0.0.0.0

upvoted 3 times

✉️  **occupatissimo** Most Recent 1 month, 2 weeks ago

NNY

Third answer look at: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm>.

upvoted 1 times

✉️  **khanda** 2 months, 1 week ago

Correct answer: NNY

Check comments

upvoted 1 times

✉️  **DerekKey** 5 months, 1 week ago

No | No | Yes

Yes -> Forced tunneling is carried out by using a virtual private network (VPN) tunnel; this tunnel requires a default site, a local gateway where all the Azure Internet-bound traffic is redirected.

upvoted 6 times

✉️  **NoeHdzMII** 6 months, 2 weeks ago

Correct answer

N - all outbound traffic from VM2 is sent to the internet by default

N - the effective route table shows all the subnets on the same VNET as a more specific one than the default route and Gateway routes. So subnets within a vnet can communicate directly.

Y - all outbound traffic from VM1 is sent to the VPN gateway

upvoted 3 times

✉️  **Takloy** 6 months, 2 weeks ago

By New York Site-to-site- VPN Connection, I assume whenever the traffic hits the VPN Gateway from the default route in Route1. Am I right? so my answer is NYY

upvoted 1 times

✉️  **Edzor** 8 months ago

Given answer is correct, since New York local gateway is the default site (forced tunneling)

to the VPN <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm>

(GatewayDefaultSite)

upvoted 3 times

✉️  **DeepMoon** 8 months, 3 weeks ago

Given answers are wrong.

Don't think too hard in trying to draw a logical network diagram in your head.

Simply realize NY is 10.9.0.0 (not on any of the route tables).

So nothing is routed through the NY. All answers are

Q1: No

Q2: No  
Q3: No

upvoted 11 times

 **hom3sick** 8 months, 3 weeks ago

I agree, there is no default route towards NY  
upvoted 3 times

 **DeepMoon** 9 months ago

I have no idea of creating a logical diagram of this network. Can someone help me out here?  
Where is NY & Seattle relative to subnet1 & subnet 2.

My drawing would be

| Vnet1- boundary subnet1(vm1) | subnet2 (vm2) vnet1-boundary |

Which way is internet?

Which way is VirtualNetworkGateway?

Which way is NY

Which way is Seattle?

upvoted 2 times

 **AdityaGupta** 9 months ago

Given answers are correct.

upvoted 5 times

 **tkcltoh** 9 months ago

default route is 0.0.0.0/0 internet. RT1 route is UDR therefore VM1 to VM2 is communicates via VPN

upvoted 1 times

 **Prutser2** 8 months, 1 week ago

from subnet1 to subnet 2 (vm1 to VM2), uses intra vnet, as its a longer match, would not choose default gateway

upvoted 3 times

 **RollinDeep** 9 months, 2 weeks ago

NNY. VM1 to VM2 are routed within Vnet1. RT1 and RT2 define default routes.

upvoted 5 times

 **Cristoicach91** 9 months, 3 weeks ago

correct

upvoted 1 times

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**

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

Reference:

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

✉ **WorkHardBeProud** Highly Voted 1 year, 8 months ago

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

upvoted 9 times

✉ **crawfish** 1 year, 7 months ago

Answer is correct. Per the link, NAT cannot be associated to an IPv6 Public IP address or IPv6 Public IP Prefix. However, it can be associated to a dual stack subnet.

upvoted 20 times

✉ **Webfacat33** Most Recent 6 months, 1 week ago

**Selected Answer: A**

NAT doesn't support ipv6

upvoted 3 times

✉ **jellybiscuit** 8 months, 3 weeks ago

**Selected Answer: A**

This page confirms you can use standard SKU only

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

This page confirms that the address must be static, and that IPv6 is not supported

<https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses#at-a-glance>

upvoted 3 times

✉ **sandeepmalik** 8 months, 3 weeks ago

IP3 only.....as NAT gateway is compatible with Standard SKU for IPv4 only

A NAT gateway can't be associated to an IPv6 public IP address or IPv6 public IP prefix

In today exam Oct 2nd 2022

upvoted 2 times

✉ **AdityaGupta** 9 months ago

**Selected Answer: A**

NAT gateway is compatible with standard SKU public IP addresses or public IP prefix resources or a combination of both. You can use a public IP prefix directly or distribute the public IP addresses of the prefix across multiple NAT gateway resources. The NAT gateway will groom all traffic to the range of IP addresses of the prefix.

Basic resources, such as basic load balancer or basic public IPs aren't compatible with Virtual Network NAT. Basic resources must be placed on a subnet not associated to a NAT gateway. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway

upvoted 2 times

✉ **Alessandro365** 9 months ago

**Selected Answer: A**

IP3 only (standard/IPv4)

upvoted 1 times

 **jeffangel28** 10 months, 2 weeks ago

**Selected Answer: A**

IP3 only.

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

upvoted 2 times

 **zerocool114** 11 months, 2 weeks ago

on exam today

upvoted 1 times

 **Fearless90** 11 months, 3 weeks ago

**Selected Answer: A**

A. IP3 only

upvoted 3 times

 **Fearless90** 11 months, 3 weeks ago

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

Virtual Network NAT basics

A NAT gateway can't be associated to an IPv6 public IP address or IPv6 public IP prefix. It can be associated to a dual stack subnet but will only be able to direct outbound traffic with an IPv4 address.

upvoted 1 times

 **Fearless90** 11 months, 3 weeks ago

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

Virtual Network NAT basics

Basic resources, such as basic load balancer or basic public IPs aren't compatible with Virtual Network NAT. Basic resources must be placed on a subnet not associated to a NAT gateway. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway

- To upgrade a basic load balancer to standard, see Upgrade a public basic Azure Load Balancer.
- To upgrade a basic public IP to standard, see Upgrade a public IP address.

upvoted 1 times

 **Fearless90** 11 months, 3 weeks ago

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

Virtual Network NAT basics

Virtual Network NAT is compatible with standard SKU public IP addresses or public IP prefix resources or a combination of both. You can use a public IP prefix directly or distribute the public IP addresses of the prefix across multiple NAT gateway resources. The NAT gateway will groom all traffic to the range of IP addresses of the prefix.

upvoted 1 times

 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam 6/28/22

upvoted 1 times

 **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

 **milan92stankovic** 1 year ago

**Selected Answer: A**

Only Standard Static IPv4 can be used. The answer is correct.

upvoted 1 times

 **Edward1** 1 year, 2 months ago

Is correct:

\*Basic resources, such as basic load balancer or basic public IPs aren't compatible with Virtual Network NAT. Basic resources must be placed on a subnet not associated to a NAT gateway. Basic load balancer and basic public IP can be upgraded to standard to work with a NAT gateway

\*A NAT gateway can't be associated to an IPv6 public IP address or IPv6 public IP prefix. It can be associated to a dual stack subnet

upvoted 3 times

 **bmulvIT** 1 year, 3 months ago

on exam 3/3/2022

upvoted 1 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **d0bermannn** 1 year, 4 months ago

**Selected Answer: A**

A. IP3 only [std sku & ipv4]

upvoted 2 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

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

You deploy another virtual machine scale set named VMSS2.

You need to configure AGW1 to direct all traffic for <http://www.adatum.com> to VMSS2.

The solution must ensure that requests to <http://www.contoso.com> continue to be directed to Pool1.

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

NOTE: Each correct selection is worth one point.

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

**Correct Answer: ADE**

Reference:

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

✉  **RickMorais** Highly Voted 1 year, 8 months ago

Correct

You need a backend for VMSS2, a listener for the site adatum.com and a rule to redirect the request from the listener to backend VMSS2  
upvoted 66 times

✉  **jeffangel28** 10 months, 2 weeks ago

Right!

upvoted 1 times

✉  **AidenYoukhana** 1 year, 5 months ago

THANKS!

upvoted 1 times

✉  **crawfish** 1 year, 7 months ago

perfect explanation

upvoted 3 times

✉  **JoMa** 1 year, 6 months ago

simple and perfect explanation

upvoted 2 times

✉  **Rajan395** Most Recent 4 months, 3 weeks ago

correct answer!

upvoted 1 times

✉  **TJ001** 5 months ago

HTTP setting can be common(if the same type of setting) across rules is important understand...

upvoted 1 times

✉  **AdityaGupta** 9 months ago

**Selected Answer: ADE**

Correct Answer, you don't have to modify or add HTTP setting.

upvoted 1 times

✉  **tartarus23** 11 months, 2 weeks ago

**Selected Answer: ADE**

A. Add a backend pool. | D. Add a listener. | E. Add a rule.

VMSS2 is newly created and would need a backend pool. AGW needs to listen to HTTP traffic and forward the HTTP requests based on the rules for VMSS1 Pool1 or VMSS2 Pool2 as per the question.

upvoted 3 times

✉  **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **d0bermannn** 1 year, 4 months ago

**Selected Answer: ADE**

ADE is correct

upvoted 2 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

 **KranthiChaitanya** 1 year, 4 months ago

Came on exam 28/Jan/22

upvoted 1 times

 **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022

upvoted 1 times

 **Pravda** 1 year, 5 months ago

Variation on exam 1/6/2022

upvoted 3 times

**HOTSPOT -**

You have an Azure Traffic Manager parent profile named TM1. TM1 has two child profiles named TM2 and TM3. TM1 uses the performance traffic-routing method and has the endpoints shown in the following table.

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

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

Name	Location	Weight
App4	West Europe	99
App5	West Europe	1

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

Name	Location
App6	West US
App2	East US

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

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

NOTE: Each correct selection is worth one point

Hot Area:

**Answer Area**

Traffic from West Europe:

	▼
App1	
App2	
App4	
App5	

Traffic from West US:

	▼
App1	
App2	
App3	
App6	

## Answer Area

Correct Answer:

Traffic from West Europe:

App1
App2
App4
App5

Traffic from West US:

App1
App2
App3
App6

Reference:

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

✉️  **crawfish** Highly Voted 1 year, 7 months ago

Traffic from West Europe:

Based on TM1 table, West Europe will trigger TM2. However, as the MinChildEndpoint is set to 2, and App4 is degraded (down), the entire TM2 will not be considered available.

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

Hence, Answer = App1

Traffic from West US:

Based on TM1 table, West US will trigger TM3. However, both App2 and App6 were degraded (down), so none of them can be considered.

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

Answer = App3

upvoted 191 times

✉️  **leotoronto123** 1 year, 5 months ago

MinChildEndpoint:

Gets or sets the minimum number of endpoints that must be available in the child profile in order for the parent profile to be considered available. Only applicable to endpoint of type 'NestedEndpoints'.

my question is here the value is 2. should it consider App5 before going to parent and considering APP1?

upvoted 2 times

✉️  **JohnnyChimpo** 1 month, 3 weeks ago

Thanks for explaining this

upvoted 1 times

✉️  **teamaws** 1 year, 7 months ago

Brilliant explanation, learned a lot from that and the documentation: <https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-faqs#how-does-traffic-manager-compute-the-health-of-a-nested-endpoint-in-a-parent-profile>

upvoted 8 times

✉️  **jeffangel28** 10 months, 2 weeks ago

Right! Official document by the way... <https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles>

upvoted 2 times

✉️  **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 3 times

✉️  **Rajan395** 4 months, 3 weeks ago

correct answer

upvoted 2 times

✉️  **sshera** 5 months, 2 weeks ago

in exam 4jan23

upvoted 1 times

✉️  **Andersonalm** 6 months, 3 weeks ago

Correct!  
upvoted 1 times

-  **Stanley3427** 1 year ago  
App5 and App3 is correct  
upvoted 1 times
-  **geuser** 7 months, 1 week ago  
it cannot be App5 because MinChildEndpoint = 2 not 1 (which is default).  
upvoted 2 times
-  **bebop** 8 months, 2 weeks ago  
How come?  
upvoted 1 times
-  **bmulvIT** 1 year, 3 months ago  
On exam today 3/3/2022  
upvoted 2 times
-  **rockethack** 1 year, 3 months ago  
This question was on the exam on 18th Feb 2022.  
upvoted 2 times
-  **Kimimoto** 1 year, 4 months ago  
Appeared in exam on 11/Feb/2022  
upvoted 1 times
-  **KranthiChaitanya** 1 year, 4 months ago  
Came on exam 28/Jan/22  
upvoted 2 times
-  **sallymaher** 1 year, 4 months ago  
i though the TM doesn't have a location and it is a global service , how come they mentioned locations for the TMs !!!!  
upvoted 2 times
-  **Contactfornitish** 1 year, 5 months ago  
Appeared in exam on 17/01/2022  
upvoted 1 times
-  **Pravda** 1 year, 5 months ago  
Not on exam 1/6/2022  
upvoted 2 times
-  **aftab7500** 1 year, 6 months ago  
Nested Traffic Manager profiles  
<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles>  
upvoted 1 times
-  **Bharat** 1 year, 8 months ago  
Well explained in the provided link. Answers are correct  
upvoted 4 times
-  **sliksl** 1 year, 8 months ago  
It should be App5 and App3.  
upvoted 3 times
-  **Roman\_Rabodzey** 1 year, 8 months ago  
There is traffic-routing method with MinChildEndpoint = 2. The parameter determines the minimum number of available endpoints in the child profile. So the parent profile considers the entire child profile to be unavailable and directs traffic to the other endpoints.  
upvoted 14 times

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

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

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

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

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

```
{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
  "operationName": "ApplicationGatewayFirewall",
  "category": "ApplicationGatewayFirewallLog",
  "properties": {
    "instanceId": "appgw_0",
    "clientIp": "137.135.10.24",
    "clientPort": "",
    "requestUri": "/login",
    "ruleSetType": "OWASP CRS",
    "ruleSetVersion": "3.0.0",
    "ruleId": "920300",
    "message": "Request Missing an Accept Header",
    "action": "Matched",
    "site": "Global",
    "details": {
      "message": "Warning. Match of \\"pm AppleWebKit Android\\" against \\"REQUEST_HEADER:User-Agent\\" required. ",
      "data": "",
      "file": "rules\REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "appl.contoso.com",
    "transactionId": "f7546159y1hjk7wall14568if513lt68h7",
    "policyId": "default",
    "policyScope": "Global",
    "popolicyScopeName": "Global",
  }
}
```

You need to ensure that the URL is accessible through the application gateway from any IP address.

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

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

The log shows that WAF rule with ruleId 920300 was triggered. Instead we should disable the WAF rule that has a ruleId 920300.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot>

✉ **Rajan395** 4 months, 3 weeks ago

correct answer!

upvoted 2 times

✉ **caliph\_noman** 5 months ago

**Selected Answer: B**

correct

upvoted 1 times

✉ **sshera** 5 months, 2 weeks ago

in exam 4jan23

upvoted 3 times

✉ **Andersonalm** 6 months, 3 weeks ago

Correct!

upvoted 3 times

✉ **ghmymmnvhvtltkwiz** 7 months, 2 weeks ago

sdfsdfsd

upvoted 2 times

**HOTSPOT -**

You have an Azure Front Door instance that provides access to a web app. The web app uses a hostname of www.contoso.com. You have the routing rules shown in the following table.

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

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

NOTE: Each correct selection is worth one point

Hot Area:

**Answer Area**

www.contoso.com/abc/def

▼
RuleA
RuleB
RuleC
RuleD

www.contoso.com/default.htm

▼
RuleA
RuleB
RuleC
RuleD

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

▼
RuleA
RuleB
RuleC
RuleD

**Answer Area**

www.contoso.com/abc/def

▼
RuleA
RuleB
RuleC
RuleD

www.contoso.com/default.htm

▼
RuleA
RuleB
RuleC
RuleD

Correct Answer:

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

▼
RuleA
RuleB
RuleC
RuleD

Reference:

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

✉ **Pravda** Highly Voted 1 year, 6 months ago

Look for any routing rule with an exact match on the Path  
If no exact match Paths, look for routing rules with a wildcard Path that matches  
If no routing rules are found with a matching Path, then reject the request and return a 400: Bad Request error HTTP response.  
upvoted 27 times

✉ **Sarvajanik** Highly Voted 1 year, 6 months ago

Longest match is the correct answer.  
upvoted 8 times

✉ **Rajan395** Most Recent 4 months, 3 weeks ago

correct answer  
upvoted 1 times

✉ **sshera** 5 months, 2 weeks ago

in exam 4jan23  
upvoted 4 times

✉ **Andersonalm** 6 months, 3 weeks ago

Correct answer  
upvoted 1 times

✉ **naidu** 9 months, 3 weeks ago

Correct Answer  
upvoted 1 times

✉ **jeffangel128** 10 months, 2 weeks ago

Right!  
upvoted 1 times

✉ **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.  
upvoted 1 times

✉ **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022  
upvoted 1 times

✉ **sleekdunga** 1 year, 4 months ago

RuleA/RuleC & RuleD  
upvoted 6 times

✉ **KranthiChaitanya** 1 year, 4 months ago

Came on exam 28/Jan/22  
upvoted 1 times

✉ **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022  
upvoted 1 times

✉ **Pravda** 1 year, 5 months ago

Not on exam 1/6/2022  
upvoted 1 times

✉ **AidenYoukhana** 1 year, 5 months ago

CORRECT ANSWER.  
upvoted 2 times

✉ **teamaws** 1 year, 7 months ago

correct, <https://docs.microsoft.com/en-us/azure/frontdoor/standard-premium/concept-route#path-matching>  
upvoted 3 times

✉ **RickMorais** 1 year, 8 months ago

Correct.  
upvoted 6 times

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

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

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

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

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

```
{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceID": "/SUBSCRIPTIONS/489f2ht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
  "operationName": "ApplicationGatewayFirewall",
  "category": "ApplicationGatewayFirewallLog",
  "properties": {
    "instanceId": "appgw_0",
    "clientIp": "137.135.10.24",
    "clientPort": "",
    "requestUri": "/login",
    "ruleSetType": "OWASP_CRS",
    "ruleSetVersion": "3.0.0",
    "ruleId": "920300",
    "message": "Request Missing an Accept Header",
    "action": "Matched",
    "site": "Global",
    "details": {
      "message": "Warning. Match of \\"pm AppleWebKit Android\\" against \\"REQUEST_HEADER:User-Agent\\" required. ",
      "data": "",
      "file": "rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "app1.contoso.com",
    "transactionId": "f7546159ylhjk7wall4568if513lt68h7",
    "policyId": "default",
    "policyScope": "Global",
    "popolicyScopeName": "Global",
  }
}
```

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

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

Does this meet the goal?

A. Yes

B. No

**Correct Answer: A**

The log shows that WAF rule with ruleId 920300 was triggered. We should disable the WAF rule that has a ruleId 920300.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot>

**AidenYoukhana** Highly Voted 1 year, 5 months ago

Selected Answer: A

CORRECT ANSWER.

upvoted 9 times

**Rajan395** Most Recent 4 months, 3 weeks ago

correct answer

upvoted 1 times

**sshera** 5 months, 2 weeks ago

in exam 4jan23

upvoted 3 times

**Fearless90** 11 months, 3 weeks ago

Selected Answer: A

A. Yes

disable the WAF rule that has a ruleId 920300

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-diagnostics#firewall-log>

Value

action

Description

Action taken on the request. Available values are Blocked and Allowed (for custom rules), Matched (when a rule matches a part of the request), and Detected and Blocked (these are both for mandatory rules, depending on if the WAF is in detection or prevention mode).

upvoted 1 times

 **samers** 1 year ago

Matched for blocking that can be disabled ,while blocking for rules that can't be disabled "builtin"  
upvoted 1 times

 **sleekdunga** 1 year, 4 months ago

A correct Answer. Disabling the WAF Rule implies not match required for " specified header string"  
upvoted 3 times

 **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022  
upvoted 2 times

 **Pravda** 1 year, 5 months ago

Not on exam 1/6/2022  
upvoted 2 times

 **cooksiecooks** 1 year, 8 months ago

To be more precise, the action should be stated as "Blocked" rather "Matched" for accuracy purposes.  
upvoted 4 times

No - the action is well stated. The action is Blocked when it reaches the max anomaly count and trigger the non-disabled rule, from that rule you will see action "Blocked"

upvoted 9 times

You have an Azure subscription that contains an Azure App Service app. The app uses a URL of <https://www.contoso.com>. You need to use a custom domain on Azure Front Door for [www.contoso.com](http://www.contoso.com). The custom domain must use a certificate from an allowed certification authority (CA).

What should you include in the solution?

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

**Correct Answer: C**

Reference:

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

 **teamaws** Highly Voted 1 year, 7 months ago

Correct, use Key Vault with your own certificate

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https#option-2-use-your-own-certificate>

upvoted 9 times

 **walkwolf3** 1 year, 7 months ago

Your own certificate means the certificate is issued by a CA.

upvoted 5 times

 **AdityaGupta** Highly Voted 9 months ago

**Selected Answer: C**

The correct answer is C, but the explanation is - you must create a complete certificate chain with an allowed certificate authority (CA) that is part of the Microsoft Trusted CA List. And Azure Key Vault allows you to store your certificates securely. Azure Front Door uses this secure mechanism to get your certificate (Self Signed or CA Provided) and it requires a few extra steps.

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https#option-2-use-your-own-certificate>

upvoted 6 times

 **Jamesat** Most Recent 10 months, 1 week ago

**Selected Answer: C**

Keyvault is the correct answers as noted in the official docs

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

upvoted 1 times

 **zerocool114** 11 months, 2 weeks ago

on exam today

upvoted 2 times

 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam 6/28/22

upvoted 2 times

 **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

 **d0bermannn** 1 year, 3 months ago

**Selected Answer: C**

C. Azure Key Vault

upvoted 3 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 2 times

 **rockethack** 1 year, 4 months ago

Azure Key Vault is the correct answer

upvoted 1 times

 **Ben\_Dover2** 1 year, 4 months ago

**Selected Answer: C**

Azure Key Vault is the correct answer

upvoted 3 times

 **KranthiChaitanya** 1 year, 4 months ago

Came on exam 28/Jan/22

upvoted 1 times

 **Pravda** 1 year, 5 months ago

on exam 1/6/2022 - Order is different.

upvoted 2 times

 **Pravda** 1 year, 5 months ago

Option 2

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

upvoted 1 times

 **AidenYoukhana** 1 year, 5 months ago

AZURE KEY VAULT.

upvoted 1 times

 **crawfish** 1 year, 7 months ago

C - Azure Key Vault is the correct answer.

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

upvoted 3 times

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

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

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

What should you do?

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

**Correct Answer: D**

Reference:

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

 **Eitant** Highly Voted 1 year, 5 months ago

**Selected Answer: D**

The certificate is an enterprise certificate and not a public certificate so you must upload the root certificate to the Application Gateway.

There is no typo, it's HTTP settings.

<https://docs.microsoft.com/en-us/azure/application-gateway/self-signed-certificates#upload-the-root-certificate-to-application-gateways-http-settings>

upvoted 27 times

 **derrrp** 11 months ago

For anyone doing any last minute cramming for this exam, you've likely encountered this question several times now. I immediately remember this top-voted comment above from Eitant. (Thanks dude). Pointing out that it's "HTTP settings" not being a typo - even though we're actually dealing with HTTPS helps me to remember the answer. This is for the Enterprise generated cert whereas the other version of this question uses a legitimate Certificate Authority (CA) Good luck, ya'll.

upvoted 18 times

 **teamaws** Highly Voted 1 year, 7 months ago

Think there's a typo in answer D, should be HTTPS settings.

Under HTTPS Settings:

Choose a certificate - Select Upload a certificate.

<https://docs.microsoft.com/en-us/azure/application-gateway/create-ssl-portal#configuration-tab>

upvoted 12 times

 **Rajan395** Most Recent 4 months, 3 weeks ago

correct answer

upvoted 1 times

 **AdityaGupta** 9 months ago

**Selected Answer: D**

You need to upload .pfx file in Http Setting.

upvoted 1 times

 **naidu** 9 months, 3 weeks ago

D is the right answer

upvoted 1 times

 **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

 **Edward1** 1 year, 2 months ago

**Selected Answer: D**

The Answer is correct.

To create a new application gateway with end-to-end TLS encryption, you'll need to first enable TLS termination while creating a new application gateway. This action enables TLS encryption for communication between the client and application gateway. Then, you'll need to put on the Safe Recipients list the certificates for the back-end servers in the HTTP settings. This configuration enables TLS encryption for communication between the application gateway and the back-end servers. That accomplishes end-to-end TLS encryption.

upvoted 3 times

 **d0bermannn** 1 year, 3 months ago

Selected Answer: D

D. Upload the public key certificate to the HTTP settings  
upvoted 1 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.  
upvoted 1 times

 **viva6516** 1 year, 3 months ago

To ensure that the application gateway provide end-to-end encryption, SSL must be enabled

Answer - B

upvoted 2 times

 **KranthiChaitanya** 1 year, 4 months ago

Came on exam 28/Jan/22  
upvoted 1 times

 **Pravda** 1 year, 5 months ago

Not on exam 1/6/2022  
upvoted 2 times

 **dusty\_dev** 1 year, 6 months ago

little confused, documentation says first enable TLS and then upload cert to listener. Is option B incorrect because it says enable SSL instead of TLS?  
upvoted 2 times

 **Pravda** 1 year, 6 months ago

Web page does say to use HTTPS  
<https://docs.microsoft.com/en-us/azure/application-gateway/self-signed-certificates#upload-the-root-certificate-to-application-gateways-http-settings>  
upvoted 2 times

 **prepper666** 1 year, 7 months ago

Correct as described here: <https://docs.microsoft.com/en-us/azure/application-gateway/self-signed-certificates>. There is no need to upload if using a well-known certificate (public)  
upvoted 5 times

 **WorkHardBeProud** 1 year, 8 months ago

Perfect !  
Since the cx is using an enterprise cert which is not a public certificate that can check publicly, he needs to upload the root cert(.cer) on the HTTPS settings to help the AppGW recognize App1 in the backend.  
upvoted 6 times

**HOTSPOT -**

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

You have the NAT gateway shown in the NATgateway1 exhibit.

**NATgateway1** 

NAT gateway

»  Delete  Refresh

**^ Essentials**

Resource group ([change](#)) : RG1

Location : North Europe (Zone 1)

Subscription ([change](#)) : Subscription1

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

Virtual network : Vnet1

Subnets : 1

Public IP addresses : 0

Public IP prefixes : 1

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

[JSON View](#)

You have the virtual machine shown in the VM1 exhibit.

**VM1** 

Virtual machine

»  Connect  Start  Restart  Stop  Capture  Delete  Refresh

**^ Essentials**

Resource group ([change](#)) : RG1 Operating system : Windows

Status : Running Size : Standard B1s (1 vcpus, 1 GiB memory)

Location : North Europe (Zone 2) Public IP address

Subscription ([change](#)) : Subscription1 Virtual network/subnet : Vnet1/Subnet1

Subscription ID : 489f2hht-se7y-987v-g571-463hw3679512 DNS name

Availability zone : 2

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

Subnet1 is configured as shown in the Subnet1 exhibit.

## Subnet1

Vnet1

Name  
Subnet1

Subnet address range \* ⓘ

10.100.1.0 – 10.100.1.255 (251 + 5 Azure reserved addresses)

Add IPv6 address space ⓘ

NAT gateway ⓘ

Network security group

Route table

### SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

### SUBNET DELEGATION

Delegate subnets to a service ⓘ

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
VM1 can communicate outbound by using NATgateway1	<input type="radio"/>	<input type="radio"/>
The virtual machines in Subnet2 communicate outbound by using NATgateway1	<input type="radio"/>	<input type="radio"/>
All the virtual machines that use NATgateway1 to connect to the internet use the same public IP address	<input type="radio"/>	<input type="radio"/>

Correct Answer:

### Answer Area

Statements	Yes	No
VM1 can communicate outbound by using NATgateway1	<input type="radio"/>	<input checked="" type="radio"/>
The virtual machines in Subnet2 communicate outbound by using NATgateway1	<input checked="" type="radio"/>	<input type="radio"/>
All the virtual machines that use NATgateway1 to connect to the internet use the same public IP address	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

VM1 is in Zone2 whereas the NAT Gateway is in Zone1. The VM would need to be in the same zone as the NAT Gateway to be able to use it. Therefore, VM1 cannot use the NAT gateway.

Box 2: Yes -

NATgateway1 is configured in the settings for Subnet2.

Box 3: No -

The NAT gateway does not have a single public IP address, it has an IP prefix which means more than one IP address. The VMs the use the NAT Gateway can use different public IP addresses contained within the IP prefix.

Reference:

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

✉️  **AdityaGupta** Highly Voted 9 months ago

Correct Answer: - YNN

1) NAT gateway can provide outbound connectivity for virtual machines from other availability zones different from itself. The virtual machine's subnet needs to be configured to the NAT gateway resource to provide outbound connectivity. Additionally, multiple subnets can be configured to the same NAT gateway resource.

While virtual machines in subnets from different availability zones can all be configured to a single zonal NAT gateway resource, this configuration doesn't provide the most effective method for ensuring zone-resiliency against zonal outages.

2) Subnet2 is not configured with NatGateway, refer exhibit 1, Nat Gateway is associated with only 1 subnet. In exhibit 2 it shows that Subnet 1 is associated with that Nat Gateway.

3) In exhibit 1 it shows that NAT Gateway is configured with Public IP Prefix, and outbound connection can use any Public from that prefix. It is NOT necessary to use same (one) Public IP.

upvoted 53 times

✉️  **rac\_sp** 3 months, 3 weeks ago

your answers are top !

upvoted 1 times

✉️  **jellybiscuit** Highly Voted 8 months, 3 weeks ago

NNN

N - The nat gateway \*could have been\* created to support multiple zones, but it was not. A gateway supporting all zones does not show the zone in the location field.

VM1 is located in a different zone and as a result, cannot use Natgateway1.

N - Subnet2 is not configured to use Natgateway1.

--- The screenshot of vnet1 shows that it is using Natgateway1.

--- The screenshot of NATgateway1 shows a Subnet count of 1.

--- If Subnet2 was configured to use the gateway, the Subnet count would be at least two.

N - The gateway is using a public IP prefix (instead of a single public ip address) so communication will happen over various outbound addresses.

I know we hear "tested in the lab" all the time. I actually did. I built two gateways... one in a zone, one without. I built a vnet and two subnets, one configured with the natgateway and one without.

upvoted 8 times

✉️  **jellybiscuit** 8 months, 3 weeks ago

Changing my answer to YNN - sorry

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones#zonal>

I was misreading this documentation - or rather, not reading far enough down.

While it says this: "When NAT gateway is deployed to a specific zone, it will provide outbound connectivity to the internet explicitly from that zone. "

It also says this:

"NAT gateway can provide outbound connectivity for virtual machines from other availability zones different from itself. "

Seems to contradict itself.

upvoted 13 times

✉️  **Goofer** 5 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones#single-zonal-nat-gateway-resource-for-zone-spanning-resources>

upvoted 2 times

✉️  **sapien45** 8 months, 2 weeks ago

No contradiction here. YNN

It says that a ZONAL NAT gateway provides internet connectivity FROM a single zone.

It does not say TO a single zone. VMs in other zones can use that ZONAL nat gateway.

<https://azurecomcdn.azureedge.net/mediahandler/acomblog/media/Default/blog/809936d8-a658-465b-9085-f4bbae9b7e33.png>  
YNN

upvoted 4 times

 **Bill831231** 7 months, 3 weeks ago

seems there are two types of NAT GW deployment, zonal or regional  
upvoted 1 times

 **MightyMonarch74** (Most Recent) 2 months, 3 weeks ago

YNN - Confirmed via lab  
upvoted 2 times

 **sapien45** 8 months, 4 weeks ago

YNN  
If not Zonal NAT would have been deployed, multiple subnets can be configured to the same NAT gateway resource.  
<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource>  
upvoted 3 times

 **sapien45** 8 months, 2 weeks ago

NNN then as VM1 is not in the same zone as the zonal NATGTWAY  
upvoted 1 times

 **BlackZeros** 8 months, 4 weeks ago

Answer should be YNY.

Minimum number of PIP you need for Nat Gateway is 1 and maximum is 16.

It will work just like your home router where multiple devices are using same IP to go out. it is not one to one ratio. If Subnet1 has 50 VMs and you can only have 16 IP addresses in Nat gateway then there will be a problem (ip exhaustion) which is not the case here.

Nat Gateways can be assigned to multiple Subnets

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/faq#can-virtual-network-nat-gateway-be-attached-to-multiple-subnets>  
upvoted 3 times

 **MrHabanero** 9 months ago

YNN  
NAT GW is attached only to subnet1  
upvoted 3 times

 **charlesr1700** 9 months ago

YNN  
Agree with Tonys link, under the Zonal header it clearly states  
'NAT gateway can provide outbound connectivity for virtual machines from other availability zones different from itself'  
upvoted 1 times

 **TonyOmar** 9 months, 1 week ago

YNN  
for part 1 you can use NATgateway1 while your VM in different zone  
check: <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-availability-zones>  
upvoted 2 times

 **zenithcsa1** 9 months, 2 weeks ago

NNN  
Only Subnet1 is connected to NATgateway1.  
upvoted 2 times

 **zenithcsa1** 9 months, 2 weeks ago

YNN  
tested) VM in zone3 can use a NATGW in zone2. It does support outbound connectivity, while it does not guarantee availability from zone-failure.  
upvoted 6 times

 **Cristoicach91** 9 months, 3 weeks ago

NNN. VM and NAT gate are in different zones. Subnet 2 is not using NAT gateway. NAT gateway uses a public prefix.  
upvoted 3 times

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

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

What should you configure on AppGW1?

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

**Correct Answer: B**

Reference:

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

 **Sarvajanik** Highly Voted 1 year, 6 months ago

Application Gateway allows you to add, remove, or update HTTP request and response headers while the request and response packets move between the client and back-end pools.

Its correct

upvoted 17 times

 **derrp** Highly Voted 11 months ago

Cramming for this exam next week. Already seen this question countless times. As soon as I see anything that involves messing around with editing headers, I immediately think Rewrites. Hope this helps.

upvoted 13 times

 **iwikneerg** 10 months, 2 weeks ago

This is the best way to approach the more confusing questions because Microsoft can only rewrite their questions so many ways :)

upvoted 4 times

 **drprepper\_** 3 months, 1 week ago

Hahaha excellent, going to remember this answer now.

upvoted 1 times

 **Rajan395** Most Recent 4 months, 3 weeks ago

correct answer

upvoted 1 times

 **AdityaGupta** 9 months ago

**Selected Answer: B**

Correct answer is B - Rewrites.

upvoted 1 times

 **rac\_sp** 11 months, 1 week ago

**Selected Answer: B**

rewrite

upvoted 1 times

 **Edward1** 1 year, 2 months ago

**Selected Answer: B**

The Answer is correct

You use rewrite actions to specify the URL, request headers or response headers that you want to rewrite and the new value to which you intend to rewrite them to.

upvoted 2 times

 **d0bermannn** 1 year, 3 months ago

**Selected Answer: B**

B. rewrites

upvoted 1 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **Ben\_Dover2** 1 year, 4 months ago

**Selected Answer: B**

Rewriters for sure !

upvoted 2 times

✉ **Joshalom** 1 year, 4 months ago

on exam 6/2/2022

upvoted 1 times

✉ **Pravda** 1 year, 5 months ago

on exam 1/6/2022

upvoted 3 times

✉ **AidenYoukhana** 1 year, 5 months ago

REWRITES.

upvoted 1 times

✉ **Pravda** 1 year, 6 months ago

Question on exam 11/2021

upvoted 2 times

✉ **Aathithyan** 1 year, 7 months ago

Answer is correct

upvoted 3 times

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

All outbound traffic to the internet uses a NAT gateway.

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

You need to increase the available SNAT connections.

What should you do?

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

**Correct Answer: B**

Reference:

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

✉  **gme999** Highly Voted 1 year, 8 months ago

Correct. Evaluate if SNAT port exhaustion should be mitigated with additional IP addresses assigned to NAT gateway resource.  
<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#snat-exhaustion>

upvoted 20 times

✉  **Ajdifasudfo0** 6 months, 3 weeks ago

the url changed to <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat-connectivity>  
upvoted 3 times

✉  **leotoronto123** 1 year, 5 months ago

Correct Answer is B.  
Evaluate if SNAT port exhaustion should be mitigated with additional IP addresses assigned to NAT gateway resource.  
upvoted 4 times

✉  **wooyourdaddy** Most Recent 3 months, 1 week ago

Selected Answer: B

The first scenario in the table at this link.

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat-connectivity#nat-gateway-not-scaled-out-enough>

Scenario

You're experiencing contention for SNAT ports and SNAT port exhaustion during periods of high usage.

Evidence:

You run the following metrics in Azure Monitor: Total SNAT Connection Count: "Sum" aggregation shows high connection volume. For SNAT Connection Count, "Failed" connection state shows transient or persistent failures over time. Dropped Packets: "Sum" aggregation shows packets dropping consistent with high connection volume and connection failures.

Mitigation:

Add more public IP addresses or public IP prefixes as need (assign up to 16 IP addresses in total to your NAT gateway). This addition will provide more SNAT port inventory and allow you to scale your scenario further.

upvoted 2 times

✉  **samir111** 4 months ago

Selected Answer: B

The answer is B

upvoted 1 times

✉  **Rajan395** 4 months, 3 weeks ago

correct answer

upvoted 1 times

✉  **sapien45** 8 months, 4 weeks ago

Selected Answer: B

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

Add more public IP addresses or public IP prefixes as need (assign up to 16 IP addresses in total to your NAT gateway). This addition will provide more SNAT port inventory and allow you to scale your scenario further.

upvoted 1 times

✉  **AdityaGupta** 9 months ago

**Selected Answer: B**

Correct Answer is B

upvoted 1 times

✉  **iwikneerg** 10 months, 2 weeks ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#outbound-connectivity-not-scaled-out-enough>

Determine if you can add more public IP addresses or public IP prefixes. This addition will allow for up to 16 IP addresses in total to your NAT gateway. This addition will provide more inventory for available SNAT ports (64,000 per IP address) and allow you to scale your scenario further.

upvoted 1 times

✉  **zerocool114** 11 months, 2 weeks ago

on exam today, correct answer

upvoted 1 times

✉  **Fearless90** 11 months, 3 weeks ago

**Selected Answer: B**

B. Add a public IP address. > Do this first since 500 session hosts

A. Bind the NAT gateway to another subnet.

upvoted 1 times

✉  **Fearless90** 11 months, 3 weeks ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#snat-exhaustion-due-to-nat-gateway-configuration>  
SNAT exhaustion due to NAT gateway configuration

Common SNAT exhaustion issues with NAT gateway typically have to do with the configurations on the NAT gateway. Common SNAT exhaustion issues include:

- Outbound connectivity on NAT gateway not scaled out enough.
- NAT gateway's configurable TCP idle timeout timer is set higher than the default value of 4 minutes.

upvoted 2 times

✉  **Fearless90** 11 months, 3 weeks ago

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/troubleshoot-nat#snat-exhaustion-due-to-nat-gateway-configuration>  
Outbound connectivity not scaled out enough

Each public IP address provides 64,512 SNAT ports to subnets attached to NAT gateway. From those available SNAT ports, NAT gateway can support up to 50,000 concurrent connections to the same destination endpoint. If outbound connections are dropping because SNAT ports are being exhausted, then NAT gateway may not be scaled out enough to handle the workload. More public IP addresses may need to be added to NAT gateway in order to provide more SNAT ports for outbound connectivity.

upvoted 2 times

✉  **Fearless90** 11 months, 3 weeks ago

<https://docs.microsoft.com/en-us/azure/load-balancer/troubleshoot-outbound-connection#configure-an-individual-public-ip-on-vm>  
Configure an individual public IP on VM

For smaller scale deployments, you can consider assigning a public IP to a VM. If a public IP is assigned to a VM, all ports provided by the public IP are available to the VM. Unlike with a load balancer or a NAT gateway, the ports are only accessible to the single VM associated with the IP address.

We highly recommend considering utilizing NAT gateway instead, as assigning individual public IP addresses isn't a scalable solution.

upvoted 2 times

✉  **milan92stankovic** 1 year ago

**Selected Answer: B**

B is the correct answer.

upvoted 2 times

✉  **d3j4n** 1 year ago

Pozdravi Radu Manojlovic brat moj !

upvoted 5 times

✉  **Edward1** 1 year, 2 months ago

**Selected Answer: B**

B is Correct

Azure Firewall proporciona 2496 puertos SNAT por dirección IP pública configurada por instancia de conjunto de escalado de máquina virtual de back-end (mínimo de 2 instancias) y puede asociar hasta 250 direcciones IP públicas . Una mejor opción para escalar los puertos SNAT salientes es usar una NAT de Azure Virtual Network como puerta de enlace NAT. Proporciona 64 000 puertos SNAT por dirección IP pública y admite hasta 16 direcciones IP públicas, proporcionando efectivamente hasta 1 024 000 puertos SNAT salientes.

upvoted 4 times

✉  **mohamed1999** 1 year, 3 months ago

**Selected Answer: B**

Answer is B

Outbound connectivity not scaled out enough

Each public IP address provides 64,512 SNAT ports to subnets attached to NAT gateway. From those available SNAT ports, NAT gateway can support up to 50,000 concurrent connections to the same destination endpoint. If outbound connections are dropping because SNAT ports are

being exhausted, then NAT gateway may not be scaled out enough to handle the workload. More public IP addresses may need to be added to NAT gateway in order to provide more SNAT ports for outbound connectivity.

upvoted 3 times

 **Kiwi28** 1 year, 3 months ago

**Selected Answer: A**

Hi all, I think answer is A, because of what it says here - <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections#:~:text=The%20frontend%20IPs%20of%20a,load%20balancer's%20public%20IP%20address>.

Basically answer A is saying assing to a subnet, meaning bigger subnet, to increase number of available IP addresses.

Answer B says assing public IP address - not sure how this will help, as NAT gateway is already used and as such must have a public IP assigned.

upvoted 1 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **d0bermannn** 1 year, 3 months ago

**Selected Answer: B**

B. Add a public IP address

upvoted 1 times

 **AckeyGraham** 1 year, 4 months ago

**Selected Answer: A**

than out of ports

upvoted 2 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

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

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

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

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

Which public IPv4 addresses can be used by LB1?

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

**Correct Answer: F**

Reference:

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

 **Cristoicach91** Highly Voted 9 months, 3 weeks ago

**Selected Answer: B**

Must match SKU and Region.

upvoted 23 times

 **Villaran** Highly Voted 9 months, 3 weeks ago

**Selected Answer: B**

I think it's B. IP3 only. Must match SKU and Location

upvoted 13 times

 **mrgreat** Most Recent 2 months, 3 weeks ago

LB1 can use IP3 only.

Explanation:

The load balancer LB1 requires a public IP address that meets the following criteria:

Type: Public

SKU: Standard

Location: West US

Among the five public IP addresses listed in the table, only IP3 meets all these criteria.

IP1 and IP4 are located in West US and have a Basic SKU, so they cannot be used for a Standard SKU load balancer in West US.

IP2 is located in West US and has a Basic SKU, but it is a dynamic IP address, which is not supported for a load balancer.

IP5 is located in West US 2 and has a Standard SKU, but it cannot be used for a load balancer in West US.

Therefore, the only public IP address that can be used by LB1 is IP3, which has a Standard SKU, a static assignment, and is located in West US.

upvoted 2 times

 **RAN\_L** 2 months, 4 weeks ago

**Selected Answer: F**

When creating a load balancer in Azure, you need to specify a public IP address to use as the frontend of the load balancer. The public IP address must be of the same SKU as the load balancer, and it can be either static or dynamic.

In this scenario, the load balancer that needs to be created is named LB1 and has the following settings:

Location: West US

Type: Public

SKU: Standard

Therefore, you can use the following public IPv4 addresses for LB1:

IP3: Standard SKU and static IP assignment, located in West US

IP5: Standard SKU and static IP assignment, located in West US 2

IP1, IP2, and IP4 are not suitable for LB1 because they have a Basic SKU, and LB1 requires a Standard SKU. Additionally, IP2 has a dynamic IP address assignment, which is not recommended for use with a load balancer.

upvoted 1 times

✉ **Apptech** 3 months ago

**Selected Answer: F**

It is in Preview ... but possible

Azure Standard Load Balancer supports cross-region load balancing enabling geo-redundant High Availability scenarios  
<https://learn.microsoft.com/en-us/azure/load-balancer/cross-region-overview>

upvoted 2 times

✉ **sridot** 3 months, 3 weeks ago

Standard Load Balancer - Equipped for load-balancing network layer traffic when high performance and ultra-low latency is needed. Routes traffic within => and across regions <=, and to availability zones for high resiliency.

<https://learn.microsoft.com/en-us/azure/load-balancer/skus>

upvoted 1 times

✉ **mVic** 4 months ago

**Selected Answer: B**

Must match SKU and Region

upvoted 2 times

✉ **Gabaky** 4 months, 1 week ago

Correct Answer is F - because Standard SKU Load Balancer routes traffic within and across regions, and to Availability Zones for high resiliency.

upvoted 3 times

✉ **pear77777** 2 months, 3 weeks ago

Right. Standard LB supports the Global tier for Public LBs enabling cross-region load balancing

upvoted 1 times

✉ **Madball** 4 months, 3 weeks ago

**Selected Answer: B**

I have tested this in my lab and the correct answer is B, IP3 only.

upvoted 1 times

✉ **TJ001** 5 months ago

match the SKU and region Answer B

upvoted 1 times

✉ **sshera** 5 months, 2 weeks ago

in exam 4jan23

upvoted 2 times

✉ **nikolas1234397** 6 months ago

**Selected Answer: B**

Must match SKU and Region

upvoted 1 times

✉ **abdulmoiz** 6 months, 1 week ago

Public can't treat as static , should be IP3 only

upvoted 1 times

✉ **jellybiscuit** 8 months, 3 weeks ago

**Selected Answer: B**

I am only able to add public IP addresses from the same region to the load balancers I create.

upvoted 1 times

✉ **AdityaGupta** 9 months ago

**Selected Answer: B**

Must match SKU and Region.

upvoted 3 times

✉ **Alessandro365** 9 months ago

**Selected Answer: B**

IP3 only

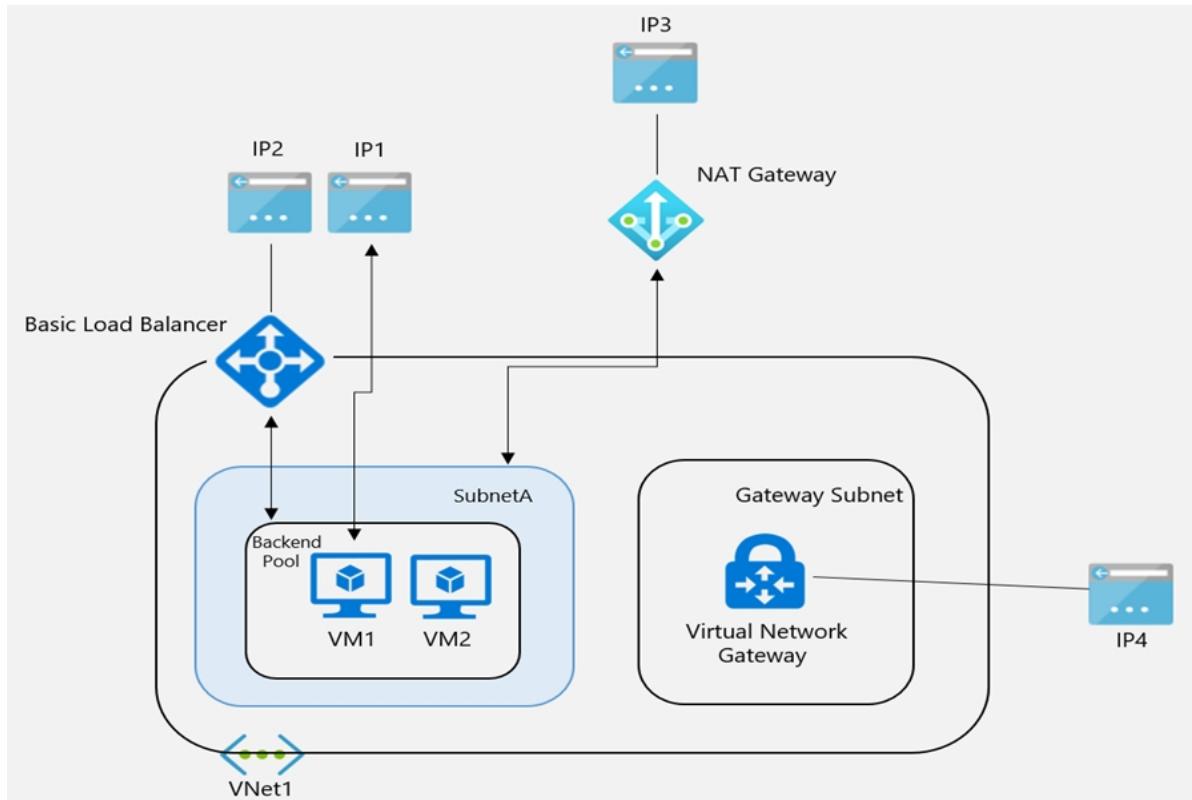
upvoted 3 times

✉ **fun\_and\_games** 9 months, 1 week ago

**Selected Answer: B**

IP3 only, Public LBs are regional and require a standard SKU PIP  
upvoted 2 times

You have the Azure environment shown in the exhibit.



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

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

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

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

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

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

**Correct Answer: A**

christianpageqc Highly Voted 1 year, 8 months ago

According to this article correct answer would be NAT Gateway (IP3)  
<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip>  
 upvoted 94 times

js\_orozco 1 week, 4 days ago

That's right! From top to bottom preference: NAT Gateway Public IP > Backend Standard LB (with defined outbound rules) > Backed Basic Public LB > VM IL Public IP.  
 upvoted 1 times

christianpageqc 1 year, 8 months ago

More this <https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip-and-public-load-balancer>

Anyway the article says "On a subnet with a NAT gateway, all outbound to Internet scenarios are superseded by the NAT gateway"  
 upvoted 33 times

nkhan19 1 year, 4 months ago

the key is "superseded" ONLY if the traffic goes via LB else , ILPIP is prioritized.  
 upvoted 2 times

✉  **vunder** 1 year, 1 month ago

No, the article says " When NAT gateway is configured to subnets, all previous outbound configurations, such as Load balancer or instance-level public IPs (IL PIPs) are superseded and NAT gateway directs all outbound traffic to the internet. " So the correct answer is C: Ref: <https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#connect-to-the-internet-with-nat-gateway>

upvoted 18 times

✉  **pear7777** 2 months, 3 weeks ago

Another benefit of Instance-Level Public IP Address is that it is used as the Outgoing IP address of the VM when connecting to external endpoints. Since a PIP uniquely identifies a VM the receiver can easily whitelist or identify the source of the traffic. For scenarios requiring large number of outbound connections such as Web crawler, it is recommended that the VMs uses Instance-Level public IPs so that it has dedicated outbound IP for Source Network Address Translation (SNAT)

upvoted 1 times

✉  **Takloy** 1 year, 5 months ago

This is the only explanation I need. Thanks!

upvoted 1 times

✉  **Bharat** 1 year, 8 months ago

I believe that you are correct.

upvoted 5 times

✉  **northgaterebel** Highly Voted  1 year, 7 months ago

Selected Answer: C

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip-and-public-load-balancer>

upvoted 13 times

✉  **Kipruto** Most Recent  2 months, 2 weeks ago

"In the presence of other outbound configurations within a virtual network, such as Load balancer or instance-level public IPs (IL PIPs), NAT gateway takes precedence for outbound connectivity. All new outbound initiated and return traffic starts using NAT gateway. There's no down time on outbound connectivity after adding NAT gateway to a subnet with existing outbound configurations." so correct answer is NAT Gateway (IP3)

upvoted 1 times

✉  **RockyAnil** 2 months, 3 weeks ago

Selected Answer: C

NAT takes precedence

upvoted 1 times

✉  **AzureLearner01** 3 months, 2 weeks ago

I think this question or scenario is not right. You can't add a NAT gateway to a subnet that have a load balancer with basic sku. Tried this in a lab and i needed to change the loadbalancer to standard sku with standard ip and not basic.

upvoted 1 times

✉  **GiorgioLDN** 3 months, 2 weeks ago

Selected Answer: C

See the "NAT and VM with an instance-level public IP" section at:

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip>

upvoted 1 times

✉  **JennyHuang36** 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 1 times

✉  **Rajan395** 4 months, 3 weeks ago

correct answer

upvoted 1 times

✉  **TJ001** 5 months ago

IP3.. NAT gateway is priority

upvoted 1 times

✉  **zukako** 5 months, 2 weeks ago

IP3 is correct. NAT Gateway is most prioritiesed.

upvoted 1 times

✉  **Nicolas\_UY** 6 months, 1 week ago

Selected Answer: C

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

Any outbound configuration from a load-balancing rule or outbound rules is superseded by NAT gateway. The VM will also use NAT gateway for outbound. Inbound originated isn't affected. The question is for outbound, inbound will use ILPIP

upvoted 1 times

 **Nicolas\_UY** 6 months, 1 week ago

**Selected Answer: A**

When initiating outbound traffic from VM1, the instance-level public IP address (ILPIP) of VM1 would be used. This is because the ILPIP is the public IP address associated specifically with VM1, and would be used for outbound traffic originating from that virtual machine. The public IP address associated with the Basic Load Balancer and the NAT Gateway, as well as the public IP address associated with the virtual network gateway, would not be used for outbound traffic originating from VM1.

upvoted 1 times

 **winy** 6 months, 4 weeks ago

Based on below

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-an-instance-level-public-ip-and-a-standard-public-load-balancer>

"Any outbound configuration from a load-balancing rule or outbound rules is superseded by NAT gateway."

upvoted 1 times

 **vicks1x** 8 months ago

VM will use NAT gateway for outbound. Inbound originated isn't affected.

So "C" is correct.

Ref : <https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#connect-to-the-internet-with-nat-gateway>

upvoted 1 times

 **sapien45** 8 months, 2 weeks ago

**Selected Answer: C**

When NAT gateway is configured to subnets, all previous outbound configurations, such as Load balancer or instance-level public IPs (IL PIPs) are superseded by NAT gateway. Outbound initiated and return traffic go through NAT gateway.

upvoted 2 times

 **BlackZeros** 8 months, 4 weeks ago

Answer is C:

The order of operations for outbound connectivity follows this order of precedence: Virtual appliance UDR / ExpressRoute >> NAT gateway >> Instance-level public IP addresses on virtual machines >> Load balancer outbound rules >> default system

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

upvoted 4 times

 **AdityaGupta** 9 months ago

**Selected Answer: C**

The IP Associated with NAT Gateway will be used for outbound connections irrespective of Basic or Standard LB. Inbound originated traffic isn't affected.

<https://learn.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#nat-and-vm-with-instance-level-public-ip-~:text=Connect%20to%20the%20internet%20with%20NAT%20gateway>

upvoted 2 times

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

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

What should you include in the solution?

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

**Correct Answer: A**

Reference:

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

 **derrp** Highly Voted 11 months ago

The solution must minimize administrative effort.

When it comes to the simplest solution, do you really want to be configuring a CDN (Azure Front Door), Azure Traffic Manager - with all those profiles and child profiles as we saw from the other convoluted question on this exam, or even an Azure Application Gateway (Whatever that is). Or do you want to stick with the tried and true method of just creating a Load Balancer and be done with it? Gentlemen, I think answer is obvious: Load Balancer. Hope this helps you to remember!

upvoted 15 times

 **sapien45** 8 months, 2 weeks ago

Your response is a lot of things ... but obvious is not one of them.

Obvious answers comes with Azure links This design uses two Azure Load Balancers to expose a cluster of NVAs to the rest of the network:  
<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha?tabs=cli>

upvoted 4 times

 **Prutser2** 8 months, 1 week ago

id have to agree with the ever so friendly sapien45

upvoted 3 times

 **Rajan395** Most Recent 4 months, 3 weeks ago

A is the correct answer

upvoted 1 times

 **Nicolas\_UY** 6 months, 1 week ago

**Selected Answer: A**

To provide high availability for the NVAs and minimize administrative effort, you should include an Azure Standard Load Balancer in the solution.

The Azure Standard Load Balancer is a load balancing service that distributes incoming traffic across multiple VMs or appliances, such as the NVAs in this case. It uses a health probe to monitor the health of the VMs or appliances, and only directs traffic to healthy instances. This ensures that traffic is always directed to a healthy NVA, providing high availability for the NVAs.

Using a Standard Load Balancer also minimizes administrative effort, as it automatically distributes traffic and monitors the health of the VMs or appliances. There is no need to manually configure or manage the load balancing process.

Therefore, the correct answer is A: Azure Standard Load Balancer.

upvoted 3 times

 **AdityaGupta** 9 months ago

**Selected Answer: A**

Standard load balancer is correct answer, when it comes to minimizing the efforts.

upvoted 1 times

 **naiju** 9 months, 2 weeks ago

A is correct.

upvoted 1 times

 **Jamesat** 10 months, 1 week ago

**Selected Answer: A**

Agree. Load balancer would be the simplest solution.

Also with the NVA you would be using Transport Layer addressing not Application Layer. So a standard Load Balancer would be best.

upvoted 2 times

 **PRABHU1993** 10 months, 2 weeks ago

How to get access to all questions

upvoted 1 times

 **zerocooll114** 11 months, 2 weeks ago

on exam today

upvoted 2 times

 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam 6/28/22

upvoted 2 times

 **lasmas** 1 year ago

**Selected Answer: A**

I think A is the correct one

upvoted 2 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 2 times

 **d0berman** 1 year, 4 months ago

**Selected Answer: A**

A. Azure Standard Load Balancer

upvoted 1 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

 **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022

upvoted 1 times

 **Pravda** 1 year, 5 months ago

Variation on exam 1/6/2022

upvoted 3 times

 **AidenYoukhana** 1 year, 5 months ago

CORRECT ANSWER: AZURE STANDARD LOAD BALANCER.

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

upvoted 1 times

 **teamaws** 1 year, 7 months ago

Correct, <https://docs.microsoft.com/en-us/azure/load-balancer/skus#skus>

upvoted 2 times

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

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

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

What should you configure?

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

**Correct Answer: C**

Reference:

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

✉  **JMGENZOR** Highly Voted 1 year, 7 months ago

**Selected Answer: C**

Correct!

upvoted 9 times

✉  **prepper666** Highly Voted 1 year, 7 months ago

URL path rules for routing to /app1 and /app2 etc.

upvoted 8 times

✉  **js\_orozco** Most Recent 1 week, 4 days ago

Correct! Only 1 path-rule is needed (associated with the 5 backend pools).

<https://learn.microsoft.com/en-us/azure/application-gateway/configuration-request-routing-rules#rule-type>

upvoted 1 times

✉  **Abid9** 3 months, 3 weeks ago

Correct

upvoted 1 times

✉  **Nicolas\_UY** 6 months, 1 week ago

**Selected Answer: C**

To control the flow of traffic based on the URL path, you should configure rules in the Azure application gateway.

Rules in an Azure application gateway define how incoming traffic is routed to the backend pool or target. Each rule consists of a listener, which specifies the protocol, port, and hostname to listen for, and a backend pool or target, which specifies the destination for traffic that matches the listener's criteria.

In this case, you can create a rule for each web app, specifying the hostname www.contoso.com and the URL path for the web app (e.g. /app1, /app2, etc.) as the listener criteria, and the corresponding virtual machine hosting the web app as the backend pool or target. This will allow you to control the flow of traffic based on the URL path, directing traffic to the appropriate virtual machine for each web app.

Therefore, the correct answer is C: rules.

upvoted 3 times

✉  **Prutser2** 8 months, 2 weeks ago

this question is around Path based routing, which can be configured under Routing Rule, answer C

upvoted 1 times

✉  **AdityaGupta** 9 months ago

**Selected Answer: C**

URL path rules for routing to /app1 and /app2 etc.

upvoted 1 times

✉  **Alessandro365** 9 months ago

**Selected Answer: C**

C = rules

upvoted 1 times

✉  **Edward1** 1 year, 2 months ago

**Selected Answer: C**

Is Correct.

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

upvoted 2 times

 **ronieto** 1 year, 3 months ago

**Selected Answer: C**

C Rules

upvoted 2 times

 **d0bermannn** 1 year, 3 months ago

**Selected Answer: C**

C. rules

upvoted 2 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **Vinit\_Singh** 1 year, 4 months ago

**Selected Answer: C**

Path based routing can be configured in Routing rules

upvoted 3 times

 **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022 with variation

upvoted 1 times

 **Pravda** 1 year, 5 months ago

on exam 1/6/2022

upvoted 3 times

 **Pamban** 1 year, 6 months ago

appeared on exam 5th Dec 2021

upvoted 2 times

 **teamaws** 1 year, 7 months ago

Correct, <https://docs.microsoft.com/en-us/azure/application-gateway/configuration-request-routing-rules#rule-type>

upvoted 5 times

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

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

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

You create a Traffic Manager profile named TMprofile1. TMprofile1 uses the weighted traffic-routing method.

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

Which DNS record should you create?

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

**Correct Answer:** C

Reference:

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

✉  **Nicolas\_UY** Highly Voted 6 months, 1 week ago

**Selected Answer: C**

To ensure that Traffic Manager routes traffic for www.contoso.com, you should create a CNAME record that maps www.contoso.com to TMprofile1.trafficmanager.net.

A CNAME (Canonical Name) record is a type of DNS record that maps a hostname to another hostname, rather than an IP address. When a client sends a request for the hostname specified in the CNAME record, the DNS server responds with the IP address of the target hostname.

In this case, you can create a CNAME record that maps www.contoso.com to TMprofile1.trafficmanager.net, which is the hostname of the Traffic Manager profile. This will allow clients to access the website using the hostname www.contoso.com, while Traffic Manager handles the routing of traffic between AS1 and AS2 based on the configured traffic-routing method.

Therefore, the correct answer is C: a CNAME record that maps www.contoso.com to TMprofile1.trafficmanager.net.

upvoted 6 times

✉  **jellybiscuit** Highly Voted 8 months, 3 weeks ago

**Selected Answer: C**

Correct

azurefd.net = Front Door  
trafficmanager.net = Traffic Manager  
upvoted 5 times

✉  **CarlosBarrero** Most Recent 7 months, 4 weeks ago

<https://vceguide.com/microsoft/az-700-designing-and-implementing-microsoft-azure-networking-solutions/>

upvoted 2 times

✉  **Alessandro365** 9 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

✉  **jilguens** 9 months, 2 weeks ago

**Selected Answer: C**

correct

upvoted 2 times

✉  **jilguens** 9 months, 2 weeks ago

**Selected Answer: C**

Correct

upvoted 2 times

 **naidu** 9 months, 2 weeks ago

correct

upvoted 2 times

 **Cristoicach91** 9 months, 3 weeks ago

correct

upvoted 2 times

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

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

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

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

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

```
{
  "timeStamp": "2021-06-02T18:13:45+00:00",
  "resourceID": "/SUBSCRIPTIONS/489f2hht-se7y-987v-g571-463hw3679512/RESOURCEGROUPS/RG1/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/AGW1",
  "operationName": "ApplicationGatewayFirewall",
  "category": "ApplicationGatewayFirewallLog",
  "properties": {
    "instanceId": "appgw_0",
    "clientIp": "137.135.10.24",
    "clientPort": "",
    "requestUri": "/login",
    "ruleSetType": "OWASP CRS",
    "ruleSetVersion": "3.0.0",
    "ruleId": "920300",
    "message": "Request Missing an Accept Header",
    "action": "Matched",
    "site": "Global",
    "details": {
      "message": "Warning. Match of \\"pm AppleWebKit Android\\" against \\"REQUEST_HEADER:User-Agent\\" required. ",
      "data": "",
      "file": "rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "app1.contoso.com",
    "transactionId": "f7546159ylhjk7wa114568if513lt68h7",
    "policyId": "default",
    "policyScope": "Global",
    "policyScopeName": "Global",
  }
}
```

You need to ensure that the URL is accessible through the application gateway from any IP address.

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

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

The log shows that WAF rule with ruleId 920300 was triggered. Instead we should disable the WAF rule that has a ruleId 920300.

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot>

✉ flurgen248 3 months, 1 week ago

**Selected Answer: B**

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-monitor?pivots=front-door-standard-premium#waf-logs>

Client IP is the IP address of the client that made the request. If there was an X-Forwarded-For header in the request, the client IP address is taken from that header field instead.

There wasn't an X-Forwarded-For header, so it is your IP address. Creating a WAF exclusion would allow you to connect, but that is not the goal. Any connections from a different IP would still get the 403 error.

The answer is No.

upvoted 1 times

✉ Nicolas\_UY 6 months, 1 week ago

**Selected Answer: B**

B. No

Creating a WAF policy exclusion for request headers that contain 137.135.10.24 will not ensure that the URL is accessible through the application gateway from any IP address. Instead, you should check the WAF rules and policy settings to ensure that the IP address or range of IP addresses from which you are trying to access the URL is not being blocked by the WAF. You may also need to check the access control lists (ACLs) and network security groups (NSGs) associated with the application gateway to ensure that traffic from the desired IP addresses is allowed.

upvoted 2 times

✉ DeepMoon 8 months, 3 weeks ago

Given Answer is Correct:

Disabling a client IP for missing an Accept Header is definitely not the answer.

upvoted 2 times

**HOTSPOT -**

Your company has 10 instances of a web service. Each instance is hosted in a different Azure region and is accessible through a public endpoint. The development department at the company is creating an application named App1. Every 10 minutes, App1 will use a list of endpoints and connect to the first available endpoint.

You plan to use Azure Traffic Manager to maintain the list of endpoints.

You need to configure a Traffic Manager profile that will minimize the impact of DNS caching.

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**

Traffic Manager algorithm:

Geographic
Multivalue
Priority
Subnet

Endpoint type:

Azure endpoint
External endpoint
Nested endpoint

**Answer Area**

Traffic Manager algorithm:

Geographic
Multivalue
Priority
Subnet

Correct Answer:

Endpoint type:

Azure endpoint
External endpoint
Nested endpoint

Reference:

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

✉️  **VonKellus**  1 year, 2 months ago

the Multivalue traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response. This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive. This pattern can increase the availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint. MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses. When a query is received for this profile, all healthy endpoints are returned and are subject to a configurable maximum return count.

upvoted 22 times

✉️  **Bon\_** 9 months, 3 weeks ago

Your statement is correct.

We know it's external endpoint due to the key word "...accessible through a public endpoint"

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-configure-multivalue-routing-method#add-traffic-manager-endpoint>  
"At this time adding endpoints using IPv4 or IPv6 addresses is supported only for endpoints of type External and hence MultiValue routing is also supported only for such endpoints." Therefore the other endpoints including Azure endpoint are not an option. Simple process of elimination.

upvoted 3 times

✉️  **wmohsen**  1 year, 2 months ago

Has to be Azure endpoints?

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

upvoted 8 times

✉️  **pipin06** 1 year, 1 month ago

• Azure endpoints are used for services hosted in Azure.

• External endpoints are used for services hosted outside Azure, either on-premises or with a different hosting provider.

• Nested endpoints are used to combine Traffic Manager profiles to create more flexible traffic-routing schemes to support the needs of larger, more complex deployments.

as per the following I assume we are talking about azure endpoints, not external endpoints

upvoted 6 times

✉️  **Dean208** 1 year ago

I have tested it in the Azure Portal. If you try to use Azure endpoint you get error ..."MultiValue profiles cannot have endpoint with domain names, Azure endpoints or nested endpoints as targets"

upvoted 6 times

✉️  **bakamon**  2 weeks, 5 days ago

:: Multivalue

:: External endpoint

sidhi baat no bakwas

upvoted 1 times

✉️  **sapien45** 8 months, 3 weeks ago

The Multivalue traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response. This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive. This pattern can increase the availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint. MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses.

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

upvoted 2 times

✉️  **1particle** 10 months, 2 weeks ago

Multivalue and External Endpoint

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-configure-multivalue-routing-method#add-traffic-manager-endpoints>

upvoted 3 times

✉️  **Fearless90** 11 months, 3 weeks ago

Traffic Manager algorithm > Multivalue

Endpoint type > External endpoint

minimize the impact of DNS caching

upvoted 4 times

✉️  **Fearless90** 11 months, 3 weeks ago

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

Multivalue traffic-routing method

The Multivalue traffic-routing method allows you to get multiple healthy endpoints in a single DNS query response. This configuration enables the caller to do client-side retries with other endpoints in case a returned endpoint being unresponsive. This pattern can increase the availability of a service and reduce the latency associated with a new DNS query to obtain a healthy endpoint. MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses. When a query is received for this profile, all healthy endpoints are returned and are subject to a configurable maximum return count.

upvoted 1 times

✉️  **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 2 times

✉️  **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

✉️  **milan92stankovic** 1 year ago

I think the answer is correct.

Multivalue is the only option that will return the list of the endpoints, which is the requirement. However, you cannot use Azure endpoints with a multivalue routing algorithm and also you are reaching out to all the WebApps from the "outside".

upvoted 5 times

✉️  **Whatsamattr81** 1 year ago

Has to be multi value which only seems to work with external (and not azure endpoints)

upvoted 3 times

✉️  **RVR** 1 year, 1 month ago

The catch is that " minimize the impact of DNS caching" and when we select Multivalue it clearly says "MultiValue routing method works only if all the endpoints of type 'External' and are specified as IPv4 or IPv6 addresses"

upvoted 5 times

✉️  **jkklim** 1 year, 1 month ago

Endpoint : Azure endpoint

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types#:~:text=Azure%20endpoints%20are%20used%20for,with%20a%20different%20hosting%20provider>.

upvoted 2 times

✉️  **Kay04** 1 year, 1 month ago

i think it has to be azure end point, as the services are hosted in Azure  
Azure endpoints are used for services hosted in Azure.

External endpoints are used for IPv4/IPv6 addresses, FQDNs, or for services hosted outside Azure. These services can either be on-premises or with a different hosting provider.

Nested endpoints are used to combine Traffic Manager profiles to create more flexible traffic-routing schemes to support the needs of larger, more complex deployments.

upvoted 2 times

"Instances are hosted in Azure but are accessible via public endpoints". Hence External endpoints.

upvoted 2 times

## DRAG DROP -

You have an Azure Front Door instance named FrontDoor1.

You deploy two instances of an Azure web app to different Azure regions.

You plan to provide access to the web app through FrontDoor1 by using the name app1.contoso.com.

You need to ensure that FrontDoor1 is the entry point for requests that use app1.contoso.com.

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

Select and Place:

Actions	Answer Area
Add a custom domain to FrontDoor1.	
Add a PTR record to DNS.	
Add a rules engine configuration to FrontDoor1.	
Add a routing rule to FrontDoor1.	
Add a CNAME record to DNS.	

## Correct Answer:

Actions	Answer Area
	Add a CNAME record to DNS.
Add a PTR record to DNS.	Add a custom domain to FrontDoor1.
Add a rules engine configuration to FrontDoor1.	 Add a routing rule to FrontDoor1. 

## Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#associate-the-custom-domain-with-your-front-door>

<https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

- ✉  **tartarus23** Highly Voted 11 months, 2 weeks ago
  1. Add a CNAME record to DNS
  2. Add a custom domain to FrontDoor1
  3. Add a routing rule to FrontDoor1
 Cname record to DNS for frontdoor to verify and then you can add the custom domain followed by the routing rule to app1.contoso.com  
 upvoted 23 times
- ✉  **jkklim** Highly Voted 1 year, 2 months ago
 above is correct as done in labs  
 upvoted 5 times
- ✉  **jkklim** 1 year, 2 months ago
 add cname to dns ==> add them externally eg in godaddy  
 upvoted 4 times
- ✉  **Skankhun** Most Recent 4 months, 2 weeks ago
 I agree answer is correct, however wouldn't it be better to structure the sequence:  
 1) Add a custom domain to FrontDoor1  
 2) Add a routing rule to FrontDoor1

3) Add a CNAME record to public DNS

That way as soon as traffic is routed to FrontDoor1 it's already configured and running.

Or we could just say it takes some time for the new public DNS record to properly propagate, which gives the admin enough time to configure FrontDoor1

upvoted 1 times

✉️👤 **Skankhun** 4 months, 2 weeks ago

Lol never mind, the next question explains why DNS record should be step1 xD

upvoted 3 times

✉️👤 **zerocool114** 11 months, 2 weeks ago

on exam today

upvoted 4 times

✉️👤 **Whatsamattr81** 1 year ago

cname for your custom domain to the given name for your front door instance, assign that custom domain to front door, tell front door where to route to

upvoted 3 times

✉️👤 **HTD** 1 year, 2 months ago

Custom rule , routing and then CNAME should be the order.

upvoted 3 times

✉️👤 **alexbic1890** 1 year, 1 month ago

The answer is correct.

"Before you can use a custom domain with your Front Door, you must first create a canonical name (CNAME) record with your domain provider to point to your Front Door's default frontend host... After Front Door verifies the CNAME record that you create, traffic addressed to the source custom domain ... is routed to the specified destination Front Door default frontend host..."

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

upvoted 4 times

✉️👤 **examlearner** 1 year, 1 month ago

Hi do you have contributor access ?

upvoted 1 times

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**

Reference:

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

**pinpin06** 1 year, 1 month ago

**Selected Answer: C**

response C: "You need to test the website and ContosoFD1 without affecting user access to the on-premises web server." afdverify permits to do it without impact.

upvoted 5 times

**JennyHuang36** 3 months, 3 weeks ago

In exam Feb,2023

upvoted 3 times

**DeepMoon** 8 months, 3 weeks ago

Production site www.contoso.com is mapped to on-prem server.

Future production site would map www.contoso.com to ContosoFD1.azurefd.net, which then would point to Azure WebApp named web1. Before you can do this you need to test while current production (on-prem) server and its current DNS mapping untouched.

Your test site afdverify.www.contoso.com is mapped to afdverify.contosofd1.azurefd.net which is pointing to Azure WebApp.

Now when you send all your DNS traffic to afdverify.www.contoso.com it ends in Azure Web App that is being tested.

upvoted 3 times

**Mike2020** 10 months, 3 weeks ago

**Selected Answer: C**

Answer is correct. This is to map the custom domain while registering to the Azure portal without affecting Web traffic traffic ...

With this method, users can access your domain without interruption while the DNS mapping occurs.

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#map-the-temporary-afdverify-subdomain%20Community%20vote%20distribution>

upvoted 4 times

 **whiteherondance** 1 year, 1 month ago

**Selected Answer: C**

"...You need to test the website and ContosoFD1 \*without affecting user access to the on-premises web server.\*"

Answer is C - read the provided document in the answer, it explains why. B would interrupt user access to on-prem server.

upvoted 3 times

 **frks** 1 year, 1 month ago

**Selected Answer: C**

Ignore my previous comment. New domain -> create cname directly, existing production domain --> afdverify

upvoted 2 times

 **frks** 1 year, 1 month ago

**Selected Answer: B**

afdverify is useless in this scenario

upvoted 1 times

 **Ochman** 1 year, 1 month ago

The answer is B

upvoted 1 times

 **HTD** 1 year, 2 months ago

As per microsoft document reference this is a correct answer.

upvoted 1 times

You have the Azure load balancer shown in the Load Balancer exhibit.

**LB2** Load balancer

Move Delete Refresh

Essentials

Resource group ([change](#)) **RG1**

Backend pool  
LB2-BEP1 (2 virtual machines)

Location  
North Europe

Load balancing rule  
-

Subscription ([change](#)) **Subscription1**

Health probe  
-

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

NAT rules  
0 inbound

SKU  
Standard

Public IP address  
**20.82.214.15 (LB2-IP1)**

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

LB2 has the backend pools shown in the Backend Pools exhibit.

**LB2 | Backend pools** Load balancer

Add Refresh

Filter by name....

Backend pool = = all Resource Name = = all Resource Status = = all IP address = = all

Network interface = = all Availability zone = = all

Group by Backend pool

Backend pool	Resource Name	Resource Status	IP address	Network interface	Availability zone
<b>LB2-BEP1</b>	VMSS1 (instance 2)	Running	10.0.0.6	RG1-vnet-nic01	
<b>LB2-BEP1</b>	VMSS1 (instance 3)	Running	10.0.0.7	RG1-vnet-nic01	

You need to ensure that LB2 distributes traffic to all the members of VMSS1.

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

NOTE: Each correct selection is worth one point.

- A. Add a network interface to VMSS1.
- B. Add a load balancing rule.
- C. Configure a health probe.

D. Add a public IP address to each member of VMSS1.

**Correct Answer: BC**

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal?tabs=option-1-create-load-balancer-standard>

 **HTD** Highly Voted 1 year, 2 months ago

This is correct. Health Probe and a rule is missing in the configuration.

upvoted 6 times

 **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 3 times

 **staffo** 4 months ago

Should it not be A and B? You need to assign different NIC's to machines for it to work.

I don't think C is needed. The question does not reference anything about distributing to healthy servers only, just distributing the traffic evenly.

upvoted 1 times

 **TJ001** 5 months ago

Typical configuration...BC correct

upvoted 2 times

 **vivikar** 5 months, 3 weeks ago

Answer: BC

B - configure the load balancing rule, which maps the frontend IP with backend Pool.

C - monitor the Backend pools

upvoted 3 times

 **DeepMoon** 6 months ago

Can anybody explain why BC is correct. Instead of just religiously repeating the mantra 'it is correct'.

Any reference docs?

upvoted 1 times

 **peterquist** 5 months, 2 weeks ago

You have an explanation in the docs posted in the answer, which says:

During the creation of the load balancer, you'll configure:

Frontend IP address

Backend pool

Inbound load-balancing rules

Health probe

upvoted 1 times

 **Alessandro365** 9 months ago

Selected Answer: BC

BC is correct

upvoted 3 times

 **jilguens** 9 months, 2 weeks ago

Selected Answer: BC

correct

upvoted 1 times

 **Hermi** 11 months, 2 weeks ago

Selected Answer: BC

Correct

upvoted 2 times

 **d3j4n** 1 year ago

Correct !

upvoted 2 times

You have an Azure subscription that contains the following resources:

- ⇒ A virtual network named Vnet1
- ⇒ Two subnets named subnet1 and AzureFirewallSubnet
- ⇒ A public Azure Firewall named FW1
- ⇒ A route table named RT1 that is associated to Subnet 1
- ⇒ A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet 1, you discover that none of the virtual machines were activated.

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

What should you do?

- A. On FW1, configure a DNAT rule for port 1688.
- B. Deploy an application security group that allows outbound traffic to 1688.
- C. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- D. On FW1, create an outbound service tag rule for Azure Cloud.

**Correct Answer: C**

Cause -

The Azure Windows VMs need to connect to the Azure KMS server for Windows activation. The activation requires that the activation request come from an Azure public IP address.

To resolve this problem, use the Azure custom route to route activation traffic to the Azure KMS server.

Reference:

<https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/custom-routes-enable-kms-activation>

 **TJ001** 5 months ago

Correct Answer C

upvoted 1 times

 **MariusFlorea99** 8 months, 1 week ago

Correct answer C - one of the main causes of activation failure is firewall blocking outbound access to kms.core.windows.net:1688 (Azure KMS)  
upvoted 1 times

 **sapien45** 8 months, 3 weeks ago

**Selected Answer: C**

Understanding Azure KMS endpoints for Windows product activation of Azure Virtual Machines

Azure uses different endpoints for KMS (Key Management Services) activation depending on the cloud region where the VM resides  
<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-activation-problems>

upvoted 1 times

 **BlackZeros** 8 months, 4 weeks ago

**Selected Answer: C**

C seems correct

upvoted 1 times

 **Alessandro365** 9 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

You have an Azure Front Door instance that has a single frontend named Frontend1 and an Azure Web Application Firewall (WAF) policy named Policy1. Policy1 redirects requests that have a header containing "string1" to https://www.contoso.com/redirect1. Policy1 is associated to Frontend1.

You need to configure additional redirection settings. Requests to Frontend1 that have a header containing "string2" must be redirected to https://www.contoso.com/redirect2.

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

NOTE: Each correct selection is worth one point.

- A. Create a custom rule.
- B. Create a policy.
- C. Create a frontend host.
- D. Configure a managed rule.
- E. Add a custom rule to Policy1.
- F. Create an association.

**Correct Answer: CEF**

E: A WAF policy consists of two types of security rules:

custom rules that are authored by the customer.

managed rule sets that are a collection of Azure-managed pre-configured set of rules.

You can create a fully customized policy that meets your specific application protection requirements by combining managed and custom rules.

A web application delivered by Front Door can have only one WAF policy associated with it at a time.

CF: We create a frontend host and associate it with the Policy.

In the Association tab of the Create a WAF policy page, select + Associate a Front Door profile, enter the following settings, and then select Add:

### Associate a Front door profile ×

Front door profiles can be added and removed after a WAF policy is created.

Front door profile \* (i)

contosoafd

#### Domain

Multiple domains can be associated with a front door profile.  
Select those you want your WAF policy to apply to.

Domain \*

contosoafd1

**Add**

**Cancel**

Reference:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview> <https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-create-portal>

✉  **Villaran** Highly Voted 9 months, 3 weeks ago

**Selected Answer: ABF**

I think the order is:

- B. Create a policy.
- A. Create a custom rule.
- F. Create an association.

upvoted 21 times

✉  **roshingrg** Most Recent 1 week, 4 days ago

The three actions you should perform to configure the additional redirection settings are:

A. Create a custom rule: This custom rule will define the condition for redirecting requests that have a header containing "string2" to the desired URL. Custom rules allow you to define specific behavior based on your requirements.

E. Add a custom rule to Policy1: Once you have created the custom rule, you need to add it to Policy1. This ensures that the new rule is part of the policy and will be applied to the incoming requests.

F. Create an association: To apply the updated Policy1 to Frontend1, you need to create an association between the policy and the frontend. This ensures that the policy is enforced for requests coming through Frontend1.

So, the correct actions to configure the additional redirection settings would be:

A. Create a custom rule.

E. Add a custom rule to Policy1.

F. Create an association.

upvoted 2 times

 **hal01** 2 months, 1 week ago

**Selected Answer: ABE**

To configure additional redirection settings to redirect requests to Frontend1 that have a header containing "string2" to <https://www.contoso.com/redirect2>, you should perform the following three actions:

B. Create a policy: If you haven't created a policy already, create a new Azure Web Application Firewall (WAF) policy named Policy1.

A. Create a custom rule: Create a custom rule in Policy1 to redirect requests that have a header containing "string2" to <https://www.contoso.com/redirect2>.

E. Add a custom rule to Policy1: Add the custom rule created in the previous step to Policy1.

The other options listed are not required for this scenario:

C. Create a frontend host: A frontend host is not required since Frontend1 already exists.

D. Configure a managed rule: Managed rules are not required for this scenario.

F. Create an association: An association is not required since Policy1 is already associated with Frontend1.

upvoted 2 times

 **\_fvt** 2 months, 2 weeks ago

Not C - You need to use Frontend 1

Not D - Not sure what it is, probably microsoft WAF policy managed rules which will no helps in our case

Not E - You cannot have two different redirect URLs in the same WAF policy, even in different rules (tested in lab)

F - you cannot create an association to the same route which would likely needs be /\* there as asked in this scenario, so you are blocker with only 1 WAF policy...

You can create a policy and a custom rule but not associate it...

I think this question is outdated, WAF policies are not meant to be used for redirect. Normally for this you just a create a Front Door rule set with all your conditions and reducts and that's it.

upvoted 2 times

 **wooyourdaddy** 2 months, 2 weeks ago

**Selected Answer: AEF**

At this link:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview#waf-policy-and-rules>

It states:

A web application delivered by Front Door can have only one WAF policy associated with it at a time.

Since the question states "Policy1 is associated to Frontend1.", this eliminates option B.

The question also states: "Requests to Frontend1 that have a header containing "string2" must be redirected to <https://www.contoso.com/redirect2>.", which tells us that we don't need a new frontend. So option C is eliminated.

At the above link, it also states: "managed rule sets that are a collection of Azure-managed pre-configured set of rules." Since we are targeting a specific value of "string2", this option would be eliminated.

That leaves us with only AEF as possible answers.

upvoted 4 times

 **Apptech** 2 months, 1 week ago

If we use existing Policy1 instead of creating a new one, we can assume that it has already an association to Frontend1. So F is no possible answer.

upvoted 2 times

 **mrgreat** 2 months, 3 weeks ago

To configure additional redirection settings, you should perform the following three actions:

- A. Create a custom rule that matches requests with a header containing "string2".
- E. Add a custom rule to Policy1 that redirects requests that match the custom rule to <https://www.contoso.com/redirect2>.
- F. Create an association between Frontend1 and Policy1.

Therefore, the correct answer is: A, E, F.

upvoted 2 times

 **breakpoint0815** 2 months, 3 weeks ago

**Selected Answer: AEF**

You already have a Policy1, no need to create a new one (= not B)

You already have a Frontend Host, Frontend1 (= Not C)

You need to deploy a custom rule (=Not D)

upvoted 2 times

 **Apptech** 2 months, 1 week ago

For Policy1 we also have an association to Frontend1 ...

upvoted 2 times

 **Apptech** 3 months ago

The text clearly says:

1. Requests to Frontend1 that have a header containing "string2" must be redirected
2. Frontend1 already has a policy assigned.

Because of the fact that you cannot add more than 1 policy to frontend1 it makes no sense to create a second policy.

For that reason my vote is CEF

upvoted 1 times

 **Apptech** 2 months, 1 week ago

I have to add that option F doesn't make sense in that scenario because Policy 1 must have an association to Frontend1

upvoted 1 times

 **DeepMoon** 5 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-create-portal>>

This link clearly states the 3 steps.

1. Create a WAF policy
2. Associate it with a frontend host
3. Configure WAF rules

So answers are C. E .F.

upvoted 1 times

 **jotajotajeje** 7 months ago

**Selected Answer: ABF**

the question itself makes no sense as already have the policy1 created hence the available options tends you to do the all process again.

B. Create a policy.

A. Create a custom rule.

F. Create an association.

But if you already have the policy created would be just to Create a custom rule, as you are already using the same domain...

upvoted 2 times

 **Ajdifasudfo** 6 months, 2 weeks ago

this is incorrect. You can only define one redirect URL per policy. That's why you need a new policy.

upvoted 3 times

 **Prutser2** 8 months, 1 week ago

**Selected Answer: CEF**

i tend to agree with provided answer: cef, first of all we need a new front end to allow the redirected traffic to, the new front end is [www.contoso.com/redirect2](https://www.contoso.com/redirect2).

question clearly stated a redirect when hitting frontend1, and policy1, so policy1 needs changing: add custom rule to policy 1.then finally associate

upvoted 4 times

 **BlackZeros** 8 months, 4 weeks ago

**Selected Answer: ABF**

ABF seems to be the right answer after reading the documents provided by the answer.

upvoted 4 times

 **A\_A\_AB** 8 months, 4 weeks ago

Agree with Villaran. ABF

The current answers are non-sense

upvoted 1 times

 **zenithcsa1** 9 months, 3 weeks ago

Is it really possible to set 2 redirection rules for one frontend(endpoint) without using rules engine configuration? As I understand, WAF policy is mapped with only one frontend and can have only one Redirect URL which is shown in 'Policy settings' blade. Could anyone help with explanation?

upvoted 2 times

Question #26

Topic 3

You have 10 Azure App Service instances. Each instance hosts the same web app. Each instance is in a different Azure region.

You need to configure Azure Traffic Manager to direct users to the instance that has the lowest latency.

Which routing method should you use?

- A. geographic
- B. weighted
- C. priority
- D. performance

**Correct Answer: D**

Select Performance routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency.

Reference:

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

 **BlackZeros** 8 months, 4 weeks ago

**Selected Answer: D**

D is right

upvoted 1 times

 **A\_A\_AB** 8 months, 4 weeks ago

**Selected Answer: D**

Select Performance routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency.

elect Geographic routing to direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. With this routing method, it enables you to be in compliance with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.

upvoted 2 times

 **Alessandro365** 9 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

 **jilguens** 9 months, 2 weeks ago

**Selected Answer: D**

correct

upvoted 2 times

Your company has offices in London, Tokyo, and New York.

The company has a web app named App1 that has the Azure Traffic Manager profile shown in the following table.

Parameter	Value	Azure region
DNS Name	app1.trafficmanager.net	Not applicable
Endpoint	app1-asia.azurewebsites.net	East Asia
Endpoint	app1-na.azurewebsites.net	East US
Endpoint	app1-na.azurewebsites.net	UK South
Routing method	Geographic	Not applicable

In Asia, you plan to deploy an additional endpoint that will host an updated version of App1.

You need to route 10 percent of the traffic from the Tokyo office to the new endpoint during testing.

What should you configure in Traffic Manager?

- A. two profiles and five endpoints
- B. two profiles and four endpoints
- C. three profiles and four endpoints
- D. one profile and five endpoints

**Correct Answer: B**

Need two profiles. Add one Child profile using Weighted routing. One additional trial endpoint, to the existing three, for the Child Profile is needed.

Note 1: Each Traffic Manager profile specifies a single traffic-routing method. However, there are scenarios that require more sophisticated traffic routing than the routing provided by a single Traffic Manager profile. You can nest Traffic Manager profiles to combine the benefits of more than one traffic-routing method.

Note 2: Weighted routing: Select Weighted routing when you want to distribute traffic across a set of endpoints based on their weight. Set the weight the same to distribute evenly across all endpoints.

Reference:

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

✉  **sapien45** Highly Voted 8 months, 3 weeks ago

**Selected Answer: B**

You cannot combine both 'Weighted' and 'Geographic' traffic-routing in a single profile.

The parent profile still uses the Geographic traffic-routing method and child profile uses the Weighted traffic-routing method. This 'child' profile act as an endpoint to the 'parent' profile.

upvoted 5 times

✉  **peterquast** 5 months, 2 weeks ago

This is why I wonder whether they do not count this child profile as a "fifth" endpoint. This is said in the documentation: "To create a nested profile, you add a 'child' profile as an endpoint to a 'parent' profile."

upvoted 1 times

✉  **vivikar** Most Recent 5 months, 3 weeks ago

For Asia: 3 Endpoints: 1+1+1(Nested Endpoint with 2 Child endpoint using Weight method)  
Another regions has 2 Endpoints,

So 2 profiles(Nested and geographic) and 5 Endpoints

upvoted 1 times

✉  **vivikar** 5 months, 3 weeks ago

Sorry, Ignore my comment.. Nested endpoint is wrong, it should be profile.. So 2 and 2 is answer  
upvoted 1 times

✉  **OliwerCiecwierz** 3 months, 2 weeks ago

That's not even a listed answer so we will ignore your comments, don't worry  
upvoted 5 times

✉  **Prutser2** 8 months, 1 week ago

**Selected Answer: B**

you will need to add the updated server to the list so you end up with 4 nodes,  
for Japan, you will need a Traffic porfile , with routing geographic and inside that a weighted group with two server, so answer B  
upvoted 4 times

HOTSPOT -

You configure a route table named RT1 that has the routes shown in the following table.

Name	Prefix	Next hop type	Next hop IP address
Route1	0.0.0.0/0	Network virtual appliance (NVA)	192.168.0.4
Route2	10.0.0.0/24	Network virtual appliance (NVA)	192.168.0.4

You have an Azure virtual network named Vnet1 that has the subnets shown in the following table.

Name	Prefix	Route table
DMZ	192.168.0.0/24	None
FrontEnd	192.168.1.0/24	RT1
BackEnd	192.168.2.0/24	None

You have the resources shown in the following table.

Name	IP address	Type
NVA1	192.168.0.4	NVA
VM1	192.168.1.4	Virtual machine
VM2	192.168.2.4	Virtual machine

Vnet1 connects to an ExpressRoute circuit. The on-premises router advertises the following routes:

⇒ 0.0.0.0/0

⇒ 10.0.0.0/16

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
Internet traffic from NVA1 is routed to the on-premises network.	<input type="radio"/>	<input type="radio"/>
Traffic from VM2 to the on-premises network is routed through NVA1.	<input type="radio"/>	<input type="radio"/>
Traffic from VM1 is routed to VM2 through NVA1.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

### Answer Area

Statements	Yes	No
Internet traffic from NVA1 is routed to the on-premises network.	<input checked="" type="radio"/>	<input type="radio"/>
Traffic from VM2 to the on-premises network is routed through NVA1.	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from VM1 is routed to VM2 through NVA1.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: Yes -

NVA1 with IP (NVA-network virtual appliance) 192.168.0.4 is on the DMZ subnet. It will use route 10.0.0.0/16 to the on-premises network.

Box 2: No -

VM2 has IP address 192.168.2.4 and is on the BackEnd subnet. VM2 will not use the RT1 route table, and will not reach the on-premises network through NVA1.

Box 3: Yes -

VM1 with IP address 192.168.1.4 is on the FrontEnd subnet, and will use the RT1 routing table. It will use Route2 and Next Hop IP address 192.168.0.4, IP address of NVA1, to reach VM2.

YNN. Route 0.0.0.0/0 is advertised to NVA from on-prem. VM2 learns route 10.0.0.0/16 from on-prem. VM1 and VM2 are in different subnets, but same virtual network, there is a system route that is a better match than the one in the route table.

upvoted 25 times

✉️  **sapien45** 8 months, 2 weeks ago

Perfect Answer.

Both below answers are based on not reading :

ONLY if If multiple routes contain the SAME address prefix, UDR prevails

upvoted 1 times

✉️  **ChrisCrown** 9 months, 1 week ago

YNY .. Box 3 is yes as it is using the UDR ( RT1 ) which points to the NVA as its default gateway. UDR gets higher priority.

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

upvoted 7 times

✉️  **mav3r1ck** 9 months ago

Agree.

If multiple routes contain the same address prefix, Azure selects the route type, based on the following priority:

- User-defined route
- BGP route
- System route

upvoted 3 times

✉️  **Lrrr\_FromOmicronPersei8** 7 months, 3 weeks ago

Well no, you get a longer prefix system-generated route with a next-hop type VnetLocal, therefore YNN.

upvoted 5 times

✉️  **TJ001** 5 months ago

VNET route is more specific address than 0/0 UDR .. so I will go with YNN

upvoted 2 times

✉️  **jellybiscuit** Highly Voted 8 months, 2 weeks ago

YNY

UDRs exist for a reason: to override the default behavior of Azure routing

- It is correct that there is a default route that would allow VM1 to communicate with VM2
- that route is superseded by the UDR
- Someone has intentionally decided that all outbound traffic from the frontend subnet should pass through the NVA (firewall).

It is important to know that the other routes exist and in what order they are used

- 1) User-defined
- 2) BGP
- 3) system/default

Just remember that if they show you a route table, it is a UDR and is always in-use.

If you want to see the full list of routes, find it by looking at Effective Routes from the portal.

upvoted 7 times

✉️  **mickeysonix** 5 months, 4 weeks ago

Thought similar, but Azure uses the longest prefix match algorithm and only after that it uses UDRs. So VNet2 has a system defined route of longer prefix than BGP ones and UDRs and therefore traffic is direct.

upvoted 1 times

✉️  **Prutser2** 8 months, 1 week ago

not always, there is still the mechanism of the longest match, for instance in box 3, even though there is a UDR, the longest match is still the route that dictates that subnets within the same vnet can flow.

upvoted 2 times

✉️  **crypto700** Most Recent 1 month, 3 weeks ago

YNN, VM1 will get to VM2 without NVA because they are in the same VNet.

upvoted 1 times

✉️  **AzureLearner01** 3 months, 2 weeks ago

My answer is Yes, No, No. I think Q1 and Q2 are obvious. but Q3 is not. UDR will overwrite the system route but only if you create a specific route not the default route 0.0.0.0/0. The default route 0.0.0.0/0 would not overwrite the system route, so next Hop is the internal GW from the subnet and not the nva. To verify this theory i've created a UDR that routes traffic from the subnet of VM1 to the subnet of VM2 over the NVA. Traffic from VM1 will go over the nva to VM2 even if they are in the same VNet.

upvoted 3 times

✉️  **Hajji** 3 months, 4 weeks ago

YNY

When you create a route table and associate it to a subnet, the table's routes are combined with the subnet's default routes. If there are conflicting route assignments, user-defined routes will override the default routes.

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

upvoted 1 times

✉ ejml 4 months, 3 weeks ago

Default routes of the one subnet are the address space of the its virtual network and virtual networks peered. In the worst case, when both routes (UDR and System Route) UDR has higher priority. Answer is YNY

upvoted 2 times

✉ eVo3000 5 months, 1 week ago

YNN

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#how-azure-selects-a-route>

"When outbound traffic is sent from a subnet, Azure selects a route based on the destination IP address, using the longest prefix match algorithm[...]. If multiple routes contain the same address prefix, Azure selects the route type, based on the following priority:

1.User-defined route

2.BGP route

3.System route

In our case, we do not take the default route

upvoted 4 times

✉ jotajotajeje 7 months ago

YNN.

1-Route 0.0.0.0/0 is advertised to NVA from on-prem and it doesn't have routing table.

2-VM2 has no routing table hence it will go via the 0.0.0.0/0 advertised via BGP from the on premises router that has more priority than system route 0.0.0.0/0 to internet via Azure network

3-VM1 and VM2 are in different subnets, but same virtual network, there is a system route in every subnet/VM interface that has the network and mask of the entire VNET where the subnet is, therefore as it has the prefix length bigger than the default route it will prefer going directly from VM to VM.

upvoted 3 times

✉ JWYANG 8 months ago

YNY

Azure automatically added this route for all subnets within Virtual-network-1, because 10.0.0.0/16 is the only address range defined in the address space for the virtual network. If the user-defined route in route ID2 weren't created, traffic sent to any address between 10.0.0.1 and 10.0.255.254 would be routed within the virtual network, because the prefix is longer than 0.0.0.0/0, and not within the address prefixes of any of the other routes. Azure automatically changed the state from Active to Invalid, when ID2, a user-defined route, was added, since it has the same prefix as the default route, and user-defined routes override default routes. The state of this route is still Active for Subnet2, because the route table that user-defined route, ID2 is in, isn't associated to Subnet2.

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#routing-example>

upvoted 2 times

✉ mickeysonix 5 months, 4 weeks ago

Thought similar, but Azure uses the longest prefix match algorithm and only after that it uses UDRs. So VNet2 has a system defined route of longer prefix than BGP ones and UDRs and therefore traffic is direct.

upvoted 2 times

✉ DeepMoon 8 months, 3 weeks ago

Given Answers are incorrect.

Correct Answers

Q1: Yes. Why?

Because On-Prem router advertises 0.0.0.0/0 route to the NVA through a Express Route. We are not told NVA has any other route.

Q2: Yes. Why?

Because VM2 is on backend subnet (192.168.2.0/24) it has no UDR. But NVA1 is advertising all the routes on its table (that includes what it learned from On-Prem) to the all of VNet1. NVA1 knows how to get to 10.0.0/16 network via On-Prem router.

Q3: No. Why?

Because VM1 & VM2 are in VNET1. Azure by default knows how to route traffic between its subnets without needing a UDR's.

upvoted 1 times

✉ sapien45 8 months, 3 weeks ago

YNN.

Read the link in its entirety ! Especially the implementation example.

The very same routes are being displayed.

Route ID1 is not invalidated by route ID12 because the prefix is longer than 0.0.0.0/0

upvoted 2 times

✉ andry79 9 months ago

Tested in lab, is YNN

upvoted 6 times

✉ Fule 9 months, 1 week ago

I will go with YNY,

"Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create system routes, nor can you remove system routes, but you can override some system routes with custom routes." so basically means custom routes is a better match than the system, which is somehow logical, you want to manipulate with system routes in some scenario.

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

upvoted 2 times

✉️  **Kafura** 2 months ago

<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#:~:text=When%20you%20create%20a%20route%20table%20and%20associate%20it%20to%20a%20subnet%2C%20the%20table%27s%20routes%20are%20combined%20with%20the%20subnet%27s%20default%20routes.%20If%20there%20are%20conflicting%20route%20assignments%2C%20user%2Ddefined%20routes%20will%20override%20the%20default%20routes.>

upvoted 1 times

✉️  **zenithcsa1** 9 months, 1 week ago

YNN

Box 3 : When communicating from VM1 to VM2, the Next-hop Type becomes VirtualNetwork due to the longest prefix. So UDR routes(0.0.0.0/0 - > NVA) are not used.

upvoted 5 times

**HOTSPOT -**

You have an Azure subscription. The subscription contains virtual machines that host websites as shown in the following table.

Name	Public host name	Location
VM1	site1.us.contoso.com	East US
VM2	site1.uk.contoso.com	UK West
VM3	site2.us.contoso.com	East US
VM4	site2.uk.contoso.com	UK West
VM5	site2.japan.contoso.com	Japan West

You have the Azure Traffic Manager profiles shown in the following table.

Name	Routing method	DNS name	Hosted on
Tm1	Performance	site1.contoso.com	VM1 and VM2
Tm2	Priority	site2.contoso.com	VM3, VM4, and VM5

You have the endpoints shown in the following table.

Name	Traffic Manager profile	Azure endpoint	Routing method parameter	Status
Ep1	Tm1	VM1	1	Degraded
Ep2	Tm1	VM2	2	Online
Ep3	Tm2	VM3	1	CheckingEndpoint
Ep4	Tm2	VM4	2	Online
Ep5	Tm2	VM5	3	Online

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:

**Statements**

A user that requests site1.contoso.com from the East US Azure region will connect to site1.us.contoso.com.

**Yes**

**No**



A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com.



A user that requests site2.contoso.com from the Japan East Azure region will connect to site2.japan.contoso.com.


**Correct Answer:****Statements**

A user that requests site1.contoso.com from the East US Azure region will connect to site1.us.contoso.com.

**Yes**

**No**



A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com.



A user that requests site2.contoso.com from the Japan East Azure region will connect to site2.japan.contoso.com.



Box 1: No -

VM1, which is hosting site1.contoso.com, is located in East US. The VM1 endpoint status is degraded. Endpoint monitoring health checks are failing. The endpoint isn't included in DNS responses and doesn't receive traffic.

When an endpoint has a Degraded status, it's no longer returned in response to DNS queries. Instead, an alternative endpoint is chosen and returned. The traffic-routing method configured in the profile determines how the alternative endpoint is chosen.

Priority. Endpoints form a prioritized list. The first available endpoint on the list is always returned. If an endpoint status is Degraded, then the next available endpoint is returned.

The user will connect to site2.us.contoso.com instead.

Box 2: No -

VM3, which is hosting site2.contoso.com, is located in East US. The VM3 endpoint status is CheckingEndpoint. The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

User will connect to site2.contoso.com, not to site2.uk.contoso.com

Box 3: No -

VM3, which is hosting site2.contoso.com, is located in East US. The VM1 endpoint status is CheckingEndpoint, which is OK (see above).

User will connect to site2.contoso.com, not to site2.japan.contoso.com

Reference:

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

✉️  **jellybiscuit**  8 months, 2 weeks ago

Correct.

N - site1.uk.contoso.com is the only site1 host online

N - In a priority routing method, lower numbers are chosen first. Traffic Manager will send traffic to endpoints with the "Checking Endpoint" status  
- so it's going to site2.us

N - same reason as Q2

upvoted 16 times

✉️  **bleemster** 6 months, 4 weeks ago

Can you back this up? "checking endpoint" will still receive traffic? I cant find anything to validate this. All i read is that when you add it you get this status while its checking the endpoint (fitting status really) and when its available traffic will then be sent there.

upvoted 3 times

✉️  **wiki715** 6 months ago

"Checking Endpoint" status == "An endpoint in this state is included in DNS responses and can receive traffic."

(At least according to <https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-monitor-status>)

upvoted 2 times

✉️  **davidkerr7**  8 months, 1 week ago

N - Choose the closest VM1, but it's degraded so choose the next closest VM2 UK [site1.uk.contoso]

Y - Choose in order, VM3 but its checking, so choose VM4 UK [site2.uk.contoso]

N - (Same) Choose in order, VM3 but its checking, so choose VM4 UK

upvoted 7 times

✉️  **TJ001**  5 months ago

NNN is right....

upvoted 3 times

✉️  **Ajdifasudfo0** 6 months, 3 weeks ago

N,N,N actually,

the last one as you can see here: <https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-monitor-status>

The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

upvoted 3 times

✉️  **geuser** 6 months, 4 weeks ago

N,N,N

<https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring#endpoint-monitor-status>

CheckingEndpoint means The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and CAN receive traffic.

upvoted 1 times

✉️  **GohanF2** 7 months, 1 week ago

1. VM1 is degraded . The traffic profile is "performance" which it will be using the closest endpoint to the region.

In this case will connect to VM which is in site1.uk.contonso.com . Answer is: No.

2. VM3 is in checkingEndpoint which is not ready for connectivity. The routing method is "priority"; which means will select the Endpoint with the lowest priority digit. We still have VM4 and VM5 which are online.

VM4 the public site is: site2.uk.contonso.com . Answer is : Yes.

3. Same scenario the profile is "Priority" in this case, the VM with the lowest priority is VM4 which is in UK West: site2.uk.contonso.com. Answer is: No.

NO

YES

NO

upvoted 4 times

✉️ **Goofer** 5 months, 1 week ago

The endpoint is monitored, but the results of the first probe haven't been received yet. CheckingEndpoint is a temporary state that usually occurs immediately after adding or enabling an endpoint in the profile. An endpoint in this state is included in DNS responses and can receive traffic.

upvoted 3 times

✉️ **Azuriste** 8 months, 2 weeks ago

For Me NNY

upvoted 2 times

Question #30

Topic 3

You have an Azure application gateway configured for a single website that is available at <https://www.contoso.com>.

The application gateway contains one backend pool and one rule. The backend pool contains two backend servers. Each backend server has an additional website that is available on port 8080.

You need to ensure that if port 8080 is unavailable on a backend server, all the traffic for <https://www.contoso.com> is redirected to the other backend server.

What should you do?

- A. Create a health probe
- B. Add a new rule
- C. Change the port on the listener
- D. Add a new listener

**Correct Answer: A**

By default, Azure Application Gateway probes backend servers to check their health status and to check whether they're ready to serve requests. Users can also create custom probes to mention the host name, the path to be probed, and the status codes to be accepted as Healthy. In each case, if the backend server doesn't respond successfully, Application Gateway marks the server as Unhealthy and stops forwarding requests to the server. After the server starts responding successfully, Application Gateway resumes forwarding the requests.

Note: The default probe request is sent in the format of <protocol>://127.0.0.1:<port>/ . For example, http://127.0.0.1:80 for an http probe on port 80. Only HTTP status codes of 200 through 399 are considered healthy. The protocol and destination port are inherited from the HTTP settings. If you want Application Gateway to probe on a different protocol, host name, or path and to recognize a different status code as Healthy, configure a custom probe and associate it with the HTTP settings.

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-backend-health-troubleshooting>

✉️ **BlackZeros** Highly Voted 8 months, 4 weeks ago

**Selected Answer: A**

Create Health Probe to monitor the port and server health

upvoted 5 times

✉️ **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 1 times

✉️ **omgMerrick** 4 months ago

**Selected Answer: A**

Option A appears correct.

By default, the health probe checks port 80 for HTTP traffic. However, you can configure the health probe to check other ports, such as port 8080 in this case. If the application gateway determines that a backend server is unavailable, it can automatically redirect traffic to the other available backend server.

upvoted 1 times

You have an Azure subscription that contains the following resources:

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

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

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

What should you do?

- A. On FW1, create an outbound service tag rule for AzureCloud.
- B. Add an internet route to RT1 for the Azure Key Management Service (KMS).
- C. On FW1, configure a DNAT rule for port 1688.
- D. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.

**Correct Answer: B**

 **flurgen248** 3 months, 1 week ago

**Selected Answer: B**

Correct Answer is B.

A: AzureCloud is the wrong tag. Apparently would need to be AzurePlatformLM-Windows licensing or key management service.  
<https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview#available-service-tags>

B: Something is blocking access to KMS, so a route should fix that.  
<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-activation-problems#cause>

C: DNAT rules are inbound only.

D: A Nat rule wouldn't work, for reasons.  
<https://learn.microsoft.com/en-us/azure/load-balancer/outbound-rules>  
upvoted 2 times

 **tester2023** 4 months, 3 weeks ago

The article below is a simiar scenario and it points out you need a route (in our case FW or Route Table) that will route traffic to the Microsoft KMS service on port 1688.

<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/custom-routes-enable-kms-activation>  
upvoted 2 times

 **TJ001** 5 months ago

There are two options ...

- 1) Add specific outbound rule for KMS in the FW as there is already default route points FW
- 2) Add specific address prefix route in route table so it can by pass default route to FW

In this case the chosen Answer - B looks correct

upvoted 3 times

 **NoeHdzMII** 5 months, 1 week ago

Correct answer C.

"DNAT rules implicitly add a corresponding network rule to allow the translated traffic."

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat>  
upvoted 1 times

 **alfonzo47** 5 months ago

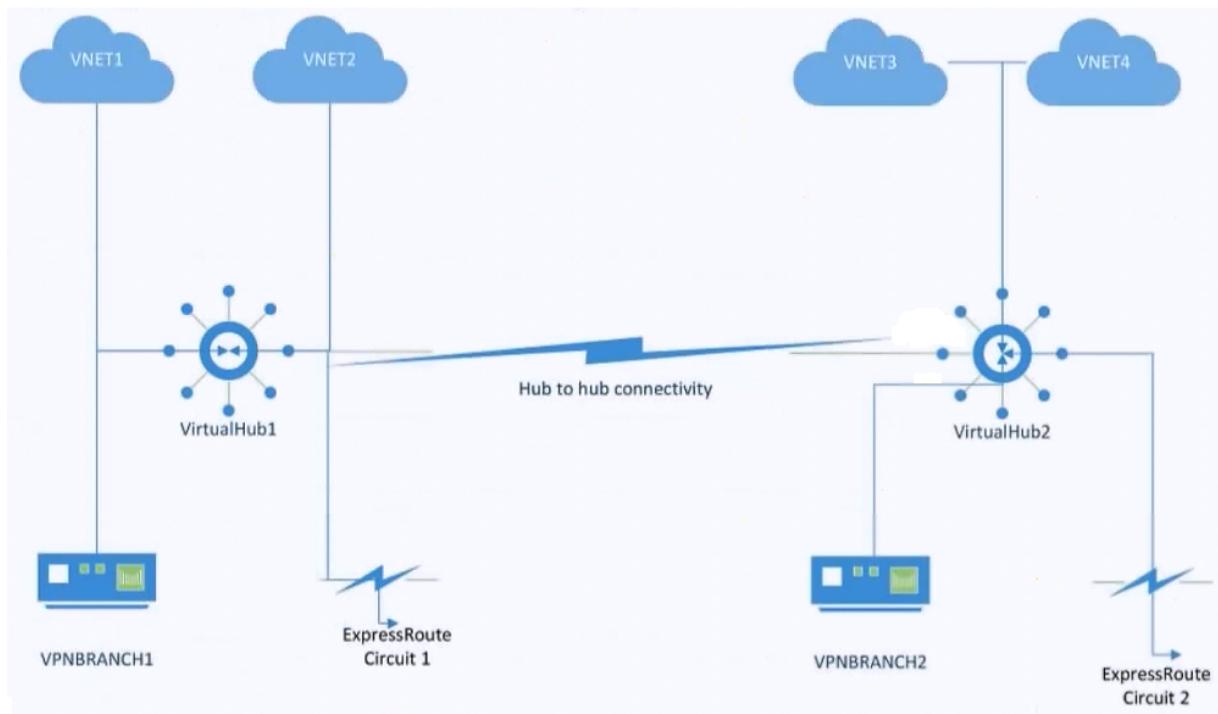
i think that DNAT is only for inbound rules. In this case the windows VMs will try to reach the KMS server (outbound traffic) hence i would go with option B even tho there is no service tag for KMS that can be chosen...

upvoted 1 times



You have an Azure subscription.

You plan to implement Azure Virtual WAN as shown in the following exhibit.



What is the minimum number of route tables that you should create?

- A. 1
- B. 2
- C. 4
- D. 6

**Correct Answer: B**

**DeepMoon** Highly Voted 5 months, 1 week ago

Standard Virtual WAN is enabled due to the presence of a router in every virtual hub. This router is instantiated when the virtual hub is first created.

If it has a router. Then it needs a routing table. Therefore two hubs. Two routing tables.

upvoted 7 times

**Salem2020s** 4 months, 4 weeks ago

can you please explain more? why dont we add routing tables for each Vnet as well?

upvoted 2 times

**DeepMoon** 5 months, 1 week ago

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

upvoted 1 times

**MrBlueSky** Most Recent 2 months, 1 week ago

Question is flawed because VWAN creates its own routes. Yes you would technically need at least two route tables, but the question asks about creating them. You wouldn't need to create these since it will create the routes on its own

upvoted 4 times

**flurgen248** 3 months, 1 week ago

**Selected Answer: B**

The given answer is correct. The minimum number of route tables you can have for this setup is 2.

By default, all connections are associated to a Default route table in a virtual hub. Each virtual hub has its own Default route table, which can be edited to add a static route(s). Routes added statically take precedence over dynamically learned routes for the same prefixes.

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

upvoted 2 times

✉ **wooyourdaddy** 3 months, 1 week ago

**Selected Answer: B**

Assuming the VNETs are using Hub virtual network connections, then each connection is associated to one route table. Associating a connection to a route table allows the traffic to be sent to the destination indicated as routes in the route table. The routing configuration of the connection will show the associated route table. Multiple connections can be associated to the same route table. All VPN, ExpressRoute, and User VPN connections are associated to the same (default) route table.

By default, all connections are associated to a Default route table in a virtual hub. Each virtual hub has its own Default route table, which can be edited to add a static route(s). Routes added statically take precedence over dynamically learned routes for the same prefixes.

Source: <https://learn.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing#association>

As there is no indication in the question that connections were pointed to any specific route table, we would assume they would get added to the Default route table in each virtual hub. So 2 route tables total.

upvoted 1 times

Question #33

Topic 3

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**

✉ **omgMerrick** 4 months ago

**Selected Answer: A**

Answer is correct, Enable floating IP.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-floating-ip#floating-ip>

upvoted 4 times

✉ **TJ001** 5 months ago

Correct Answer

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

If you want to reuse same port for both load balancing rules then Floating IP needs to be enabled

upvoted 4 times

Your company has 40 branch offices that are linked by using a Software-Defined Wide Area Network (SD-WAN). The SD-WAN uses BGP.

You have an Azure subscription that contains 20 virtual networks configured as a hub and spoke topology. The topology contains a hub virtual network named Vnet1.

The virtual networks connect to the SD-WAN by using a network virtual appliance (NVA) in Vnet1.

You need to ensure that BGP route advertisements will propagate between the virtual networks and the SD-WAN. The solution must minimize administrative effort.

What should you implement?

- A. An Azure VPN Gateway that has BGP enabled
- B. a NAT gateway
- C. Azure Traffic Manager
- D. Azure Route Server

**Correct Answer: D**

✉️  **DeepMoon** Highly Voted 5 months, 1 week ago

<https://learn.microsoft.com/en-us/azure/route-server/overview>

Azure Route Server is a fully managed service and is configured with high availability.

Azure Route Server simplifies dynamic routing between your network virtual appliance (NVA) and your virtual network. When BGP Peering is set up with this, it eliminates the need to manually update routes across all connected networks.

upvoted 13 times

✉️  **occupatissimo** 1 month ago

Virtual gateway

A route server propagates to a subnet existing inside a VNet, here the subnet is outside

upvoted 2 times

✉️  **TJ001** 5 months ago

Agree with the answer

upvoted 3 times

**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**

To add VM4 to LB1, you must create a new backend pool.

**Yes****No**

VM1 is connected to Vnet2.

Connections to HTTPS://10.3.0.7 will be load balanced between VM1, VM2, and VM3.

**Answer Area****Statements**

Correct Answer:

To add VM4 to LB1, you must create a new backend pool.

**Yes****No**

VM1 is connected to Vnet2.

Connections to HTTPS://10.3.0.7 will be load balanced between VM1, VM2, and VM3.

✉️  **Goofer**  5 months, 1 week ago

Y - VM4 is in another Vnet. A backend pool can only contain resources from one virtual network.

Y - Backend pool Virtual Network is Vnet2. VM1 is in Vnet2

N - Load balancing rule: rule1 (Tcp/80) is HTTP not HTTPS

upvoted 13 times

✉️  **\_fvt**  2 months, 2 weeks ago

N - 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 (in fact same vnat than the first frontend IP chosen at deployment: then you can't create another Frontend IP in a different VNet or remove all frontend IP; So it's not possible to change this VNet once LB is deployed). Backend pools must be in the same VNet than the Frontend IP. So in facts a Loadbalancer cannot span multiple vnets. (all tested in lab) (may change with cross-region load balancer which is still in preview <https://learn.microsoft.com/fr-fr/azure/load-balancer/cross-region-overview>)

Y - Loadbalancer backend pool is in VNet2 so following the explanations above, all the VMs in the pool are in VNet 2. So VM1 which is in this backend pool is in VNet2.

N - 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.

upvoted 3 times

✉️  **wooyourdaddy** 2 months, 2 weeks ago

The fist answer is no because VM4 exists in VNET3/Subnet3, so it can never be added to LB1, even as a 2nd backend pool. We can see the LB has a private address, meaning it is an internal LB. When you create the ILB, it assigns the FE configuration to a VNET/Subnet of your choosing. When you go to the backend pool page, the Virtual Network is always hardcoded to the VNET your FE is assigned to. When you click on "+ Add a backend pool", you get the Add backend pool page, which states:

IP configurations

IP configurations associated to virtual machines and virtual machine scale sets must be in same location as the load balancer and be in the same virtual network.

The answer to question 1 also confirms that the 2nd answer is Yes, as the VMs need to be in the same VNET as the LB Virtual Network which the question defines as VNET2.

The 3rd answer is no, because the inbound rule is for HTTP (Port 80) only. No HTTPS (Port 443).

upvoted 1 times

✉️  **MightyMonarch74** 2 months, 3 weeks ago

N - Tested in lab and confirmed once 1 backend pool has been configured you cannot add another backend pool on a different VNET, the original VNET is always selected.

Y - VM1 is on VNET2

N - rule 1 is TCP/80, not 443 (HTTPS)

upvoted 4 times

✉️  **Apptech** 2 months, 4 weeks ago

NYN is the correct answer:

It is important to note that the backend pool configuration for backend1 is set to "NIC", which means that the load balancer is configured to load balance traffic between the network interfaces associated with the virtual machines (VMs) in the backend pool.

In order to add VM4 to LB1, you would need to create a new NIC for VM4 that is associated with a subnet in the same virtual network as the existing backend pool, Vnet2. This would allow LB1 to load balance traffic between the NICs associated with all the VMs in the backend pool, including VM4.

upvoted 2 times

✉️  **AzureLearner01** 3 months ago

Provided answer is correct. NYN. 1. You can't add the VM to the loadbalancer because

IP configurations associated to virtual machines and virtual machine scale sets must be in same location as the load balancer and be in the same virtual network.

2. True because of the previous sentence

3. No https is not in the rule

upvoted 2 times

✉️  **flurgen248** 3 months, 1 week ago

I think it's NYN.

1. It says the backend pool is NIC based, and I can't find anything saying that resources in a NIC based backend pool have to be in the same VNET.

If it were IP-based, that is directly stated in this link: <https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management#limitations>

I assume that link would say if it were also a requirement for NIC based backend pools.

2. VM1 is in the backend pool, which is assigned to VNET2.

3. rule1 is on port 80, which is HTTP. HTTPS requires port 443.

upvoted 1 times

✉️  **flurgen248** 3 months, 1 week ago

Maybe it's YYN. There's just so little information about NIC based backend pools that I can't find proof one way or the other.

upvoted 1 times

✉️ **Ayokun** 3 months, 4 weeks ago

Y Y N

- 1) A VM on a different Vnet cannot be added on a backend LB on VNET2 | VM4 on VNET 3
  - 2) VM1 is connected in VNET 2
  - 3) Watch out the rule is on "HTTP" = 80 port not on "HTTPS" = 443
- upvoted 4 times

✉️ **omgMerrick** 4 months ago

Yes Yes No.

To add VM4 to LB1, you must create a new backend pool.

Yes. In order to add VM4 to LB1, you must create a new backend pool that includes VM4's network interface (vm4981) in Vnet3/Subnet3.

VM1 is connected to VNET2.

Yes. VM1 is a part of the backend pool "backend1" which is associated with the virtual network Vnet2.

Connections to https://10.3.0.7 will be load balanced between VM1, VM2, and VM3.

No. The load balancing rule "rule1" is configured to load balance traffic on TCP port 80, not HTTPS (TCP port 443). Therefore, connections to https://10.3.0.7 will not be load balanced by LB1.

upvoted 4 times

✉️ **GeorgeMilev91** 5 months ago

Backend hosts have to be in the same vnet - <https://stackoverflow.com/questions/66529619/can-azure-internal-loadbalancer-have-backends-belonging-to-different-subnets-in>

upvoted 2 times

✉️ **alfonzo47** 5 months ago

N Y N - Backend resources must be in the same virtual network as the load balancer for IP based load balancers <https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management#limitations>.

1, Since Vms in the current backed pool are in Vnet2 we can assume that load balancer is also in vnet2. Hence vms from Vnet3 cant be added as backend resources = N.

2, VM must be in the same vnet as load balancers backend pool so it must be in vnet2 = Y.

3,Https defaults to port 443 and there is not load balancing rule for port 443 = N

upvoted 3 times

✉️ **TJ001** 5 months ago

so 1. is Y not N !

upvoted 5 times

✉️ **NoeHdzMII** 5 months, 1 week ago

A backend pool can only contain resources from one virtual network.

HTTPS is using port tcp 443

upvoted 3 times

✉️ **eVo3000** 5 months, 1 week ago

I think we need to create a new backend pool

upvoted 3 times

✉️ **tester2023** 4 months, 2 weeks ago

Disagree.

The question shows "Backend pool configuration: NIC" for the existing pool, which means any new VMs added by NIC must be from the same vNet.

If we create a new backend pool that is IP-based, Microsoft states, "The backend resources must be in the same virtual network as the load balancer for IP based LBs"

Reference:

<https://learn.microsoft.com/en-us/azure/load-balancer/backend-pool-management#limitations>

upvoted 2 times

✉️ **tester2023** 4 months, 3 weeks ago

Creating a new backend pool will not allow you to add a VM that is on a different vNet.

upvoted 1 times

## DRAG DROP

Your company, named Contoso, Ltd., has an Azure subscription that contains the resources shown in the following table.

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

You plan to deploy Azure Front Door. The solution must meet the following requirements:

- Requests to a URL of https://contoso.azurefd.net/uk must be routed to App1uk.
- Requests to a URL of https://contoso.azurefd.net/us must be routed to App1us.
- Requests to a URL of https://contoso.azurefd.net/images must be routed to the storage account closest to the user.

What is the minimum number of backend pools and routing rules you should create? To answer, drag the appropriate number to the correct components. Each number 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.

## Number

## Answer Area

Backend pools:

Routing rules:

## Answer Area

Correct Answer: Backend pools:

Routing rules:

  tester2023  4 months, 2 weeks ago

3 Backend Pools | 3 Rules

I believe this is a Classic Front Door question. The first reference link provides an overview of classic routing. The questions shows we have a single frontend (contoso.azurefd.net) and there are three paths - /uk, /us, and /images.

The second link shows the three paths would each be a separate rule.

Regarding the number of backend pools, the question states, "...must be routed to [App1uk or App1us]" for the two App Services. The third link does not indicate there is a way to route traffic to a specific app service based on location. However, if we put each app service in its own backend pool, we can have the path rule route to the correct App Service everytime. The Latency routing logic is fine for storage accounts, but not the App Services based on the question requirements.

#### References

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

upvoted 9 times

✉️ **Kafura** 2 months ago

I agree

upvoted 1 times

✉️ **Mbrigaldino97** Highly Voted 5 months ago

correct answer should be 2 and 2.

You have 1 Frontend, which is contoso.com, this is one frontend with a custom domain and not App Service as origin!

You then create 2 Backend Pools, (1 for the App Services, one for both Storage Accounts) and 2 routing rules -> 1 routing rule containing both entries for the App Services (/uk and /us) and 1 for the Storage Accounts (/images). The latter one will be configured to route by latency (default)

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

<https://learn.microsoft.com/en-us/azure/frontdoor/front-door-route-matching?pivot=front-door-standard-premium#frontend-host-matching>

The App Service Routing Rules specifies the precise paths, the Storage Account routing rule

upvoted 5 times

✉️ **TJ001** 5 months ago

for storage account yes ...it will be one pool containing two storage accounts... but for app service it should be separate as the routing is totally path based ...so 3 ,3

upvoted 6 times

✉️ **roshingrg** Most Recent 1 week, 2 days ago

To meet the requirements mentioned, you would need to create the following backend pools and routing rules:

Backend pools:

Backend pool for App1uk: This backend pool will include the App1uk Azure App Service.

Backend pool for App1us: This backend pool will include the App1us Azure App Service.

Backend pool for the storage account closest to the user: This backend pool will include the storage account in the location closest to the user.

Routing rules:

Routing rule for <https://contoso.azurefd.net/uk>: This routing rule will route requests to the App1uk backend pool when the URL is <https://contoso.azurefd.net/uk>.

Routing rule for <https://contoso.azurefd.net/us>: This routing rule will route requests to the App1us backend pool when the URL is <https://contoso.azurefd.net/us>.

Routing rule for <https://contoso.azurefd.net/images>: This routing rule will route requests to the backend pool for the storage account closest to the user when the URL is <https://contoso.azurefd.net/images>.

Therefore, the minimum number of backend pools to create is 3, and the minimum number of routing rules to create is also 3.

upvoted 1 times

✉️ **Cabelen** 2 months, 3 weeks ago

2 and 2, 2 different websites required each one requires 1 backend pool and 1 rules.

upvoted 1 times

✉️ **Apptech** 2 months, 4 weeks ago

Agree to 3 backend pools and 3 Rules. Check this video on minute 4:37: <https://www.bing.com/videos/search?q=azure+front+door+%22latency%22+traffic-routing&&view=detail&mid=DB458D3377D5DDEBD61DDB458D3377D5DDEBD61D&&FORM=VRDGAR&ru=%2Fvideos%2Fsearch%3Fq%3Daz>

ure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26qs%3Dn%26form%3DQBVR%26%3D%2525elhren%2520Suchverlauf%2520verwalten%2525E%26sp%3D-1%26lq%3D0%26pq%3Dazure%2520front%2520door%2520%2522latency%2522%2520traffic-routing%26sc%3D10-42%26sk%3D%26cvid%3D2EA1718352724A27AAB92A15B0444F7B%26ghsh%3D0%26ghacc%3D0%26ghpl%3D

You can see that a rule maps a frontend host (in our case contoso.azurefd.net) and a matching URL path to a specific backend pool. So, it is a 1:1 relation. Each URL needs 1 backend pool. We have three URLs. /uk, /us, /images. Backend Pool for uk contains 1 backend, same for us.

Backend pool for images contains 2 backends. Within the routing rule you can define routing method

upvoted 1 times

✉️ **saad\_SEIU** 2 months, 4 weeks ago

I asked ChatGPT, answer is 3 rules and 4 backend pools and I think that is correct.

The backend pools would be:

App1uk pool - contains the backend instances for the UK app

App1us pool - contains the backend instances for the US app

StorageAccountUK pool - contains the backend instance for the storage account storing images for users in the UK

StorageAccountUS pool - contains the backend instance for the storage account storing images for users in the US

The routing rules would be:

Route requests to <https://contoso.azurefd.net/uk> to the App1uk backend pool.

Route requests to <https://contoso.azurefd.net/us> to the App1us backend pool.

Route requests to <https://contoso.azurefd.net/images> to the appropriate backend pool based on the geographic location of the user.

- a. If the user is located in the UK, route the request to the StorageAccountUK pool.
- b. If the user is located in the US, route the request to the StorageAccountUS pool.

So, you would need three routing rules and four backend pools to meet the requirements you specified.

upvoted 1 times

✉️ **DeepMoon** 5 months, 1 week ago

Each URL is a separate 'edge front end' on Azure Front Door with its own Routing Rule and its own backend pool.

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

upvoted 2 times

✉️ **DeepMoon** 5 months, 1 week ago

But correcting myself there are 3 frontends here; each frontend with a rule will require 3 rules.

upvoted 6 times

✉️ **TJ001** 5 months ago

I agree with this 3 urls needed 3 rules...

upvoted 5 times

✉️ **TJ001** 5 months ago

it is called origin groups and not backend pool ....frontend is called endpoint...

upvoted 1 times

**HOTSPOT**

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

Name	Location
RG1	East US
RG2	UK West

You have the virtual networks shown in the following table.

Name	Location	Subnet	Resource group
Vnet1	East US	Sb1	RG1
Vnet1	East US	Sb2	RG1
Vnet2	West US	Sb3	RG2
Vnet2	West US	Sb4	RG2

Vnet1 contains two virtual machines named VM1 and VM2. Vnet2 contains two virtual machines named VM3 and VM4.

You have the network security groups (NSGs) shown in the following table that include only default rules.

Name	Associated to
Nsg1	Sb1
Nsg2	Network interface of VM2
Nsg3	Network interface of VM3
Nsg4	Sb4

You have the Azure load balancers shown in the following table.

Name	Resource group	Location	Type	Backend pool	Virtual machine	Rule
Lb1	RG1	East US	Public	Vnet1	VM1	Protocol: TCP Port: 80 Backend port: 80
Lb2	RG2	West US	Internal	Vnet2	VM3	Protocol: TCP Port: 1433 Backend port: 1433

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

VM2 can be added to the backend pool of Lb2.

Yes

No

VM4 can access VM3 via port 1433 by using the frontend address of Lb2.

Yes

No

VM1 can be accessed via port 80 from the internet by using the frontend address of Lb1.

Yes

No

Answer Area		
	Statements	Yes
Correct Answer:	VM2 can be added to the backend pool of Lb2.	<input type="radio"/>
	VM4 can access VM3 via port 1433 by using the frontend address of Lb2.	<input checked="" type="radio"/>
	VM1 can be accessed via port 80 from the internet by using the frontend address of Lb1.	<input checked="" type="radio"/>

✉ **NoeHdzMII** Highly Voted 5 months, 1 week ago

1. NO. A backend pool can only contain resources from one virtual network. VM2 (VNet1) VM3 (VNet2)
- 2.YES. using the frondend ip address.
3. NO. the defualt NSGs are blocking any ingress internet traffic

upvoted 12 times

✉ **Goofer** 5 months, 1 week ago

3. YES. NSG is Blocking ingress internet traffic but not traffic from the load balancer. (AllowAzureLoadBalancerInBound)

upvoted 6 times

✉ **tfkfk** 3 weeks, 2 days ago

3.YES.

Inbound default Security Rules:

AllowVNetInbound: Allows inbound traffic from within the virtual network.  
AllowAzureLoadBalancerInbound: Allows inbound traffic from Azure Load Balancer.  
DenyAllInbound: Denies all inbound traffic from any source.

so as Goofer said NSG is Blocking ingress internet traffic but not traffic from the load balancer.

upvoted 1 times

✉ **JohnnyChimp0** 1 month ago

- 3 is YES - Default NSG rules all have a AllowAzureLoadBalancerInbound rule

upvoted 1 times

✉ **occupatissimo** 3 weeks, 2 days ago

that's for LB probes, not for client traffic

upvoted 1 times

✉ **SaadKhamis** 1 month, 2 weeks ago

3. Tested in the lab and confirmed answer to be NO.
- A rule for port 80 must be added to the NSG to be able to reach VM1 using port 80.

upvoted 2 times

✉ **Madball** 4 months, 2 weeks ago

Completely agree with this.

upvoted 1 times

✉ **occupatissimo** Most Recent 1 month ago

3. always start learning from overview: <https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>
- Standard -> Standard load balancers and standard public IP addresses are closed to inbound connections unless opened by Network Security Groups.
- Basic -> open to the internet by default

In this case SKU is missing ....

upvoted 1 times

✉ **occupatissimo** 1 month ago

however basic is never for production so .... 3 is N  
upvoted 1 times

✉ **sierra1784** 1 month, 2 weeks ago

3. NO - When you create NSGs to filter traffic coming through an Azure Load Balancer, the source port and address range applied are from the originating computer, not the load balancer frontend.

upvoted 1 times

✉ **flurgen248** 1 month, 3 weeks ago

1. No - It's in another VNET and would need another backend pool
2. Yes - It's in the same VNET, so default rules allow it.

3. No -

Virtual machines in load-balanced pools: The source port and address range applied are from the originating computer, not the load balancer. The destination port and address range are for the destination computer, not the load balancer.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#azure-platform-considerations>

So the NSG would still block traffic internet traffic, because the Source IP isn't from the load balancer.

upvoted 1 times

✉ **hal01** 2 months ago

NO,YES,No

NO, VM2 is not in the VNET 2 so it's an another network and cannot be add to the backend pool

YES, because they can use the public ip address

NO, because the the network security groups (NSGs) include only default rules

upvoted 1 times

✉ **\_fvt** 2 months, 2 weeks ago

N - VM2 is not in the same VNet and cannot be added to the backend pool

Y - VM4 is in the same VNet than Lb2 so it can access his fronted IP therefore access VM3 through it

Y - VM1 is in Lb1 backend pool. Lb1 is a public LB and rule specify port 80

NSGs should not be an issue there because it's specified that they have default rules only. These default rules allow Inbound Loadbalancers traffic; VNet to VNet traffic (inbound and outbound); and outbound internet access.

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

upvoted 1 times

✉ **\_fvt** 2 months, 2 weeks ago

After further reading, the 3rd should be "No": Azure Load Balancer is not an App Gateway / a Reverse Proxy and doesn't replace the client IP address.

<https://stackoverflow.com/questions/59541796/how-to-restrict-direct-access-from-internet-to-azure-public-loadbalancer-backend>

"for example, client1 send a request to backend via LB front IP, it will generate a flow source client1, source port, protocol, destination LB IP, destination port. When hitting the load balancer, with Inbound NAT rules, it will change to source client1, source port, protocol, destination VM IP, dest port but the source IP for incoming traffic does not change, the NSG rule still is evaluated with the same source IP in the inbound rules. with LB or not, it will work the same for a client for NSG rules."

upvoted 3 times

✉ **alkorkin** 5 months ago

3. Will be YES just in case we have Basic LB. Standard requires NSG in order to explicitly open access from the Internet

upvoted 2 times

✉ **DeepMoon** 5 months, 1 week ago

1. No - Lb2 is a ILB in US West. VM2 is in East US. ILB cannot use cross region load balancing.

<https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-basic-upgrade-guidance#basic-load-balancer-sku-vs-standard-load-balancer-sku>

2. Yes- VM3 is connected to Lb2 and backend port 1433

3. Yes - Port 80 is opened on Lb1.

upvoted 2 times

✉ **TJ001** 5 months ago

3- port is defined in LB1 but not in the default NSG attached

upvoted 1 times

✉ **TJ001** 5 months ago

my bad ...did not watch that the load balancer is a public so 3. YES

upvoted 2 times

✉ **DeepMoon** 5 months, 1 week ago

Box 1 : can be Yes depending on the load balancer SKU being basic or standard. That is currently not given. So you cannot definitively answer this question.

upvoted 1 times

✉ **tester2023** 4 months, 3 weeks ago

The issue isn't SKU-related. The issue with adding the VM is that it is on a different vNet than the LB, which isn't allowed.

## Question #38

## Topic 3

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

Name	Type	Description
App1	Azure App Service	A web app
Gateway1	Azure Application Gateway	includes an SSL certificate that has a subject name of *.contoso.com

Gateway1 provides access to App1 by using a URL of <https://app1.contoso.com>.

You create a new web app named App2.

You need to configure Gateway1 to enable access to App2 by using a URL of <https://app2.contoso.com>. The solution must minimize administrative effort.

What should you configure on Gateway1?

- A. a backend pool and a routing rule
- B. a listener and a routing rule
- C. a listener, a backend pool, and a routing rule
- D. a listener and a backend pool

**Correct Answer: B**

✉  **energie** Highly Voted 4 months, 1 week ago

**Selected Answer: C**

You can't use the same backend pool.

upvoted 7 times

✉  **harshit101** Highly Voted 4 months, 1 week ago

**Selected Answer: C**

Backend pool also needed

upvoted 6 times

✉  **roshingrg** Most Recent 1 week, 2 days ago

In order to enable access to App2 through Gateway1 with the URL <https://app2.contoso.com>, you need to configure the following components:

Listener: A listener is responsible for handling incoming traffic and directing it to the appropriate backend pool based on the defined routing rules. In this case, you need to configure a new listener on Gateway1 to handle requests for the URL <https://app2.contoso.com>.

Backend Pool: A backend pool is a collection of resources that can serve the incoming requests. In this scenario, you need to create a new backend pool specifically for App2, which will contain the necessary resources (in this case, the web app App2).

Routing Rule: A routing rule determines how the incoming requests should be forwarded to the appropriate backend pool. In this case, you need to create a routing rule that matches requests for the URL <https://app2.contoso.com> and directs them to the backend pool associated with App2.

By configuring a listener, a backend pool, and a routing rule, you can ensure that Gateway1 routes the incoming requests for <https://app2.contoso.com> to the correct backend pool (App2), thus enabling access to App2 through the specified URL.

upvoted 1 times

✉  **\_fvt** 2 months, 2 weeks ago

**Selected Answer: C**

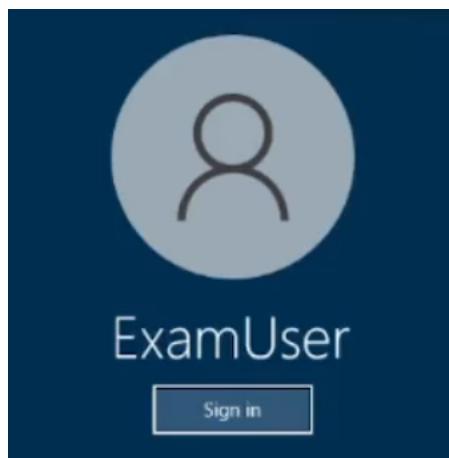
You will have to use a multi site listener to be able to listen on the same (HTTPS) for specific host only, then you will create a routing rule to a NEW back-end pool (you don't want to balance the traffic between the two app service but separate it for each listener)

upvoted 1 times

✉  **MightyMonarch74** 2 months, 3 weeks ago

backend pool and rule

upvoted 1 times

**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: xxxxxxxxx

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 plan to deploy a firewall to subnet1-2. The firewall will have an IP address of 10.1.2.4.

You need to ensure that traffic from subnet1-1 to the IP address range of 192.168.10.0/24 is routed through the firewall that will be deployed to subnet 1-2. The solution must be achieved without using dynamic routing protocol.

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

#### Correct Answer:

Custom routes, User-defined

You can create custom, or user-defined(static), routes in Azure to override Azure's default system routes, or to add more routes to a subnet's route table. In Azure, you create a route table, then associate the route table to zero or more virtual network subnets. Each subnet can have zero or one route table associated to it.

Create a route table (Skip Step 1 to Step 4 if route table already present=

Step 1: From the Azure portal menu, select + Create a resource > Networking > Route table, or search for Route table in the portal search box.

Step 2: Select Create.

Step 3: On the Basics tab of Create route table, enter or select information:

The screenshot shows the 'Create Route table' wizard on the 'Basics' tab. It includes fields for Project details (Subscription: Contoso Subscription, Resource group: myResourceGroup), Instance details (Region: East US, Name: myRouteTablePublic, Propagate gateway routes: Yes selected), and navigation buttons (Review + create, < Previous, Next : Tags >).

Step 4: Select the Review + create tab, or select the blue Review + create button at the bottom of the page.

#### Create a route

In this section, you'll create a route in the route table that you created in the previous steps.

Step 5: Select Go to resource or Search for myRouteTablePublic (The route table you created earlier) in the portal search box.

Step 6: In the myRouteTablePublic page, select Routes from the Settings section.

Step 7: In the Routes page, select the + Add button.

Step 8: In Add route, enter or select this information:

Route name: SomeName

Address prefix destination: Select IP Addresses.

Destination IP addresses/CIDR ranges: Enter 192.168.10.0/24 - The address range of to be routed from.

Next hop type: Select Virtual appliance.

Next hop address: Enter 10.1.2.4 (The address of the firewall in the sbunet1-2 subnet).

#### Reference:

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

<https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table-portal>

correct, by as the last step, you should associate the routing table with subnet 1-1  
upvoted 10 times

Question #40

Topic 3

You have two Azure virtual networks in the East US Azure region as shown in the following table.

Name	IP address space
Vnet1	192.168.0.0/20
Vnet2	10.0.0.0/20

The virtual networks are peered to one another. Each virtual network contains four subnets.

You plan to deploy a virtual machine named VM1 that will inspect and route traffic between all the subnets on both the virtual networks.

What is the minimum number of IP addresses that you must assign to VM1?

- A. 1
- B. 2
- C. 4
- D. 8

**Correct Answer: B**

✉  **Kipper\_2022** 1 month ago

**Selected Answer: A**

agree with Jonav94  
upvoted 1 times

✉  **jonav94** 1 month, 2 weeks ago

**Selected Answer: A**

I think it must be 1, both vnets are peered so we don't need to add an IP from each vnet.  
upvoted 4 times

✉  **\_fvt** 2 months, 2 weeks ago

**Selected Answer: A**

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq#can-azure-firewall-forward-and-filter-network-traffic-between-subnets-in-the-same-virtual-network-or-peered-virtual-networks>

Can Azure Firewall forward and filter network traffic between subnets in the same virtual network or peered virtual networks?

Yes. However, configuring the UDRs to redirect traffic between subnets in the same VNET requires additional attention. While using the VNET address range as a target prefix for the UDR is sufficient, this also routes all traffic from one machine to another machine in the same subnet through the Azure Firewall instance. To avoid this, include a route for the subnet in the UDR with a next hop type of VNET. Managing these routes might be cumbersome and prone to error. The recommended method for internal network segmentation is to use Network Security Groups, which don't require UDRs.

upvoted 4 times

✉  **MrBlueSky** 2 months, 1 week ago

This link and answer are completely irrelevant to the question being asked.

The question asks about setting up a VM to perform this traffic inspection, not an Azure Firewall. The VM would function as a Network Virtual Appliance (NVA). NVAs are frequently configured as Firewalls using third party OS (Barracuda, Palo Alto, Cisco, etc), but this doesn't make it an Azure Firewall.

This should be easily doable with a single IP on the NIC attached to the VM that will be configured as an NVA.

Answer = 1

upvoted 5 times

You have an Azure subscription that contains the following resources:

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

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

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

What should you do?

- A. On FW1, configure a DNAT rule for port 1688
- B. Deploy a NAT gateway.
- C. Add an internet route to RT1 for the Azure Key Management Service (KMS).
- D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

**Correct Answer: C**

You have an on-premises network.

You have an Azure subscription that includes a virtual network named VNet1 and a private Azure Kubernetes Service (AKS) cluster named AKS1. VNet1 is connected to your on-premises environment via an Azure ExpressRoute circuit. AKS1 is connected to VNet1.

You need to implement an off-cluster ingress controller for AKS1. The solution must provide connectivity from the on-premises environment to containerized workloads hosted on AKS1.

Which Azure service should you use?

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

**Correct Answer:** A

✉️  **flurgen248** 1 month, 3 weeks ago

**Selected Answer: A**

Answer is A.

The Application Gateway Ingress Controller (AGIC) is a Kubernetes application, which makes it possible for Azure Kubernetes Service (AKS) customers to leverage Azure's native Application Gateway L7 load-balancer to expose cloud software to the Internet.

<https://learn.microsoft.com/en-us/azure/application-gateway/ingress-controller-overview>

upvoted 1 times

✉️  **Ben\_88** 1 week, 1 day ago

But AGIC is within the K8s cluster , question ask for a an ingress controller outside the cluster . would go with D

upvoted 1 times

✉️  **Apptech** 1 month, 4 weeks ago

A is correct. reference: <https://learn.microsoft.com/en-us/azure/application-gateway/ingress-controller-overview>

upvoted 1 times

✉️  **seth\_saurabh84** 2 months, 2 weeks ago

Why not D? AKS by default uses a standard load balancer for ingress. App Gateway will mean we are pointing towards AGIC which is not what the questions mentions.

upvoted 1 times

✉️  **Marcoos** 5 days, 9 hours ago

A load balancer will only do layer 4. Ingress controllers, if i remember correctly, will operate on layer 7 in the vast majority of cases. You need layer 7 functionality to do the type of ingress that's asked for.

upvoted 1 times

✉️  **25max** 2 months, 2 weeks ago

The LB is in front of a service and does not provide ingress controller solution for the cluster only for the service that type is LoadBalancer.

upvoted 3 times

**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 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**

**Correct Answer:**

Set the DNS record target to:

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



MrBlueSky Highly Voted 2 months, 1 week ago

Answer listed is correct: A Secret in Azure Key Vault + FD93.azurefd.net

Source: <https://learn.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>  
upvoted 7 times

**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 Area**

Minimum number of Traffic Manager profiles required:

 1  
 2  
 3  
 4

Correct Answer:

Routing method for the traffic in each region:

 Geographic  
 Performance  
 Priority  
 Weighted

 **manny72** Highly Voted 2 months ago

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

So:

3 minimum profiles

Weighted (the question is the routing method in each region)

upvoted 14 times

✉  **khksoma** 1 month, 2 weeks ago

I agree

It says - App1 traffic must be assigned equally to each App Service instance in each Azure region. So shouldnt it be weighted ? Parent profile will have Geographic routing method, once it hits the child profiles in each region the traffic should be split equally between the instances(50/50).

upvoted 1 times

✉  **stack120566**  2 months, 2 weeks ago

one parent profile configured for 'performance' and 2 child profiles configured for 'priority' each child profile configured on having 2 nodes.

upvoted 5 times

✉  **Apptech**  2 weeks, 3 days ago

Based on this description I would say Performance routing is correct and not the geographical routing: "Performance: Select Performance routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency. Geographic: Select Geographic routing to direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. With this routing method, it enables you to be in compliance with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions." --> <https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods>

My conclusion:

1 parent profile T1 with performance routing

2 child profiles TM2 (North EU) and TM3 (EAST US) with weighted routing (50/50) and minChildEndpoint=1

upvoted 1 times

✉  **Apptech** 2 weeks, 3 days ago

in addition: we also have to think which method (geographic / performance) is better to route equally between the instances when requests originate from other regions than North Europe and East US

upvoted 1 times

✉  **occupatissimo** 1 month, 2 weeks ago

1) App1 traffic must be assigned equally to each App Service instance in each Azure region. -> weight method (look at the word assigned equally)

2) 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. -> geographic method in a child profile (look at the word "traffic from")

3) If an App Service instance fails, all the traffic for that instance must be routed to the remaining instances in the same region. -> in the child profile set MinChildEndpoints = 1

so 2 profiles and geographic method inside the region

upvoted 1 times

✉  **occupatissimo** 1 month ago

sorry, i was absolutely drunk.

parent profile can be only geographic (if weighted could be EU request sent to US and viceversa)

then we have two location so we need a weighted child profile each one

total 3 profile (1 parent and 2 child) end weighted inside the region

MinChildEndpoints = 1 remain

problem here is how is bild the question, be careful and read well !!

upvoted 1 times

✉  **crypto700** 1 month, 3 weeks ago

the Given Answer is correct

Two profiles

Traffic Manager Profile 1 - Performance Routing method to distribute the traffic equally to each App Service instance in each Azure region.

Traffic Manager Profile 2 - Geographic Routing method

upvoted 1 times

✉  **crypto700** 1 month, 3 weeks ago

I have read the questions again.. it seems we need 3 profiles ( 1 Parent profile with Geographical routing method + 2 Child for each region with Weighted method)

i think the right answers

3 Profile and Weighted for Each Region

upvoted 3 times

✉  **\_fvt** 2 months, 2 weeks ago

I have difficulties understanding how it should be done with 2 or 3 profiles...

I would have created 4 profiles instead:

- TM\_Parent : Geographical

-> World => TM\_Child\_All (AS1 AS2 AS3 AS4 / weighted 50-50)

-> NorthEurope => TM\_Child\_NE (AS3 AS4 / weighted 50-50)

-> NorthAmerica => TM\_Child\_EUS (AS1 AS2 / weighted 50-50)

So TM profiles: TM\_Parent, TM\_Child\_All, TM\_Child\_NE, TM\_Child\_EUS

upvoted 2 times

 **flurgen248** 1 month, 3 weeks ago

It doesn't need to be split evenly across all 4 app service instances, just across the instances in each listed region. You don't need the "World" profile TM\_Child\_All.

upvoted 1 times

Question #45

Topic 3

You have an Azure subscription that contains the Azure App Service web apps shown in the following table.

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

You need to deploy Azure Traffic Manager. The solution must meet the following requirements:

- Traffic to https://www.fabrikam.com must be directed to App1eu.
- If App1eu becomes unresponsive, all the traffic to https://www.fabrikam.com must be directed to App1us.

You need to implement Traffic Manager to meet the requirements.

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

NOTE: Each correct selection is worth one point.

- A. a Traffic Manager profile that uses the priority routing method
- B. a Traffic Manager profile that uses the geographic routing method
- C. a CNAME record in a DNS domain named fabrikam.com
- D. a TXT record in a DNS domain named fabricam.com
- E. a real user measurements key in Traffic Manager

**Correct Answer: AC**

 **\_fvt** Highly Voted 2 months, 2 weeks ago

**Selected Answer: AC**

Priority to force all traffic to active instance

DNS CName on your registrar to the Traffic manager DNS Name

upvoted 5 times

 **Zeppoontstream** 2 months ago

but cant you also use a txt entry for varification?

upvoted 1 times

 **Zeppoontstream** 2 months ago

i just checked the documentation. he is correct.

upvoted 1 times

**HOTSPOT**

You have an Azure subscription that contains an app named App1. App1 is deployed to the Azure App Service apps shown in the following table.

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

You need to publish App1 by using Azure Front Door. The solution must ensure that all the requests to App1 are load balanced between all the available worker instances.

What is the minimum number of origin groups and origins that you should configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Origin groups:

Origins:

**Answer Area**

Correct Answer:

Origin groups:

Origins:

**sierra1784** 1 month, 2 weeks ago

1 group: Multi-region active/active deployment: Create a single origin group. Within that origin group, create an origin for each of the App Service apps.

2 origins: Your App Service app might be configured to scale out across worker instances, but from Front Door's perspective there's a single origin.

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

upvoted 3 times

**occupatissimo** 1 month, 2 weeks ago

Define the origin group as a logical grouping of your application instances that receives the same traffic and responds with an expected behavior, then add the origins to this group.

So 1 group and 2 origins

<https://learn.microsoft.com/en-us/azure/frontdoor/origin?pivots=front-door-standard-premium>

Question #47

*Topic 3*

You have an Azure subscription that contains the following resources:

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

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

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

What should you do?

- A. On FW1, configure a DNAT rule for port 1688.
- B. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- C. Deploy an application security group that allows outbound traffic to 1688.
- D. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.

**Correct Answer: B**

Question #1

Topic 4

You have an Azure virtual machine named VM1.

You need to capture all the network traffic of VM1 by using Azure Network Watcher.

To which locations can the capture be written?

- A. blob storage only
- B. blob storage, a file path on VM1, and a premium storage account
- C. a file path on VM1 only
- D. blob storage and a file path on VM1 only
- E. blob storage and a premium storage account only
- F. a premium storage account only

**Correct Answer: D**

Once your packet capture session has completed, the capture file is uploaded to blob storage or to a local file on the virtual machine. The storage location of the packet capture is defined during creation of the packet capture.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

 **GohanF2** Highly Voted 7 months, 1 week ago

It's correct.

To blob storage account or to VM's valid path.

Storage account or file: Select Storage account, File, or both. If you select File, the capture is written to a path within the virtual machine.

Local file path: The local path on the virtual machine where the packet capture will be saved (valid only when File is selected). The path must be a valid path. If you are using a Linux virtual machine, the path must start with /var/captures.

Storage accounts: Select an existing storage account, if you selected Storage account. This option is only available if you selected Storage.  
upvoted 5 times

 **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 2 times

 **TJ001** 5 months ago

Correct Answer is D

upvoted 2 times

 **TJ001** 5 months ago

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

upvoted 2 times

 **Prutser2** 8 months, 1 week ago

**Selected Answer: D**

as stated

upvoted 1 times

 **jellybiscuit** 8 months, 3 weeks ago

**Selected Answer: D**

It seems illogical to me that you couldn't write to blockblob storage, but M\$ says it's a no-go.

So only blob storage or file path on the VM that is being captured.

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

upvoted 1 times

 **Alessandro365** 9 months ago

**Selected Answer: D**

D is correct.

de acordo com o doc: "Storage account or file: Select Storage account, File, or both. If you select File, the capture is written to a path within the

virtual machine."

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

upvoted 1 times

✉ **leonidagolfe** 9 months, 1 week ago

**Selected Answer: D**

According to the doc:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

"Storage account or file: Select Storage account, File, or both. If you select File, the capture is written to a path within the virtual machine." So D is the correct one.

upvoted 3 times

✉ **gr4** 9 months, 2 weeks ago

**Selected Answer: A**

I would say only blob storage  
SA doesn't have to premium one

upvoted 1 times

✉ **Chriscrown** 9 months, 1 week ago

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal>

Premium storage accounts are currently not supported for storing packet captures

Answer: D

upvoted 2 times

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

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

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

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

What should you do?

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

**Correct Answer: D**

Reference:

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

✉  **izidorf** Highly Voted 1 year, 7 months ago

Network rule is based on port Ivank23. Application rules are based in FQDN. The answer is correct, I suppose.

upvoted 29 times

✉  **Bbb78** 4 months, 2 weeks ago

you can use FQDN in the network rules, network rules are processed before AppRules and if there is a DENY on the outbound traffic in the NETWORK rule - adding to the APPRule will not help

upvoted 1 times

✉  **mammoat** 4 months ago

According to this, you can NOT use FQDN in a network rule

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

upvoted 3 times

✉  **Pravda** Highly Voted 1 year, 5 months ago

D - FQDN

Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.

Network rules that define source address, protocol, destination port, and destination address.

upvoted 15 times

✉  **leotoronto123** 1 year, 5 months ago

thanks!

upvoted 2 times

✉  **tester2023** Most Recent 4 months, 3 weeks ago

DNAT - use a DNAT rule when you want a public IP address to be translated into a private IP address.

Network - use a network rule when you want to filter traffic based on IP addresses, any ports, and any protocols

Application - use an application rule when you want to filter traffic based on fully qualified domain names (FQDNs), URLs, and HTTP/HTTPS protocols

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

upvoted 2 times

✉  **wiki715** 6 months ago

**Selected Answer: D**

as explained here: <https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets>

Application rules

Application rules allow or deny outbound and east-west traffic based on the application layer (L7). You can use an application rule when you want to filter traffic based on fully qualified domain names (FQDNs), URLs, and HTTP/HTTPS protocols.

upvoted 1 times

✉  **Syldana** 8 months ago

**Selected Answer: D**

The requirement mentions the HTTP URL so it can only be done through FQDN application rules

upvoted 2 times

 **lobs\_wort** 11 months ago

**Selected Answer: D**

In exam 22-July-2022.

upvoted 2 times

 **tartarus23** 11 months, 2 weeks ago

D. In a firewall policy, create an application rule.

The requirement mentions the HTTP URL so it can only be done through FQDN application rules

upvoted 1 times

 **Sixfun** 1 year, 1 month ago

**Selected Answer: D**

It is correct answer.

upvoted 1 times

 **HTD** 1 year, 2 months ago

in order words allow https (ssl) traffic thru. APPID and also http .

upvoted 1 times

 **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

 **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022

upvoted 1 times

 **aftab7500** 1 year, 6 months ago

Correct:

Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.

Network rules that define source address, protocol, destination port, and destination address.

upvoted 3 times

 **Ivank23** 1 year, 7 months ago

Is this not supposed to be C. the network rule?

upvoted 1 times

 **Eitant** 1 year, 5 months ago

No. A scenario, contoso.com changed the domain IP address. With networking rule you will have to modify the rules.

upvoted 1 times

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

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

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

What is the minimum number of objects you should create?

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

**Correct Answer: A**

Reference:

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

✉️  **walkwolf3** Highly Voted 1 year, 7 months ago

Answer is correct since all 3 requirements have different conditions and actions.

upvoted 12 times

✉️  **pinchocr** 1 year ago

actions are the same for two of them (block)

upvoted 1 times

✉️  **jeepTango123456** 10 months, 1 week ago

<https://techcommunity.microsoft.com/t5/azure-network-security-blog/azure-waf-custom-rule-samples-and-use-cases/ba-p/2033020>  
"Another concept to make use of in constructing effective Custom Rules is compound conditions. Rules can be created with a single condition, or you can add multiple conditions that must be satisfied to constitute a match. When adding multiple conditions, they are added as an AND statement, so all conditions must be met for the Action to take place. If you need to construct a rule with OR logic, it is best to create multiple rules with the same Action."

so three rules are needed

upvoted 5 times

✉️  **Jamesat** Highly Voted 10 months, 1 week ago

**Selected Answer: A**

I would go with A as you would need 3 separate rules for this.

Rule 1 - Match rule, condition match Australia, action Log

Rule 2 - Match rule, condition match New Zealand action Deny

Rule 3 - Rate Limit rule, condition match IP range and rate, action Deny

upvoted 9 times

✉️  **polinoma** Most Recent 2 months, 1 week ago

The answer should be B, because we are looking for a "minimum number of objects you should create"

Answer A not covering this rule.

You could create three custom rules, one to log all connections from Australia, another to deny all connections from New Zealand, and a third to deny further connections from a network of 131.107.100.0/24 if there are more than 100 connections during one minute.

However, this approach requires creating three custom rules instead of one, which increases the number of objects to manage, so it is not the most efficient solution.

upvoted 1 times

✉️  **MightyMonarch74** 2 months, 3 weeks ago

three custom rules that each has one condition

1 x Geographic - Log Australia

1 x Geographic - Block New Zealand

1 x Rate Limit - limit specific IP

upvoted 1 times

✉️  **GohanF2** 7 months, 1 week ago

Answers are correct.

upvoted 1 times

 **jellybiscuit** 8 months, 3 weeks ago

**Selected Answer: A**

A

The three conditions  
- from australia  
- from new zealand  
- from 131.107.100.0

They are not related and not additive, so you need three rules.

When you add multiple conditions they come with a "and if". There is no "or" option. You have to get "or" with a new rule.  
upvoted 3 times

 **Cristoicach91** 9 months, 3 weeks ago

**Selected Answer: A**

You need 3 rules because you can either allow/deny/log  
upvoted 4 times

 **lobswort** 11 months ago

In exam on 21-July-2022.  
upvoted 1 times

 **cyphe9** 11 months ago

A rule is made of a match condition, a priority, and an action.  
Action types supported are: ALLOW, BLOCK, LOG, and REDIRECT.

3 different conditions = 3 custom rules

upvoted 2 times

 **armand10** 11 months, 4 weeks ago

D correct since each custom rule is mapped only to one action (log,allow, deny).  
upvoted 2 times

 **Kannanthalaiappan** 1 year, 3 months ago

Ans D ??  
one rule type "match" with first two conditions, another rule type "Rate limit" with last condition.  
upvoted 5 times

 **Prutser2** 8 months, 1 week ago

that would require a Boolean OR statement, which is not available under the condition, its on IF which can be combined with AND IF  
upvoted 1 times

 **pinchocr** 1 year ago

You can only give one action "Deny" or "Allow" per rule. Not sure if you can use one rule for block traffic from one region AND per number of request. The other rule would contain the Allow traffic from first region  
upvoted 1 times

 **nitinkumarmca** 1 year, 4 months ago

**Selected Answer: A**

Correct answer is A  
upvoted 3 times

 **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022  
upvoted 1 times

 **Pravda** 1 year, 5 months ago

Variation on exam 1/6/2022  
upvoted 3 times

 **gme999** 1 year, 7 months ago

Correct  
upvoted 3 times

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

You need to use Traffic Analytics.

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

NOTE: Each correct answer selection is worth one point.

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

**Correct Answer: BC**

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

 **sapien45** Highly Voted 8 months, 3 weeks ago

**Selected Answer: BC**

Traffic Analytics requires the following prerequisites:

A Network Watcher enabled subscription.

Network Security Group (NSG) flow logs enabled for the NSGs you want to monitor.

An Azure Storage account, to store raw flow logs.

An Azure Log Analytics workspace, with read and write access.

upvoted 8 times

 **gr4** Highly Voted 9 months, 2 weeks ago

**Selected Answer: BC**

This is correct

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq#what-are-the-prerequisites-to-use-traffic-analytics>

upvoted 7 times

**HOTSPOT -**

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

Name	Connected to
VM1	Vnet1/Subnet1
VM2	Vnet1/Subnet2

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

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

You create a private endpoint that has the following settings:

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Statements	Yes	No
From VM2, you can create a container in storage1	<input type="radio"/>	<input type="radio"/>
From VM1, you can upload data to a blob storage container in storage1	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload data to a blob storage container in storage1	<input type="radio"/>	<input type="radio"/>

Correct Answer:

**Answer Area**

Statements	Yes	No
From VM2, you can create a container in storage1	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can upload data to a blob storage container in storage1	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload data to a blob storage container in storage1	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

Correct!

Service Tag "storage" represents Azure Storage Accounts and can only be applied on the Outbound direction.

Here the NSG is denying the access to any Storage account (direction is Outbound, read well) and it is applied on the Subnet level not on the NIC level.

No - VM2 being on the subnet 2 not on subnet 1 will be deny

Yes - VM1 and Private 1 are in the same subnet so VM1 will have access

No - VM2 has been denied the access by the NSG

upvoted 47 times

✉️ **Pamban** 1 year, 6 months ago

Wrong. Lab tested. answer is YES YES YES

There is no block between subnets.

upvoted 19 times

✉️ **waqas** 1 year, 5 months ago

You are wrong. Answer must be NYN. When you configure Private Endpoint then you always mention the Vnet alongwith Subnet. Here Subnet1 is selected for Private endpoint deployment not Subnet2. So According to this article <https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints#network-security-group-rules-for-subnets-with-private-endpoints>

"NSG rules applied to the subnet hosting the private endpoint are not applied to the private endpoint". So VM1 would use private endpoint without any NSG filtering. Whereas Subnet2 will use NSG which has a Deny action. There is no linkage of Subnet 2 Subnet communication as the only subnet configured to Private Endpoint is Subnet1. Thats why the answer is NYN.

upvoted 20 times

✉️ **MikeB19** 1 year, 4 months ago

The nsg in subnet 2 applies to the public IP address of the storage account. In this case the private end point provides a private IP address on subnet 1. And since subnet 1 and 2 are in the same vnet all traffic is routed between the subnets by default. The nsg has no relevance in this scenario. Therefore y y y

upvoted 10 times

✉️ **Fule** 9 months, 1 week ago

ok, it's important to note that security rules in an NSG associated to a subnet can affect connectivity between VMs within it. So, we have that in production, we blocked certain VMs, and Azure resources with NSG, and we have only one VNet with a bunch of subnets, some subnets cant talk with others.

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#intra-subnet-traffic>

upvoted 1 times

✉️ **Fule** 9 months, 1 week ago

ahh now i am a bit confused,

"Private endpoints don't support network policies such as Network Security Groups (NSGs) or Azure Firewall, so security rules won't apply to them. User-defined routes (UDR) are bypassed by traffic coming from private endpoints. User-defined routes can be used to override traffic destined for the private endpoint." i mean than i would say YYY

upvoted 3 times

✉️ **leotoronto123** 1 year, 5 months ago

thanks Waqas ..

upvoted 1 times

✉️ **Prutser2** 8 months, 1 week ago

your lab azure or aws?

upvoted 2 times

✉️ **Pradh** 8 months, 2 weeks ago

Stop fooling and confusing people. Answer is NYN

upvoted 6 times

✉️ **christianpageqc** Highly Voted 1 year, 8 months ago

According to this article <https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints#network-security-group-rules-for-subnets-with-private-endpoints>

"NSG rules applied to the subnet hosting the private endpoint are not applied to the private endpoint". So VM1 would use private endpoint without any NSG filtering.

upvoted 15 times

✉️ **Roman\_Rabodzey** 1 year, 8 months ago

The same is for VM2. There is no rule to deny subnet-to-subnet communication which is open by default. It will have access to a storage account because it uses private endpoint

upvoted 6 times

✉️ **sapien45** 8 months, 2 weeks ago

Well answered Sir

upvoted 1 times

✉️ **srikanth1987** 1 year, 7 months ago

I agree with you @Roman. It's subnet to subnet communication, the source has no idea whether the destination PE belongs to storage or sql or whatever.

upvoted 2 times

✉️ **RandomUser** 1 year, 8 months ago

That gives us 3 yes. And it makes sense as the Service Tag essentially is just a collection of public IP addresses. And we do not use any of PIPs to connect to the storage.

upvoted 7 times

✉️ **WorkHardBeProud** 1 year, 8 months ago

Be careful guys it is not the case anymore.

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

upvoted 2 times

✉️ **Morgana** 1 year, 7 months ago

NSG for private endpoints are "public preview only" I still think the Answer are YES.YES.YES.

upvoted 14 times

✉️ **AjdIfasudfo0** 6 months, 2 weeks ago

this feature is now available, but you still have to opt-in manually

upvoted 1 times

✉️ **Bharat** 1 year, 8 months ago

Yes. You are correct.

upvoted 1 times

✉️ **Crazysaffer** [Most Recent] 3 weeks, 6 days ago

I thought private endpoints ignores NSG's. Therefore everything should be yes

upvoted 1 times

✉️ **25max** 2 months, 2 weeks ago

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

Using service tags to allow or deny traffic to your Azure resources to and from public IP endpoints.

upvoted 1 times

✉️ **\_fvt** 2 months, 2 weeks ago

YYY - Service TAGS are for Public services IP, doesn't contains private endpoints so don't filter any flow to the private endpoint, even on VM NICs or if Network Policies For Private endpoint were enabled for the Subnet where the private endpoint is located.

"<https://learn.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services>"

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

upvoted 1 times

✉️ **\_fvt** 2 months, 2 weeks ago

"Using service tags to allow or deny traffic to your Azure resources to and from public IP endpoints."

upvoted 1 times

✉️ **JennyHuang36** 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 3 times

✉️ **tzatziki** 4 months, 2 weeks ago

...I always wanted to say this... Tested in Lab... And i did just that. All answers are Y. Set the public access level of the containers to blob, did the nsg-rules to the subnets and 2 vms with bastion access and the private endpoint... all test where made with powershell from the vms ... Also pointing out that when the private endpoint was created a note was saying that if i have an nsg on the subnet given, it would be disabled for private endpoints on that subnet... so thats that...

upvoted 7 times

✉️ **TJ001** 5 months ago

will go with yes yes yes...it is very clear private endpoint connections are local and the dns resolution happens to a private IP of the private endpoint and service tag resolves to public IP wont be applicable here

upvoted 2 times

✉️ **phoenix14** 5 months, 3 weeks ago

NYN is Correct because. For outbound traffic, Azure processes the rules in a network security group associated to a network interface first, if there's one, and then the rules in a network security group associated to the subnet, if there's one. This includes intra-subnet traffic as well.

upvoted 1 times

✉️ **Takloy** 7 months, 1 week ago

NYN

N - Outbound is Denied so VM2 can't jump to VM1.

Y - Because of the Private Endpoint

N - Same explanation as the first one.

upvoted 1 times

✉️ **Disparate** 7 months, 2 weeks ago

NYN is correct!

The NSG apply only a VM2 because the private endpoint is only for VM1.

Easy!

upvoted 1 times

✉ **Prutser2** 8 months, 2 weeks ago

the answers above are correct, ONLY if it would have stated priavet1 instead of storage1. because as ppl have stated below, storage1 is really accessible through a public ip address. as per ususal, these questions are sloppy and badly written

upvoted 1 times

✉ **sapien45** 8 months, 2 weeks ago

YYY.

Just tested it

Two VMs in two distincs Subnets, even though the private endpoint is assigned to one subnet , both VMs will have in their Network interface effective routes a destination to the private endpoint, because all traffcis is routed between the subnets by default

upvoted 3 times

✉ **viva6516** 8 months, 2 weeks ago

Have we considered Storage explorer? if the VM can access Storage explorer then surely you can access the blobs and create as well?

upvoted 1 times

✉ **jellybiscuit** 8 months, 3 weeks ago

YYY

The "Storage" service tag refers to storage resources sitting in the Azure cloud.

As soon as you put a private endpoint on the storage account, the NSG becomes irrelevant. It does prevent you from getting to public storage accounts, but does not apply to this one.

Beyond that, you just need to know that the two subnets can communicate by default.

upvoted 5 times

✉ **Prutser2** 8 months, 1 week ago

concur, best explanation i have seen in this discussion

upvoted 1 times

✉ **Alessandro365** 9 months ago

YYY

<https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints#network-security-group-rules-for-subnets-with-private-endpoints>

"NSG rules applied to the subnet hosting the private endpoint are not applied to the private endpoint"

upvoted 2 times

✉ **andry79** 9 months, 1 week ago

Tested in lab and is YYY

upvoted 4 times

HOTSPOT -

You have an Azure firewall shown in the following exhibit.

The screenshot shows the Azure Firewall Manager portal with Firewall1 selected. The page includes a header with a cloud icon, the name Firewall1, a gear icon, and three dots. Below the header are buttons for '>>', 'Delete', and 'Lock'. A message says 'Visit Azure Firewall Manager to configure and manage this firewall.' Under the 'Essentials' section, various configuration details are listed:

Resource group ( <a href="#">change</a> ) RG1	Firewall sku Standard
Location North Europe	Firewall subnet <a href="#">AzureFirewallSubnet</a>
Subscription ( <a href="#">change</a> ) <a href="#">Subscription1</a>	Firewall public IP <a href="#">Firewall-IP1</a>
Subscription ID 489f2hht-se7y-987v-g571-463hw3679512	Firewall private IP 10.100.253.4
Virtual network <a href="#">Vnet1</a>	Management subnet
Firewall policy <a href="#">FirewallPolicy1</a>	Management public IP
Provisioning state Succeeded	Private IP Ranges <a href="#">Managed by Firewall Policy</a>
Tags ( <a href="#">change</a> ) <a href="#">Click here to add tags</a>	

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

On Firewall1, forced tunneling [answer choice]

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

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

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

**Correct Answer:**

**Answer Area**

On Firewall1, forced tunneling [answer choice]

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

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

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

Box 1:

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

Box 2:

The [Visit Azure Firewall Manager to configure and manage this firewall](#) link in the exhibit shows that the firewall is managed by Azure Firewall Manager.

 **jkklim** Highly Voted 1 year, 1 month ago

from 1st diagram, if you see that Management Subnet and Management IP is empty, it means NO FORCE TUNNELING. And of course, force tunnelling can only be enabled during FW creation

upvoted 16 times

 **Geo13AZ** Highly Voted 1 year, 5 months ago

The Answer is correct, but the explanation of the first question has a mistake, it says "the Firewall subnet" but it should be "the Management Subnet would be AzureFirewallManagementSubnet". Also, the "Management Public IP" would be "ManagementPublicIP".  
<https://azure.microsoft.com/en-us/blog/azure-firewall-forced-tunneling-and-sql-fqdn-filtering-now-generally-available/>

upvoted 13 times

 **BlackZeroes** Most Recent 8 months, 3 weeks ago

Answer for both is Cannot be Enabled.

"In Forced Tunneling mode, the Azure Firewall service incorporates the Management subnet (AzureFirewallManagementSubnet) for its operational purposes." This is clearly missing in the screenshot.  
<https://learn.microsoft.com/en-us/azure/firewall/forced-tunneling>

upvoted 1 times

 **MrBlueSky** 2 months, 1 week ago

Wrong.

This AzureFirewallManagementSubnet is not the indicator for if it's being managed by Azure Firewall Manager. The fact that there is a Firewall Policy attached to this is what indicates that Firewall Manager is already in use.

Answers:

1. Cannot be Enabled
2. Already Enabled

upvoted 2 times

 **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022

upvoted 2 times

 **Pravda** 1 year, 5 months ago

Not on exam 1/6/2022

upvoted 3 times

 **AidenYoukhana** 1 year, 5 months ago

The answers are correct!

upvoted 1 times

 **Pamban** 1 year, 6 months ago

appeared on exam 5th Dec 2021

upvoted 3 times

 **sadsak** 1 year, 7 months ago

This answer appears to be correct - <https://docs.microsoft.com/en-us/azure/firewall/forced-tunneling#forced-tunneling-configuration>

upvoted 4 times

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

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

What should you use?

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

**Correct Answer:** C

Reference:

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

✉ **Takloy** Highly Voted 1 year, 5 months ago

**Selected Answer: C**

Correct answer is C.

Connection Monitor provides unified, end-to-end connection monitoring in Azure Network Watcher. The Connection Monitor feature supports hybrid and Azure cloud deployments. Network Watcher provides tools to monitor, diagnose, and view connectivity-related metrics for your Azure deployments.

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

upvoted 5 times

✉ **Alessandro365** Most Recent 9 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

✉ **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 1 times

✉ **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

✉ **jj22222** 1 year, 2 months ago

on test 4.10.2022 Cannot be enabled - forced tunneling on firewall 1  
is enabled already - azure firewall manager

upvoted 3 times

✉ **jj22222** 1 year, 2 months ago

sorry this is for earlier question, this one is connection manager

upvoted 4 times

✉ **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

✉ **nitinkumarmca** 1 year, 4 months ago

**Selected Answer: C**

Correct

upvoted 1 times

✉ **Joshalom** 1 year, 4 months ago

on exam 6/2/2022

upvoted 1 times

✉ **Eitant** 1 year, 5 months ago

**Selected Answer: C**

Correct answer

upvoted 1 times

✉ **Pravda** 1 year, 5 months ago

on exam 1/6/2022

upvoted 3 times

 **JoMa** 1 year, 6 months ago

Correct

Connection monitor probes the connection every 60 seconds, so you can monitor latency over time

upvoted 1 times

 **Dooa** 1 year, 7 months ago

correcta

upvoted 2 times

You have an Azure subscription that contains the following resources:

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

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

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

What should you do?

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

**Correct Answer: B**

Reference:

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

✉  **srs27**  1 year, 6 months ago

This is correct. When you use Force tunneling, then for Windows activation traffic should be allowed for Azure KMS Servers. Either the way mentioned in Option B or you add UDR to point Internet for KMS outbound traffic.

upvoted 5 times

✉  **Grafting** 1 year, 5 months ago

where does it mention force tuneling?

upvoted 1 times

✉  **hendylaja** 1 year, 2 months ago

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

upvoted 2 times

✉  **jellybiscuit** 8 months, 3 weeks ago

I see you learned something from the previous question ;)

upvoted 3 times

✉  **peterquast** 5 months, 2 weeks ago

Incorrect, there would be 2 FW subnets, one regular one and the second which is management one.

upvoted 1 times

✉  **MrBlueSky**  2 months, 1 week ago

Careful, there may be a slightly different worded version of this on the actual exam.

upvoted 1 times

✉  **Skankhunt** 4 months, 2 weeks ago

Déjà vu ^\_~

upvoted 2 times

✉  **Alessandro365** 9 months ago

**Selected Answer: B**

B is correct

upvoted 1 times

✉  **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 1 times

✉  **kinder2** 1 year ago

**Selected Answer: B**

the answer "B" is correct.

you should have this rule

{

```
"ruleType": "NetworkRule",
"name": "azure-to-kms",
"ipProtocols": ["TCP"],
"sourceAddresses": [
"[parameters('envParameters').firewall.properties.baseNetworkPrefix]"
],
"sourceIpGroups": [],
"destinationAddresses": ["23.102.135.246"],
"destinationIpGroups": [],
"destinationFqdns": [],
"destinationPorts": ["1688"]
}
```

upvoted 4 times

✉ **wsrudmen** 1 year ago

**Selected Answer: B**

Correct!

Azure VM activation issues occur if the Windows VM is not configured by using the appropriate KMS client setup key, or the Windows VM has a connectivity problem to the Azure KMS service.

This link is better:

<https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/troubleshoot-activation-problems>

upvoted 2 times

✉ **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

✉ **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

✉ **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022

upvoted 1 times

✉ **Pravda** 1 year, 6 months ago

KMS is the correct answer.

upvoted 3 times

✉ **Bharat** 1 year, 8 months ago

Based on the linked article, it should be D not B, i.e., o Subnet1, associate a network security group (NSG) that allows outbound access to port 1688. Because the Key Management Service Port is 1688.

upvoted 4 times

✉ **Bharat** 1 year, 8 months ago

Apologies. The provided answer is correct upon reading the article carefully.

upvoted 9 times

**HOTSPOT -**

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

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

AppGW1 has the listeners shown in the following table.

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Statements	Yes	No
From 131.107.10.15, you can access www.contoso.com	<input type="radio"/>	<input type="radio"/>
From 131.107.10.15, you can access www.fabrikam.com	<input type="radio"/>	<input type="radio"/>
From 131.107.10.15, you can access www.adatum.com	<input type="radio"/>	<input type="radio"/>

**Answer Area**

Statements	Yes	No
Correct Answer: From 131.107.10.15, you can access www.contoso.com	<input checked="" type="radio"/>	<input type="radio"/>
From 131.107.10.15, you can access www.fabrikam.com	<input checked="" type="radio"/>	<input type="radio"/>
From 131.107.10.15, you can access www.adatum.com	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

 **WorkHardBeProud**  1 year, 8 months ago

Correct !

Say your application gateway has a global policy applied to it. Then you apply a different policy to a listener on that application gateway. The listener's policy now takes effect for just that listener. The application gateway's global policy still applies to all other listeners and path-based

rules that don't have a specific policy assigned to them.

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/policy-overview#per-site-waf-policy>

upvoted 58 times

✉️ **Kafura** 2 months ago

Say your application gateway has a global policy applied to it. Then you apply a different policy to a listener on that application gateway. The listener's policy now takes effect for just that listener. The application gateway's global policy still applies to all other listeners and path-based rules that don't have a specific policy assigned to them

upvoted 1 times

✉️ **llj** 1 year, 6 months ago

correct! global policy only affects the listeners which don't have listener policies applied on them

upvoted 3 times

✉️ **kilosh123** 1 year, 1 month ago

What about the priorities?

upvoted 2 times

✉️ **xavi1** 1 year, 4 months ago

great explanation

upvoted 1 times

✉️ **Morgana** [Highly Voted] 1 year, 7 months ago

Priority [required]

Determines the rule valuation order. The lower the value, the earlier the evaluation of the rule. The allowable range is from 1-100.

Must be unique across all custom rules. A rule with priority 40 is evaluated before a rule with priority 80.

Priority [required]

Determines the rule valuation order. The lower the value, the earlier the evaluation of the rule. The allowable range is from 1-100.

Must be unique across all custom rules. A rule with priority 40 is evaluated before a rule with priority 80.

So the priority 50 is a Deny, and will not allow the connection to listen2 be allowed.

I still go for YES, NO, NO.

upvoted 31 times

✉️ **MightyMonarch74** 2 months, 3 weeks ago

YYN - you can ignore the priority column, as these are all separate WAF custom policies assigned to different components of the app gateway, the priorities would come into play if there were multiple custom rules within the same policy

upvoted 1 times

✉️ **izidorf** 1 year, 7 months ago

Agree. As we have Global deny applied with low priority, Listener 2 won't be allowed. YES, NO, NO.

upvoted 7 times

✉️ **blacknurse** 1 year, 7 months ago

If you read this document <https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/policy-overview#per-site-waf-policy> then the answer is Yes, Yes, No. Because the listener's policy takes effect for just listener 2 despite the priority.

upvoted 26 times

✉️ **JennyHuang36** [Most Recent] 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 2 times

✉️ **afhilal** 4 months, 3 weeks ago

the answer is correct yes, yes, no

upvoted 1 times

✉️ **GohanF2** 7 months, 1 week ago

Also, keep in mind the priorities. The lower the integer number in the "priority" field, the highest the priority to be processed. It's like setting up "metrics" in a network; the lower the integer the higher is the priority.

upvoted 1 times

✉️ **GohanF2** 7 months, 1 week ago

Answer is: YES, NO, NO.

The priority of the policy orders matters.

1. The first one is analyzed by customized rule 1 which is set to allow traffic by default behavior of "Detection mode".

2. The second goes through the Global Policy attached to the Application Gateway which is set to deny and then stops processing rules.

3. It's the same as 2. It goes through the global policy rule which is set to deny and then it stops processing policies. The policy 3 is never processed due to the global policy that is set to deny.

upvoted 2 times

✉️ **wetraining123** 9 months, 4 weeks ago

The answer is correct.

If your Application Gateway has an associated policy, and then you associate a different policy to a listener on that Application Gateway, the

listener's policy will take effect, but just for the listener(s) that they're assigned to. The Application Gateway policy still applies to all other listeners that don't have a specific policy assigned to them.

If you assign a policy to your Application Gateway (or listener) that already has a policy in place, the original policy is overwritten and replaced by the new policy.

upvoted 2 times

 **Azuriste** 10 months ago

For me YES NO NO

upvoted 1 times

 **lobs\_wort** 11 months ago

In exam 21-Jul-22.

upvoted 1 times

 **Payday123** 11 months, 3 weeks ago

Contoso.com - Y - this policy overrides deny for AppGW1. By default traffic is allowed so even if it is set to Detection only it changes nothing and still does not block the traffic

Fabrikam.com - Y - again this policy overrides deny for AppGW1 and it is set to Prevention and allow  
Adatum.com - N - takes policy from AppGW1 so Prevention and deny

upvoted 2 times

 **Payday123** 11 months, 3 weeks ago

Priorities does not matter here because every rule is associated with different listener.

upvoted 4 times

 **Payday123** 11 months, 3 weeks ago

What is default Action in Application Gateway if none of conditions in rules are matching?

upvoted 1 times

 **Payday123** 11 months, 3 weeks ago

I've found it. If there are no custom rules the traffic is scanned by by other global managed rules and allowed.

upvoted 1 times

 **SCATEST** 1 year ago

Policy2 is only in "Detection" mode - so only logging is active but all traffic is allowed: No, Yes, No

upvoted 1 times

 **d3j4n** 1 year ago

N,Y,N Tested in Lab!

upvoted 1 times

 **sapien45** 8 months, 2 weeks ago

YYN. Meth Labs do not count

upvoted 2 times

 **FaceBack** 1 year ago

Correct is YYN

Policy 2 is a deny poliy that will deny all access when no such IP is included.

So we are looking at policies 1,3.

upvoted 1 times

 **RVR** 1 year, 1 month ago

NYN

Policy 2 is in detection mode, so it won't take any action.

upvoted 4 times

 **jkklim** 1 year, 1 month ago

1. Listener takes precedence than at the gateway level.
2. Priority rules takes place WITHIN listener. Look at the screen properly. It is the priority within the listner

Answer is YYN - which is correct

upvoted 3 times

 **VonKellus** 1 year, 2 months ago

my two pence:

yes - request from 131.107.10.15 to www.contoso.com - hits Listener1 which has polciy2 applied, a specific policy overrides the generally applied policy1. Policy2 is in detection mode which means it logs only and doesnt block incoming requests. Once a rule is matched, the corresponding action that was defined in the rule is applied to the request. IN WAF once a rule is matched lower priority rules aren't processed further.

yes - request from 131.107.10.15 to www.fabrikam.com - hits listener2 which has policy 3 applied, this allows traffic from source ip

no - request from 131.107.10.15 to www.adatum.com - no specific listener rule which means the rule applied to appgw1 is matched - working in prevention mode it is set to deny traffic from 131.107.10.15

upvoted 6 times



You have an Azure virtual network that contains a subnet named Subnet1. Subnet1 is associated to a network security group (NSG) named NSG1. NSG1 blocks all outbound traffic that is not allowed explicitly. Subnet1 contains virtual machines that must communicate with the Azure Cosmos DB service. You need to create an outbound security rule in NSG1 to enable the virtual machines to connect to Azure Cosmos DB. What should you include in the solution?

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

**Correct Answer: A**

Reference:

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

✉️  **HTD** Highly Voted 1 year, 1 month ago

The ideal option is a Private point , but the question says outbound connection is needed , then adding a rule with a service tag make sense , also if security is not a concern and cost is needed to be minimum. Else a Private point is a perfect solution here  
upvoted 5 times

✉️  **jeffangel28** 10 months, 2 weeks ago

100% right!  
upvoted 1 times

✉️  **tartarus23** Highly Voted 11 months, 2 weeks ago

Selected Answer: A  
A. a service tag

Create a service tag pointing to Azure Cosmos DB to allow the outbound connectivity.

upvoted 5 times

✉️  **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023  
upvoted 1 times

✉️  **Alessandro365** 9 months ago

Selected Answer: A  
A is correct  
upvoted 2 times

✉️  **zerocool114** 11 months, 2 weeks ago

on exam today  
upvoted 2 times

✉️  **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22  
upvoted 1 times

✉️  **VonKellus** 1 year, 2 months ago

why not B. a private endpoint?  
upvoted 2 times

✉️  **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.  
upvoted 1 times

✉️  **nitinkumarmca** 1 year, 4 months ago

Selected Answer: A  
Service Tags  
upvoted 4 times

 **Joshalom** 1 year, 4 months ago

on exam 6/2/2022

upvoted 1 times

 **Pravda** 1 year, 5 months ago

on exam 1/6/2022

upvoted 3 times

 **Pravda** 1 year, 6 months ago

What is service tag in Azure?

Image result for azure service tags

A service tag represents a group of IP address prefixes from a given Azure service. ... You can use service tags to define network access controls on network security groups or Azure Firewall. Use service tags in place of specific IP addresses when you create security rules.

upvoted 5 times

 **SSTan** 1 year, 6 months ago

User defined service tag to enable connection to Cosmos DB.

upvoted 1 times

 **Pravda** 1 year, 6 months ago

You can use service tags to define network access controls on network security groups or Azure Firewall. Use service tags

upvoted 2 times

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**

 **Payday123** Highly Voted 11 months, 3 weeks ago

**Selected Answer: C**

"Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied."

upvoted 10 times

 **SaadKhamis** Most Recent 1 month, 2 weeks ago

**Selected Answer: C**

Just tested in the lab with the following:

```
$IPMatchCondition = New-AzFrontDoorWafMatchConditionObject -MatchVariable RemoteAddr -OperatorProperty IPMatch -NegateCondition $false -MatchValue "20.234.16.25", "20.234.16.26", "20.234.16.27"
$IPAllowRule = New-AzFrontDoorWafCustomRuleObject -Name "IPAllowRule" -RuleType MatchRule -MatchCondition $IPMatchCondition -Action Allow -Priority 10
$IPAllowPolicyExamplePS = New-AzFrontDoorWafPolicy -Name "IPRestrictionExamplePS" -resourceGroupName rg-test -Customrule $IPAllowRule -Mode Detection -EnabledState Enabled
I, also, created the rule with one IP address then, manually, was able to add two more IPs.
```

upvoted 1 times

 **Darkren4eveR** 2 months, 3 weeks ago

Option B is Correct

upvoted 1 times

 **p0OM22** 2 months, 4 weeks ago

in exam march 23

upvoted 3 times

 **Sbr82** 3 months ago

**Selected Answer: B**

To apply a rate limit of 100 requests for traffic that originates from each office, you should create two additional associations. This is because the current configuration applies a rate limit of 100 requests for traffic that originates from the office in Montreal only. By creating two additional associations, you can apply a rate limit of 100 requests for traffic that originates from each office

upvoted 3 times

 **TJ001** 5 months ago

When a custom rule is created in WAF policy there is option to add IP address not just on but multiple so 1 rule is sufficient ..all that is needed all the edge IPs from all locations in the one rule

upvoted 1 times

 **TJ001** 5 months ago

so agree with Answer C

upvoted 1 times

 **1particle** 10 months, 2 weeks ago

B

Per this link

<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-configure-ip-restriction#create-a-waf-policy>  
You can add an IP address or range only. You would need to create two additional associations for the other 2 locations.

upvoted 1 times

 **pinchocr** 1 year ago

**Selected Answer: C**

It's correct. Lab tested, you can add IP addresses as conditions in the same rule.

upvoted 4 times

✉ **25max** 2 months, 1 week ago

Yes, but in this case the 3 IPs share the 100 request and the task is 100 req/branch so you need 3 rules.

upvoted 1 times

✉ **25max** 2 months, 1 week ago

ignore my comment above, it is IP based and emphasized that the offices has own single

upvoted 1 times

✉ **mdnick** 1 year, 1 month ago

<https://github.com/MicrosoftDocs/azure-docs/issues/32333>, as per the above doc, tried the below. So yes the answer is Modify the condition.  
\$testIPmatches = New-AzFrontDoorWafMatchConditionObject -MatchVariable RemoteAddr -OperatorProperty IPMatch -NegateCondition \$true -MatchValue "103.78.18.242", "103.78.18.245"

upvoted 4 times

✉ **Jorex** 1 year ago

Also through the portal it's clearly visible, if you add an IP another text box appears to add another one.

upvoted 3 times

✉ **milan92stankovic** 1 year ago

That will apply the rate limit of 100 requests in total for all listed IPs.

I haven't tested it yet. If someone has, please teach us :)

upvoted 1 times

✉ **JulienYork** 1 year, 1 month ago

Should be B

Create a two additional associations they are individual resources, individual locations.

upvoted 3 times

✉ **pinpin06** 1 year, 1 month ago

As per the following link <https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell> and this one

<https://azure.microsoft.com/en-us/resources/templates/front-door-rate-limiting/>

I understand that each rate-limit is for a specific IP address only, I never found anything about a group of IPs, so I would consider the response B : create a two additional associations

upvoted 4 times

✉ **vunder** 1 year, 1 month ago

I am a bit confused about this line "Your company has offices in Montreal, Seattle, and Paris. The outbound traffic from each office originates from a specific public IP address." so then when you factor in this line "Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied." from "<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-rate-limit-powershell>", I then see why C is correct.

upvoted 4 times

✉ **lavermil** 10 months ago

Agreed! See the note on the link provided above. It says: "Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied."

upvoted 1 times

You have an Azure virtual network named Vnet1.

You need to ensure that the virtual machines in Vnet1 can access only the Azure SQL resources in the East US Azure region. The virtual machines must be prevented from accessing any Azure Storage resources.

Which two outbound network security group (NSG) rules should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a deny rule that has a source of VirtualNetwork and a destination of Sql
- B. an allow rule that has the IP address range of Vnet1 as the source and destination of Sql.EastUS
- C. a deny rule that has a source of VirtualNetwork and a destination of 168.63.129.0/24
- D. a deny rule that has the IP address range of Vnet1 as the source and destination of Storage

**Correct Answer: BD**

Reference:

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

✉ milan92stankovic Highly Voted 1 year ago

Selected Answer: BD

Correct Answer - B & D

upvoted 8 times

✉ pinchocr Highly Voted 1 year ago

Selected Answer: BD

Correct

upvoted 6 times

✉ Apptech Most Recent 2 months, 2 weeks ago

I don't get it. Default outbound rule for NSG is "allow all". For this case for SQL access requirement we would need answers A + B. For storage access prevention we would also need answer D.

If we would assume that outbound default NSG rule is "deny all" we would need allow rule for Sql.East and an allow rule for storage. So, in none of the scenarios we have a perfect answer option when just choosing 2 answers

upvoted 1 times

✉ \_fvt 2 months, 2 weeks ago

"Each correct answer presents part of the solution." the key is here.

So;

B - because you need to allow only VMs to SQL in specific East US region not All SQL (so not A).

D - because as asked you need to deny VMs to all Storage.

And you'll probably will add a deny rule if you had to complete "parts" of the solution.

upvoted 1 times

✉ staffo 4 months ago

A would work but question only mentions working with VNET1. It does not specifically mention other VNET's. D is more specific.

upvoted 1 times

✉ omgMerrick 4 months ago

Selected Answer: BD

B & D

Explanation:

Rule B allows traffic from the virtual machines in Vnet1 to the Azure SQL resources in the East US Azure region.

Rule D denies traffic from the virtual machines in Vnet1 to any Azure Storage resources.

Rule A is incorrect because it allows traffic from the virtual machines in Vnet1 to any destination that contains "Sql".

Rule C is incorrect because it denies traffic from the virtual machines in Vnet1 to the Azure instance metadata service, which is not related to the given requirements.

upvoted 3 times

✉ rac\_sp 11 months, 1 week ago

Selected Answer: AB

Because Storage is NOT the same as SQL. There are completely different TAGs to SQL and STORAGE.SQL is database, Storage is Storage.

upvoted 1 times

✉  **cypher9** 11 months ago

reference?

upvoted 1 times

✉  **cypher9** 11 months ago

I dont get it, why would you have a deny rule that has a source of VirtualNetwork?

upvoted 1 times

✉  **tng69** 10 months ago

Even if it's not what anyone would do, it is the solution closest to the ideal solution (which would be to set the VM's IP as source)

upvoted 1 times

✉  **rac\_sp** 11 months, 1 week ago

should be A and B. Storage Tags is different from SQL( that is a database actually ). Also take a look that there is a TAG specifically for SQL which is a completely different resource than a Storage.

upvoted 2 times

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

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

You have an Azure subscription that contains the following resources:

- ⇒ A virtual network named Vnet1
- ⇒ A subnet named Subnet1 in Vnet1
- ⇒ A virtual machine named VM1 that connects to Subnet1
- ⇒ Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You configure the firewall on storage1 to only accept connections from Vnet1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

✉  **Alessandro365** 9 months ago

**Selected Answer: B**

B is correct.

VM1 can only access storage1, so firewall has to be configured on storage2 and storage3 to block access from VM1  
upvoted 2 times

✉  **Jamesat** 10 months, 1 week ago

**Selected Answer: B**

Correct.

Setting a firewall setting to only allow access to Storage1 from VM 1 wouldn't stop access to the other 2 storage accounts.

As per requirements, VM1 should only be able to access Storage1. NOT Storage1 should only be accessed from VM1.  
upvoted 4 times

✉  **Housseonline** 10 months, 3 weeks ago

any explanation ? i think A- YES

upvoted 1 times

✉  **Alessandro365** 9 months ago

correct is NO.

VM1 can only access storage1, so firewall has to be configured on storage2 and storage3 to block access from VM1  
upvoted 1 times

✉  **derrp** 11 months, 1 week ago

This solution does not prevent access to Storage2 and Storage3.

upvoted 4 times

✉  **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 1 times

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

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

You have an Azure subscription that contains the following resources:

- ☞ A virtual network named Vnet1
- ☞ A subnet named Subnet1 in Vnet1
- ☞ A virtual machine named VM1 that connects to Subnet1
- ☞ Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You create a network security group (NSG) and associate the NSG to Subnet1.

Does this meet the goal?

A. Yes

B. No

**Correct Answer: B**

✉️  **derrp** Highly Voted 11 months, 1 week ago

Assuming the NSG does not magically know what you're trying to do, we can assume the answer is no.

upvoted 26 times

✉️  **tartarus23** Highly Voted 11 months, 2 weeks ago

**Selected Answer: B**

B. No

I do not think it meets the goal since the NSG was not specific on what account or access it allowed or denied.

upvoted 11 times

✉️  **omgMerrick** Most Recent 4 months ago

**Selected Answer: B**

B. No

This solution does not fully meet the goal.

Although creating a network security group (NSG) and associating it to Subnet1 is a step in the right direction for securing network traffic, simply associating an NSG to a subnet does not restrict outbound traffic from VM1 to the storage accounts.

To ensure that VM1 can access storage1 and is prevented from accessing any other storage accounts, you need to apply a specific set of rules to the NSG. One way to achieve this is by configuring the NSG to allow outbound traffic only to storage1 and deny outbound traffic to all other storage accounts.

So, to fully meet the goal, you need to create an NSG, associate it to Subnet1, and then configure appropriate rules in the NSG to allow traffic from VM1 to storage1 and block traffic to all other storage accounts.

upvoted 2 times

✉️  **TJ001** 5 months ago

NSG wont help...we can define rules to deny/allow access to Storage service or a regional storage service by using service tags...but in this case the VM should access only one storage account... so NSG wont help here... Answer No

upvoted 1 times

✉️  **TJ001** 5 months ago

Creating service endpoint policy is a good idea

upvoted 2 times

✉️  **AzureJobsTillRetire** 5 months, 3 weeks ago

**Selected Answer: A**

Hey guys, I think the answer might be A yes. I had this question in my exam in a group of three YES/NO questions. I passed the exam with a score of 900, which is not very high but enough. I thought that there would be one YES in the three questions, and if that is true, this one is the only one could be YES. We can either assume the NSG does not configure well and give it a NO, or assume the NSG is configured as it should be and give it a YES.

upvoted 2 times

✉️  **wooyourdaddy** 2 months, 2 weeks ago

All of these 3 questions would be a no. The simplest solution to this problem would be to implement a service endpoint for storage on the subnet that VM1 is on and then use a service endpoint policy to limit it to the storage1 resource only.

Source: <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview>  
upvoted 1 times

✉️ **Aunehwet79** 5 months, 1 week ago

That's a pretty good score bro  
upvoted 2 times

✉️ **GohanF2** 7 months, 1 week ago

it's too vague the solution so the answer is NO.  
upvoted 2 times

✉️ **Prutser2** 8 months, 1 week ago

**Selected Answer: B**  
it doesn't stipulate what is in the NSG, so assuming it is empty, in which case it will not do anything  
upvoted 2 times

✉️ **BlackZeros** 8 months, 3 weeks ago

**Selected Answer: B**  
default NSG will allow the traffic to still go out.  
upvoted 2 times

✉️ **Alessandro365** 9 months ago

**Selected Answer: B**  
No is correct  
upvoted 2 times

✉️ **azeem0077** 10 months ago

**Selected Answer: B**  
Just adding an NSG won't do any change. So answer is B. Incase if the question also said that outbound and inbound rules are there in the NSG, then the answer may have been A.  
upvoted 3 times

✉️ **Jamesat** 10 months, 1 week ago

**Selected Answer: B**  
A NSG would do nothing without Rules.

Also if the Storage Accounts are public then you would need to set a Service Endpoint and then block it. This would affect all the storage accounts.

Without clarity this is cleared a NO.

upvoted 3 times

✉️ **jeffangel28** 10 months, 2 weeks ago

**Selected Answer: B**  
Correct!, is not only create and associate NSG necessary!  
upvoted 3 times

✉️ **hogemax** 10 months, 3 weeks ago

**Selected Answer: B**  
B. No  
This just creates a network security group and associates it to Subnet1. Further configuration is required.  
upvoted 7 times

✉️ **rac\_sp** 11 months, 1 week ago

extremely abstract the information provided in the question.  
upvoted 2 times

✉️ **Swetareddy** 11 months, 2 weeks ago

It happens only thru service endpoint policies using which u can restrict access to only one storage account.  
upvoted 3 times

✉️ **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22  
upvoted 1 times

✉️ **BenH** 1 year ago

**Selected Answer: A**  
I think this will meet the goal.  
upvoted 5 times

- ✉  **Diazan** 3 weeks, 3 days ago  
A NSG by itself (with only default rules configured) won't work at all  
upvoted 1 times
- ✉  **jeffangel28** 10 months, 2 weeks ago  
explain how pls  
upvoted 2 times

Question #15

Topic 4

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure subscription that contains the following resources:

- ☞ A virtual network named Vnet1

A subnet named Subnet1 in Vnet1 -

- - ☞ A virtual machine named VM1 that connects to Subnet1
  - ☞ Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You create a network security group (NSG). You configure a service tag for Microsoft.Storage and link the tag to Subnet1.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

- ✉  **Prutser2** Highly Voted 8 months, 1 week ago
- Selected Answer: B**  
the service tag in a blanket rule can only deny all storage or permit all storage, it would have no further granularity  
upvoted 5 times

- ✉  **BlackZeros** Most Recent 8 months, 3 weeks ago
- Selected Answer: B**  
correct  
upvoted 1 times

- ✉  **Jamesat** 10 months, 1 week ago
- Selected Answer: B**  
Correct.

I am assuming they mean to create an NSG rule with Storage Service Tag. Not sure whether they are denying access or not, however, this would apply to all Storage Accounts access via public endpoints.  
upvoted 3 times

- ✉  **derrp** 11 months, 1 week ago  
No. This proposed solution does not mention any means of blocking VM1 from Storage2 and Storage3.  
upvoted 1 times

- ✉  **unclegrandfather** 11 months, 3 weeks ago  
Appeared on exam Jun/28/22  
upvoted 1 times

You need to use Traffic Analytics to monitor the usage of applications deployed to Azure virtual machines.

Which Azure Network Watcher feature should you implement first?

- A. NSG flow logs
- B. IP flow verify
- C. Connection monitor
- D. Packet capture

**Correct Answer: A**

Network Watcher: A regional service that enables you to monitor and diagnose conditions at a network scenario level in Azure. You can turn NSG flow logs on and off with Network Watcher.

Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG.

Why use NSG Flow Logs?

It is vital to monitor, manage, and know your own network for uncompromised security, compliance, and performance.

Common use cases include Network Monitoring: Identify unknown or undesired traffic. Monitor traffic levels and bandwidth consumption. Filter flow logs by IP and port to understand application behavior.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview>

 **JennyHuang36** 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 3 times

 **TJ001** 5 months ago

Answer A

Enable NSG Flog Logs. Part of the activity requires the below

Requires a Log Analytics Workspace to enable Traffic Analytics Solution

Storage account is needed to store NSG Flow Logs

upvoted 2 times

 **sapien45** 8 months, 3 weeks ago

**Selected Answer: A**

Traffic analytics examines raw NSG flow logs. It then reduces the log volume by aggregating flows that have a common source IP address, destination IP address, destination port, and protocol.

Reduced logs are enhanced with geography, security, and topology information and then stored in a Log Analytics workspace.

upvoted 3 times

 **BlackZeros** 8 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

NSG Flow Logs are the key component

upvoted 2 times

 **BlackZeros** 8 months, 3 weeks ago

**Selected Answer: A**

A seems to be the correct answer.

upvoted 1 times

**HOTSPOT -**

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

Name	Virtual network	Subnet	Workload
SQL1	VNet1	Subnet1	Microsoft SQL Server 2019
Web1	VNet1	Subnet1	IIS
Web2	VNet1	Subnet2	IIS
SQL2	VNet2	Subnet1	Microsoft SQL Server 2019
Web3	VNet2	Subnet1	IIS
SQL3	VNet2	Subnet2	Microsoft SQL Server 2019

VNet1 and VNet2 are NOT connected to each other.

You need to block traffic from SQL Server 2019 to IIS by using application security groups. The solution must minimize administrative effort.

How should you configure the application security groups? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area:**

Minimum number of application security groups:

1
2
3
6

Minimum number of application security group assignments:

1
2
3
6

**Correct Answer:****Answer Area:**

Minimum number of application security groups:

1
2
3
6

Minimum number of application security group assignments:

1
2
3
6

Box 1: 2 -

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

We need one application security group for each of the two virtual networks.

Box 2: 3 -

One network assignment in VNet1. Two network assignments in VNET2.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>

keilah123 [Highly Voted] 3 months, 2 weeks ago

2 ASG and 2 ASG assignments

The question is looking for minimum.

VNET 1:

Create 1 ASG for SQL. Create outbound deny rule and assign to SQL1 Nic

VNET2: Create 1 ASG for IIS. Create inbound deny rule and assign to Web3 Nic

upvoted 8 times

Apptech 2 months, 2 weeks ago

Yes, but question also says: "block traffic from SQL Server 2019 to IIS". With your ASG for IIS you deny any kind of instance / service to access IIS.

upvoted 2 times

NoeHdzMII [Highly Voted] 6 months, 1 week ago

Confuse answer, the correct answer is to have 2 ASG and 3 associations per VNET, in this case, there are 2 VNETs. Total 4 ASG and 6 associations, one association per VM

upvoted 5 times

TJ001 5 months ago

agree but the options does not have 4 ASG

upvoted 3 times

occupatissimo [Most Recent] 1 month, 2 weeks ago

2 & 3

key word is "minimize administrative effort", and remember goal is to block sql.

so work only with outbound rule applied to SQL server, when building the rule will have the tcp-80, doesn't matter which destination (use any), for sure IIS server are in.

in this case 2 ASG (1 each vnet) for sql are required and 3 ssignment (1 each sql server nic).

upvoted 1 times

occupatissimo 1 month ago

or think in this way too

communication between vnet is deny due to default rule in nsg, so only to block traffic between subnet in the same vnet. Assuming in the sql subnet the source as any and the dest the ASG necessary is for web server only, this is in each vnet, so 2 ASG in total.

Associate then the three web server nics to them.

upvoted 1 times

guchao2000 2 months, 4 weeks ago

NSG and ASG can be used in different vnet. Tested.

upvoted 2 times

iVath 3 months ago

it's only required : from SQL Server 2019 to IIS. what about these 3 ASG assignments:

(Source=Vnet1/Sub1/SQL, Destination=Vnet1/Sub1/IIS, Access=Deny)

(Source=Vnet2/Sub1/SQL, Destination=Vnet2/Sub1/IIS, Access=Deny)

(Source=Vnet2/Sub2/SQL, Destination=Vnet2/Sub1/IIS, Access=Deny)

upvoted 3 times

TJ001 5 months ago

No of ASGs [Ans 4] - So there are 2 VNETs, 2 types of applications in both VNET one of type IIS and one of type SQL. The best practice is to use ASG assignment for both app types... which means 2 ASGs per VNET = 4 ASGs required. Note ASG cannot reference multiple VNETs  
2) No of associations [Ans 6] ? - The assignment is at subnet level, so we could do add either an outbound rule for SQL server subnet or an inbound rule at IIS server subnet or both .. Assume we are adding only one rule (either inbound or outbound) and the question asks minimum no of assignments

- In VNET 1 add an outbound rule for Subnet 1 to deny traffic from SQL ASG to IIS ASG

- In VNET 2 add an inbound rule for Subnet 1 to deny traffic from SQL ASG to IIS ASG

so 1 NSG rule per VNET is sufficient to introduce the control.. To meet this solution the ASG needs to be associated to all the VMs in all VNET ... so total 6 associations are needed (if by 'association' it means attaching ASG to VM NIC)

upvoted 1 times

TJ001 5 months ago

it appears the option does not have an ideal set up and it looks like it is only considering attaching ASG to SQL component in which case ....we could half the consideration above to conclude the answers as 2 ASG and 3 assignments ...not elegant/scalable approach but will have to go with that

upvoted 4 times

Goofer 5 months, 1 week ago

I think you must create one ASG for all IIS NIC's and one NSG on all SQL server NICs  
In the NSG Block all outgoing traffic to IIS ASG. (You need only to block traffic from SQL Server 2019 to IIS)  
1 ASG (for all IIS NICs)  
1 NSG (for all SQL NICs)  
It's not a pretty solution, but with the least administrative effort  
upvoted 3 times

✉️ **Goofer** 5 months, 1 week ago

If all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. You need 2 ASG's  
upvoted 1 times

✉️ **mhmyz** 5 months, 3 weeks ago

2 ASGs  
How to make the IIS side (receiving side) an application group,  
How to make the SQL side (sending side) an application group  
There are two, and both methods create one application group for each VNET, so there are two application groups.

2 Assignments

In VNET1, the IIS side is set as an application group, and transmission to the IIS application group can be suppressed in the transmission traffic of Subnet1 or NIC of SQL1.  
In VNET2, the SQL side is set as an application group, and reception to the IIS application group should be suppressed in the reception traffic of Subnet1 or NIC of Web3.

upvoted 4 times

✉️ **Goofer** 5 months, 1 week ago

How do you block traffic between Web1 and SQL1. They are on the same subnet.  
upvoted 2 times

✉️ **palthainon** 3 months, 1 week ago

NSG's can be assigned at the NIC level.  
upvoted 1 times

✉️ **Prutser2** 8 months, 1 week ago

answer is correct  
upvoted 4 times

✉️ **sapien45** 8 months, 3 weeks ago

By network security group assignment, they mean how many Microsoft SQL servers assigned within an Application security group  
upvoted 4 times

✉️ **Alessandro365** 9 months ago

2 ASGs e 3 assignments, answer is correct.

"All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in."  
<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups>

the ASG needs to be associated with the network card of the VMs, so there are 3 associations  
upvoted 4 times

✉️ **Ayokun** 3 months, 3 weeks ago

But being that is requested the configuration of the ASG only on the SQL vm's to minimize administrative effort the answer should be halved:  
4 asg = 2 (onlysql)  
6 assignments per nic = 3 (only sql)  
upvoted 1 times

✉️ **Ayokun** 3 months, 3 weeks ago

Hence being the ASG associated per NIC it should be 6 the second answer.  
upvoted 1 times

**HOTSPOT -**

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

Name	Address space	Associated network security group (NSG)
Subnet1	10.10.0.0/24	NSG1
Subnet2	10.10.1.0/24	NSG2

In NSG1, you create inbound rules as shown in the following table.

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

NSG2 has only the default rules configured.

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

Name	Subnet
VM1	Subnet1
VM2	Subnet1
VM3	Subnet2

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	<b>Yes</b>	<b>No</b>
VM3 can connect to port 8080 on VM1.	<input type="radio"/>	<input type="radio"/>
VM1 and VM2 can connect on port 9090.	<input type="radio"/>	<input type="radio"/>
VM1 can connect to VM3 on port 9090.	<input type="radio"/>	<input type="radio"/>

**Correct Answer:****Answer Area**

Statements	<b>Yes</b>	<b>No</b>
VM3 can connect to port 8080 on VM1.	<input checked="" type="radio"/>	<input type="radio"/>
VM1 and VM2 can connect on port 9090.	<input type="radio"/>	<input checked="" type="radio"/>
VM1 can connect to VM3 on port 9090.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

VM3 is Subnet2. NSG2 applies. The default rule will allow communication.

Box 2: No -

VM1 & VM2 is in Subnet1. NSG1 applies. Only traffic on ports 80 and 443 will be allowed. Connection on port 9090 will be denied.

Note: Priority: A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

Box 3: No -

VM1 is in Subnet1. NSG1 applies. Only traffic on ports 80 and 443 will be allowed. Connection on port 9090 will be denied.

Reference:

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

✉️  **Sheriboy**  9 months, 3 weeks ago

should be N,N, Y

- 1) Inbound rule on subnet1 will deny
- 2) Inbound rule on subnet2 will deny
- 3) No rule on VM3 so it would allow connections

upvoted 63 times

✉️  **Chriscrowne** 9 months, 1 week ago

Agree but explanation for #2 is incorrect they are both (VM1 and VM2) in subnet 1 so they are effected by NSG1 attached to subnet 1.

upvoted 6 times

✉️  **Prutser2** 8 months, 2 weeks ago

correct intra subnet traffic can be effected by an NSG associated with that subnet as per:

ntra-Subnet traffic

It's important to note that security rules in an NSG associated to a subnet can affect connectivity between VMs within it. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. If a rule is added to \*NSG1 that denies all inbound and outbound traffic, VM1 and VM2 will no longer be able to communicate with each other.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic> so NNY

upvoted 14 times

✉️  **AWSAZO** 6 months ago

N,N,Y Agree, and I tested it in the LAB using ICMP

upvoted 3 times

✉️  **EdinaldoJunior1981** 6 months, 1 week ago

N,N,Y correct

upvoted 1 times

✉️  **mav3r1ck** 9 months ago

Disagree.. Should be N Y Y

upvoted 11 times

✉️  **charlesr1700**  9 months ago

N, inbound rule on subnet one will deny

Y, Communication within the same subnet does not go through an NSG, so nothing blocking

Y, Standard rules do not block vNet to vNet communication unless explicit.

upvoted 22 times

✉️  **davidkerr7** 8 months, 3 weeks ago

2) is wrong

"It's important to note that security rules in an NSG associated to a subnet can affect connectivity between VM's within it."

upvoted 7 times

✉️  **sapien45** 8 months, 2 weeks ago

<For inbound traffic, Azure processes the rules in a network security group associated to a subnet first, if there's one, and then the rules in a network security group associated to the network interface, if there's one. " "

That means NNY,

I recommend you pass AZ-900 Microsoft Azure Fundamentals Certification .

AZ700 is not for you homie.

upvoted 7 times

✉️  **WMG** 1 month, 4 weeks ago

Savage but true..

upvoted 1 times

✉️  **Stevy\_nash** 4 months, 4 weeks ago

that was hard = )

upvoted 3 times

✉️  **ABIGK**  2 weeks, 6 days ago

1. N — VM3 is trying to access VM1 through port 8080 and port 8080 not in allowed port list of NSG1

2. N — VM1 and VM2 tryin to talk with each other. Even though the are on the same subnet the NSG1 deny rule will include port 9090

3. Y — VM1 and VM3 can have connection NSG1 will not affect any outbound connection.

NSG 1 is applied inbound and which means it affect connections that comes Subnet 1 only. The only allowed port is http (80) and https (443) and the rest is blocked. Any connection going out side of Subnet 1 is allowed. VM1 and VM2 will be affected by NSG1 because they are under Subnet1. NG2 will not affect anything because only default rules are configured.

upvoted 1 times

✉️  **ABIGK** 2 weeks, 6 days ago

The answer should be

N

N

Y

upvoted 1 times

✉ **MrBlueSky** 2 months, 1 week ago

I re-created this in a lab and can confirm that the VMs could not communicate with one another even though they are in the same subnet. As others have discussed and provided the link for... NSGs are still used for intra-subnet communication.

Answer is NNY

upvoted 1 times

✉ **faeem** 2 months, 1 week ago

I would go with N,N,Y as described, "By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. If a rule is added to \*NSG1 that denies all inbound and outbound traffic, VM1 and VM2 will no longer be able to communicate with each other." With NSG1 having custom rules, intra-communication is defined by the rules.

upvoted 1 times

✉ **Apptech** 2 months, 2 weeks ago

should be NYN

1. Inbound rule on subnet1 will deny

2. By default, virtual machines in the same subnet can communicate based on a default NSG rule allowing intra-subnet traffic. (<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works#intra-subnet-traffic>)

3. VM3 has default rule as the text states. DenyAllInbound is the default for NSG. See here: <https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

upvoted 1 times

✉ **Libaax01** 3 months, 1 week ago

VM3, which is part of Subnet 2, can not connect to port 8080 on VM1, because we have inbound rule that denies all ports except port 80 and 443. so, the answer is No!

VM1 and VM2 are on the same subnet and by default inbound rules within a virtual network are allowed, however we have NSG with a lower priority(200) over riding the default allowed rule which is priority 65000. So the Answer is NO!

VM1 is on Subnet 1 and VM3 is on Subnet 2, and outbound communication by default between subnets in the same virtual network is allowed and the question states NSG2 has only the default rules configured. so the answer is YES!

N

N

Y

upvoted 3 times

✉ **samir111** 4 months ago

It should be N,N, Y

upvoted 2 times

✉ **TJ001** 5 months ago

N,N,Y .... NSG1 is incomplete there is no reference to Destination...(assumed it is Subnet1)

upvoted 1 times

✉ **Goofer** 5 months, 2 weeks ago

<https://www.youtube.com/watch?v=fICoRc1uv9o>

upvoted 1 times

✉ **NoeHdzMII** 6 months, 1 week ago

That is correct N,N,Y

1) Inbound rule on subnet 1

2) Inbound rule also applied intraVNET traffic

3) The NSG is stateful and with no inbound rule the connection is working

upvoted 2 times

✉ **Nisha318** 6 months, 2 weeks ago

I think the answer is N, N, N.

1 - Inbound rule on subnet1 will deny

2 - Inbound rule on subnet2 will deny

3 - Traffic sourced from the virtual network for any port deny. The NSG is a stateful firewall and an inbound rule created on it automatically creates the same outbound rule.

upvoted 4 times

✉ **GohanF2** 7 months, 1 week ago

1. VM3 is attached to subnet; which has default outband connection. However, VM1 has NSG that denies traffic in any ports except 80 and 443 from any IP address. But, communication from Virtual network is set to Deny so, the answer here is NO

2. VM1 and VM2 belongs to the same subnet 1 and each of them has default Outbound policy rule that will allow the traffic but Inbound is restricted for any port except 80 and 443. So, answer here is NO

3. VM1 can communicate to VM3 due that there is no restriction in Outbound policy for NSG1 and no restrictions for NSG2 inbound. So, answer here is YES.

NO

NO  
YES

upvoted 5 times

 **mr\_slow** 7 months, 4 weeks ago

Tested in lab,

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

upvoted 4 times

 **Syldana** 8 months ago

N, inbound rule on subnet one will deny

Y, Communication within the same subnet does not go through an NSG, so nothing blocking

Y, Standard rules do not block vNet to vNet communication unless explicit.

upvoted 2 times

 **GiorgioLDN** 8 months, 1 week ago

The correct answer is N,Y,Y. Let me explain why.

NSG1 basically allows all traffic towards subnet 1 on ports 80 and 443. It will block everything else.

1. VM3 will be allowed to access VM1 on any port outbound on NSG2. VM3 will be blocked by NSG1 inbound since it is trying to access port 8080.
2. VM1 and VM2 can connect on any port between themselves since they are communicating inside the subnet. Thus the answer is yes.
3. Since NSG2 has the default rules applied, it means that Subnet2 can accept traffic from any subnet within the VNET. Thus the answer is Yes.

upvoted 5 times

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

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

You have the Azure resources shown in the following table.

Name	Type	Virtual network	Resource group	Location
VM1	Virtual machine	Vnet1	RG1	East US
VM2	Virtual machine	Vnet2	RG2	UK West
VM3	Virtual machine	Vnet3	RG3	East US
App1	App Service	Vnet1	RG4	East US
St1	Storage account	<b>Not applicable</b>	RG5	UK West

You need to check latency between the resources by using connection monitors in Azure Network Watcher.

What is the minimum number of connection monitors that you must create?

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

**Correct Answer: C**

In the Region UK West region we have one single virtual machine VM2.

There is not anything to monitor here.

In the Region East US region we have two virtual machines VM1 & VM3, and App1.

We can monitor the connections: VM1-VM3, VM1-App1, VM3-App1.

Note: Connection Monitor includes the following entities:

Connection monitor resource: A region-specific Azure resource. All the following entities are properties of a connection monitor resource.

Endpoint: A source or destination that participates in connectivity checks. Examples of endpoints include Azure VMs, on-premises agents, URLs, and IP addresses.

Reference:

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

✉  zenithcsa1 Highly Voted 9 months, 2 weeks ago

Tested

Source : must be in the same region / VM or VMSS

Target : region doesn't matter / VM, URL, etc.

ConnecitonMonitor1 : VM1, VM3 --> other resources

ConnecitonMonitor2 : VM2 --> other resources

upvoted 5 times

✉  zenithcsa1 9 months, 2 weeks ago

I mean 'B'

upvoted 10 times

✉  GohanF2 Highly Voted 7 months, 1 week ago

Answer is B.

The Connection Monitor is established per region.

And depending on the region we can connect multiple VMS, VMSS, endpoints and on-premises devices. Since, we have two regions only, we will need to Connection Monitors.

upvoted 5 times

 **woyourdaddy** Most Recent 2 months, 2 weeks ago

**Selected Answer: B**

At this link:

<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal#create-test-groups-in-a-connection-monitor>

It states as part of the test group creation process:

To choose Azure agents, select the Azure endpoints tab. Here you see only VMs or Virtual Machine Scale Sets that are bound to the region that you specified when you created the connection monitor.

This confirms that you would need 1 connection monitor per region. So the correct answer is B.

upvoted 2 times

 **samir111** 3 months, 3 weeks ago

**Selected Answer: B**

Correct: B

upvoted 1 times

 **JennyHuang36** 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 2 times

 **energie** 4 months, 1 week ago

**Selected Answer: C**

Connection monitor is regional resource but destination VM can be in any region.

upvoted 2 times

 **Thanveer** 4 months, 3 weeks ago

**Selected Answer: B**

Connection monitor resource is a region-specific Azure resource

upvoted 2 times

 **caliph\_noman** 5 months ago

**Selected Answer: A**

correct

upvoted 1 times

 **TJ001** 5 months ago

will go with B .. per region 1 monitor but can add multiple sources and destinations

upvoted 3 times

 **Nicolas\_UY** 6 months ago

**Selected Answer: C**

my previous answer was wrong, sorry for the confusion:

In the UK West region, there is only a single virtual machine (VM2). You do not need to create a connection monitor for this resource, as there are no other resources in the region to connect to.

In the East US region, there are two virtual machines (VM1 and VM3) and an App Service (App1). To check the latency between these resources, you would need to create the following connection monitors:

VM1 and VM3: This connection monitor would test the latency between VM1 and VM3 in the East US region.

VM1 and App1: This connection monitor would test the latency between VM1 and App1 in the East US region.

VM3 and App1: This connection monitor would test the latency between VM3 and App1 in the East US region.

Overall, you would need to create a total of three connection monitors to check the latency between all of the resources in the East US region.

upvoted 4 times

 **Nicolas\_UY** 6 months ago

**Selected Answer: D**

To check the latency between the resources in the table you provided, you would need to create a minimum of four connection monitors. The correct answer is therefore D.

A connection monitor in Azure Network Watcher is a tool that allows you to continuously test connectivity between two resources. It sends a series of packets to a specified destination at a specified interval, and measures the round-trip time (RTT) of the packets.

In this case, you would need to create at least one connection monitor for each pair of resources that you want to monitor. For example:

VM1 and App1 (located in the same resource group and VNet)

VM2 and St1 (located in different resource groups and VNets)

VM3 and VM1 (located in the same region, but with different resource groups and VNets)

This would require a minimum of four connection monitors to cover all of the resources in the table.

upvoted 1 times

 **Syldana** 8 months ago

**Selected Answer: B**

B is correct  
upvoted 2 times

 **Prutser2** 8 months, 1 week ago

**Selected Answer: B**

each connection monitor can have multiple sources and destinations, but can only be set up in 1 region, because question provides 2 regions, we need 2 separate connection monitors, so B  
upvoted 3 times

 **sapien45** 8 months, 2 weeks ago

**Selected Answer: B**

Takes a few seconds to try to create a connection monitor in the portal :  
Connection Monitor enables you to monitor connectivity in your Azure and hybrid network. Select your preferred subscription and REGION from which monitoring will be performed.  
upvoted 1 times

 **Alessandro365** 8 months, 3 weeks ago

**Selected Answer: B**

B is correct  
upvoted 1 times

 **BlackZeros** 8 months, 3 weeks ago

**Selected Answer: B**

Answer is B  
Connection monitor resource: A region-specific Azure resource. All the following entities are properties of a connection monitor resource.  
<https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview>

you may need to install the agent 3 times, but the connection monitor set will be two (it is a regional service)  
upvoted 2 times

 **promo** 9 months ago

**Selected Answer: B**

I'm still thinking 2 regions.  
upvoted 3 times

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

RG1 contains an Azure Network Watcher instance named NW1.

You need to ensure that Admin1 can place a lock on NW1. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

- A. User Access Administrator
- B. Resource Policy Contributor
- C. Network Contributor
- D. Monitoring Contributor

**Correct Answer: A**

 **chatlisi** Highly Voted 5 months, 1 week ago

It seems the provided answer to be correct:

"To create or delete management locks, you need access to Microsoft.Authorization/\* or Microsoft.Authorization/locks/\* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks."

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#who-can-create-or-delete-locks>

\* The question is about placing a lock, not about using Network Watcher  
upvoted 9 times

 **Aunehwet79** 5 months, 1 week ago

Yes I have to agree. The Network watcher comment throws us but only owner and user Access Admin can create locks

upvoted 3 times

 **omgMerrick** Highly Voted 3 months, 3 weeks ago

**Selected Answer: A**

Well, after reviewing more, I think I was premature in saying the answer was 100% C. I was 100% wrong!! The correct answer is absolutely, 100%  
A. User Access Administrator

The key to the questions is that we're being asked what permissions are required to place a \_\_lock\_\_ (resource lock) on the Network Watcher resource. To create or delete management locks, you need access to Microsoft.Authorization/\* or Microsoft.Authorization/locks/\* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks. You can create a custom role with the required permissions.

Source:

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json#who-can-create-or-delete-locks>  
upvoted 5 times

 **SaadKhamis** Most Recent 1 month, 2 weeks ago

**Selected Answer: A**

Who can create or delete locks

To create or delete management locks, you need access to Microsoft.Authorization/\* or Microsoft.Authorization/locks/\* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks. You can create a custom role with the required permissions.

Network Contributor

Microsoft.Authorization/\*/read Read roles and role assignments

upvoted 1 times

 **MrBlueSky** 2 months, 1 week ago

This question really has nothing to do with Network Watcher or Azure Networking.

What they want you to know is that you need the User Access Administrator role in order to make changes to create/delete management locks to ANY resource, not just Network Watcher.

I doubt this question would be on the test

upvoted 1 times

 **raj\_evergreen** 3 months, 1 week ago

A is the correct answer. Network Contributor cannot add lock

upvoted 1 times

 **Vanja10** 3 months, 3 weeks ago

Tested. User Access Administrator is right answer.  
upvoted 3 times

 **omgMerrick** 3 months, 3 weeks ago

**Selected Answer: C**  
The correct answer is 100% C. Network Contributor

To use Network Watcher capabilities, the account you log into Azure with, must be assigned to the Owner, Contributor, or Network contributor built-in roles, or assigned to a custom role that is assigned the actions listed for each Network Watcher capability in the sections that follow.

Source:

<https://learn.microsoft.com/en-us/azure/network-watcher/required-rbac-permissions>

upvoted 1 times

 **harshit101** 4 months ago

**Selected Answer: A**  
A is right answer  
upvoted 1 times

 **samir111** 4 months ago

**Selected Answer: C**  
C. Network Contributor  
upvoted 1 times

 **samir111** 4 months ago

Assigning the "User Access Administrator" role to Admin1 would allow them to manage access to all resources in the Azure subscription, including managing role assignments for all users, groups, and service principals. This would be excessive and not in line with the principle of least privilege since Admin1 only needs to be able to place a lock on the Azure Network Watcher instance named NW1.

Assigning the "User Access Administrator" role to Admin1 would provide them with more permissions than necessary and could potentially lead to accidental or intentional misuse of the additional privileges. Therefore, it is not recommended to assign the "User Access Administrator" role to Admin1 for placing a lock on NW1. The "Network Contributor" role would be more appropriate in this scenario.

C. Network Contributor  
upvoted 1 times

 **TJ001** 5 months ago

agree with Answer A  
upvoted 1 times

 **Th3Nk** 5 months, 1 week ago

**Selected Answer: A**  
Who can create or delete locks:  
To create or delete management locks, you need access to Microsoft.Authorization/\* or Microsoft.Authorization/locks/\* actions. Only the Owner and the User Access Administrator built-in roles can create and delete management locks. You can create a custom role with the required permissions.

Answer: A

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>  
upvoted 3 times

 **Akodo\_Shado** 5 months, 1 week ago

**Selected Answer: C**  
"To use Network Watcher capabilities, the account you log into Azure with, must be assigned to the Owner, Contributor, or Network contributor built-in roles"  
<https://learn.microsoft.com/en-us/azure/network-watcher/required-rbac-permissions>  
upvoted 2 times

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**

✉ **omgMerrick** 3 months, 3 weeks ago

**Selected Answer: A**

A. Standard general-purpose v2 storage account

Read my correction and source:

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal#enable-nsg-flow-log>  
upvoted 2 times

✉ **omgMerrick** 4 months ago

**Selected Answer: B**

B. An Azure Log Analytics workspace.

To enable network security group (NSG) flow logs for NSG1, you need to create an Azure Log Analytics workspace first. The flow logs can then be sent to the workspace for analysis and monitoring.

After creating the Log Analytics workspace, you can then configure NSG flow logs to be sent to the workspace by specifying the Log Analytics workspace ID and key in the NSG flow log settings. You can also configure retention policies for the logs within the workspace.

upvoted 2 times

✉ **JohnnyChimpo** 1 month, 2 weeks ago

If you attempt to enable on any NSG, it only presents the option for storage accounts

upvoted 2 times

✉ **omgMerrick** 3 months, 4 weeks ago

After further study, I'm changing my answer to A. the standard general-purpose v2 storage account.

It very clearly states that NSG flow logs require a storage account as that is where the log data is actually written. The tutorial on the source link below even states that you should create a standard storage account.

Source:

<https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal#enable-nsg-flow-log>

upvoted 2 times

✉ **samir111** 4 months ago

**Selected Answer: B**

The correct answer is B

upvoted 1 times

✉ **alkorkin** 4 months, 4 weeks ago

Retention is available only if you use General purpose v2 Storage accounts (GPv2).

upvoted 1 times

✉ **TJ001** 5 months ago

Agree with Answer A

upvoted 1 times

✉ **alfonzo47** 5 months ago

**Selected Answer: A**

The answer is correct as stated right here in documentation: <https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal#enable-nsg-flow-log>

overview#:~:text=Retention%20is%20available%20only%20if%20you%20use%20General%20purpose%20v2%20Storage%20accounts%20(GPv2).

upvoted 4 times

 **Yassine145** 5 months ago

**Selected Answer: B**

The correct answer is B. An Azure Log Analytics workspace

To enable NS flow logs for NSG1 and support retention policies, you must first create an Azure Log Analytics workspace. Once created, you can configure the NSG1 to send flow logs to the Log Analytics workspace, then you can use the Log Analytics workspace to view and analyze the flow logs data and also set retention policies for the data.

upvoted 1 times

 **TJ001** 5 months ago

No wrong ...when enabling NSG flow log it asks for what storage account and what retention is needed (0 means forever or provide the required no of days upto 365).. Log Analytics workspace is only needed if Traffic Analytics solution needs to be enabled.

upvoted 2 times

 **Akodo\_Shado** 5 months, 1 week ago

**Selected Answer: A**

"Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG. Flow data is sent to Azure Storage accounts from where you can access it as well as export it to any visualization tool, SIEM, or IDS of your choice."

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

upvoted 2 times

Question #22

Topic 4

You have an Azure subscription that contains the following resources:

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

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

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

What should you do?

- A. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- B. On FW1, create an outbound service tag rule for Azure Cloud.
- C. Deploy a NAT gateway.
- D. Deploy an application security group that allows outbound traffic to 1688.

**Correct Answer: A**

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains a virtual machine named VM1 and an Azure firewall named FW1.

You have an Azure Firewall Policy named FP1 that is associated to FW1.

You need to ensure that RDP requests to the public IP address of FW1 route to VM1.

What should you configure on FP1?

- A. a network rule
- B. URL filtering
- C. a DNAT rule
- D. an application rule

**Correct Answer:** C

✉️  **omgMerrick** Highly Voted 4 months ago

**Selected Answer:** C

C. a DNAT rule

To allow RDP requests to reach VM1 through the public IP of FW1, you need to create a rule that translates the destination IP address of the incoming RDP requests to the private IP address of VM1. This is done through a type of rule called a DNAT rule, which is configured on the Azure Firewall Policy (FP1). Other types of rules, such as network rules, URL filtering, and application rules, are not relevant to this specific scenario.

upvoted 5 times

✉️  **omgMerrick** 3 months, 4 weeks ago

Source:

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat-policy>

upvoted 1 times

✉️  **mVic** Most Recent 3 months, 3 weeks ago

**Selected Answer:** C

DNAT rule

<https://learn.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat-policy>

upvoted 1 times

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

content\_type  
 query\_string  
 uri\_path

Set  to buy.aspx and category={var\_uri\_path\_1}&product={var\_uri\_path\_2}

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

**Correct Answer:**

If server variable  equals to the pattern `(.+)/(.+)`

content\_type  
 query\_string  
 uri\_path

Set  to buy.aspx and category={var\_uri\_path\_1}&product={var\_uri\_path\_2}

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

 **tzatziki** (Highly Voted) 4 months, 2 weeks ago

Correct... Hey.. New question it seems... Nice to see these are updated! Thank you!

<https://learn.microsoft.com/en-us/azure/application-gateway/rewrite-url-portal#configure-url-rewrite>  
upvoted 12 times

You have an Azure subscription that contains the following resources:

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

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

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

What should you do?

- A. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
- B. On FW1, create an outbound service tag rule for Azure Cloud.
- C. Deploy a NAT gateway.
- D. On FW1, configure a DNAT rule for port 1688.

**Correct Answer: A**

✉️  **breakpoint0815** Highly Voted 2 months, 3 weeks ago

Why this question/answer appears multiple times??

upvoted 5 times

✉️  **WMG** 1 month, 4 weeks ago

On the exam it will appear at least 6 times, so better be ready!!

upvoted 6 times

✉️  **meow10** 1 month ago

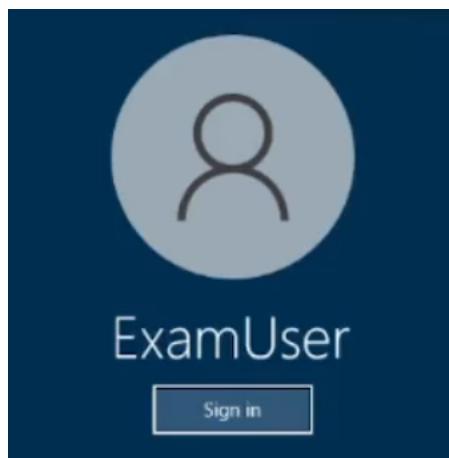
Thats 6 easy points then, Yeeey !!

upvoted 1 times

✉️  **ABIGK** Most Recent 3 weeks, 4 days ago

I think the admin of the page better to check the question and remove the reoccurrence.

upvoted 2 times

**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: xxxxxxxxxxx

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 create an Azure Firewall instance named FW1 that meets the following requirements:

- Has an IP address from the address range of 10.1.255.0/24
- Uses a new Premium firewall policy named FW-policy1
- Routes traffic directly to the internet

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

Step 1: On the Azure portal menu or from the Home page, select Create a resource.

Step 2: Type firewall in the search box and press Enter.

Step 3: Select Firewall and then select Create.

Step 4: On the Create a Firewall page, use the following table to configure the firewall:

\* Name - Enter FW1

\* Firewall management - Select Use a Firewall Policy to manage this firewall.

\* Firewall policy - Select Add new, and enter FW-policy1.

\* Choose a virtual network - Select Create new

Step 4.1: Enter or select the appropriate values:

Subscription - Select your Azure subscription.

Resource group -

Name -

Region -

**Correct Answer:**

Step 4.2 Select Next: IP addresses.

Step 4.3 For IPv4 Address space, accept the default 10.0.0.0/16.

Step 4.4 Under Subnet, select default.

Subnet name -

For Address range, type 10.1.255.0/24

Step 4.5 Select Save.

Step 4.6 Select Review + create.

Step 4.7: Select Create.

Step 5: Back to the Create a Firewall page:

\* Public IP address - Add new

Step 6: Accept the other default values, then select Review + create.

Step 7: Review the summary, and then select Create to create the firewall.

**Reference:**

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

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

✉  **wooyourdaddy**  3 months, 1 week ago

I believe the requirement:

- Routes traffic directly to the internet

Is supposed to indicate that the FW should not use Forced Tunneling.

When you configure a new Azure Firewall, you can route all Internet-bound traffic to a designated next hop instead of going directly to the Internet. For example, you may have a default route advertised via BGP or using User Defined Route (UDR) to force traffic to an on-premises edge firewall or other network virtual appliance (NVA) to process network traffic before it's passed to the Internet.

Source: <https://learn.microsoft.com/en-us/azure/firewall/forced-tunneling>

upvoted 5 times

✉  **JohnnyChimpo** 1 month ago

Does that mean that no further configuration is needed since all traffic will be router to the Internet by default?

upvoted 1 times

✉  **Aziza\_Adam**  3 months, 4 weeks ago

1- create FW with policy (also create vnet using /16 and choose the provided range for the subnet).

2- Create Route table

3- Add routing rule that route 0.0.0.0/0 to NVA then give the private IP address of your firewall

upvoted 4 times

✉  **ABINYK** 2 weeks, 3 days ago

Route table needs to be associated. Defining a routing table will not do anything. This means routeable could only be associated to a Subnet not a Firewall.

upvoted 1 times

✉️👤 **MrBlueSky** 2 months, 1 week ago

NVA =/= Azure Firewall

NVAs are frequently Firewalls that are hosted on Azure VMs. This is not the same thing as the actual product called 'Azure Firewall'

upvoted 1 times

✉️👤 **tzatziki** 4 months, 2 weeks ago

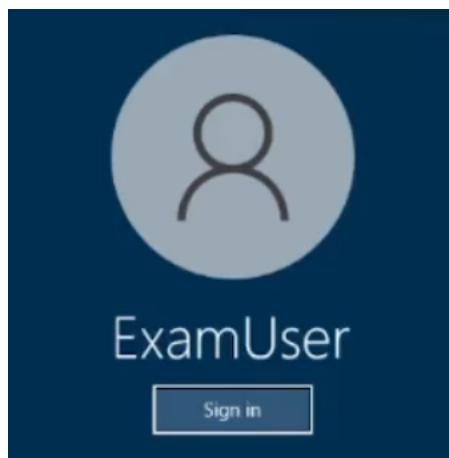
\*Routes traffic directly to the internet

So, in order to achieve this: I made a route pointing to my firewall IP (0.0.0.0/0 -> Virtual Appliance + IP) and an application rule allowing http / https in the firewall. ... Network rule made no difference as concerned my vm reaching its internet bound traffic.

Used this for reference:

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

upvoted 4 times

**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: xxxxxxxxx

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 plan to implement an Azure application gateway in the East US Azure region. The application gateway will have Web Application Firewall (WAF) enabled.

You need to create a policy that can be linked to the planned application gateway. The policy must block connections from IP addresses in the 131.107.150.0/24 range. You do NOT need to provision the application gateway to complete this task.

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



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

#### Part 1: Create a WAF policy

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

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

Step 2: On Create a WAF policy page, Basics tab, enter or select the following information and accept the defaults for the remaining settings:

Policy for - Regional WAF (Application Gateway)

Subscription - Select your subscription name

Resource group - Select your resource group

Policy name - Type a unique name for your WAF policy.

Location: East US

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

##### Setting - Value

Application Gateway- Select the application gateway, and then select Add.

HTTP Listener - Select the application gateway, select the listeners, then select Add.

Route Path - Select the application gateway, select the listener, select the routing rule, and then select Add.

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

Home > WAF policies > Create a WAF policy

## Create a WAF policy

Basics Policy settings Managed rules Custom rules Association Tags Review + create

Malicious attacks such as SQL Injection, Cross Site Scripting (XSS), and other OWASP top 10 threats could cause service outage or data loss, and pose a big threat to web application owners. Web Application Firewall (WAF) protects your web applications from common web attacks, keeps your service available and helps you meet compliance requirements.

[Learn more about WAF policy for Front Door](#)  
[Learn more about WAF policy for Application Gateway](#)

**Project details**

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

Policy for \* ⓘ

Subscription \* ⓘ

Resource group \*  [Create new](#)

**Instance details**

Policy name \* ⓘ  ✓

Location \* ⓘ

Policy state ⓘ   Enabled

#### Part 2: Configure WAF rule

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

##### Custom rules

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

Step 6: On the Add custom rule page, use the following test values to create a custom rule:

Setting - Value  
 Custom rule name - AnyName  
 Status - Enabled  
 Rule type- Match  
 Priority - 100  
 Match type- IP address  
 Match variable - SocketAddr (for example)  
 Operation - Does contain  
 IP address or range - 131.107.150.0/24  
 Then Deny traffic

## Edit custom rule

X

A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. [Learn more about custom rules](#)

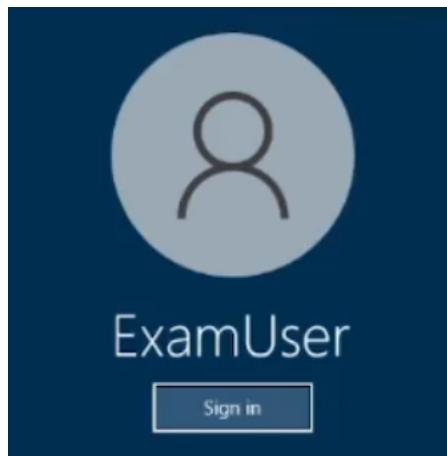
Custom rule name *	<input type="text" value="FdWafCustRule"/>
Status ⓘ	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Rule type ⓘ	<input checked="" type="radio"/> Match <input type="radio"/> Rate limit
Priority * ⓘ	<input type="text" value="100"/>
<b>Conditions</b>	
<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <b>If</b> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">           Match type ⓘ  <input type="text" value="IP address"/> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">           Match variable  <input type="text" value="SocketAddress"/> </div> <div style="margin-bottom: 5px;">           Operation  <input type="radio"/> Does contain <input checked="" type="radio"/> Does not contain         </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">           IP address or range  <input type="text" value="10.10.10.0/24"/>  <input type="text" value="IPv4 or IPv6 address or ranges"/> </div> <div style="text-align: center; margin-top: 10px;"> <a href="#" style="color: blue;">+ Add new condition</a> </div> </div>	
<b>Then</b>	<input type="text" value="Deny traffic"/>

Step 7: Select Add.

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

Reference:

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

**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: xxxxxxxxx

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 configure VNET1 to log all events and metrics. The solution must ensure that you can query the events and metrics directly from the Azure portal by using KQL.

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



## Plan

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

Stage 1: Determine the resource group of VNET1

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

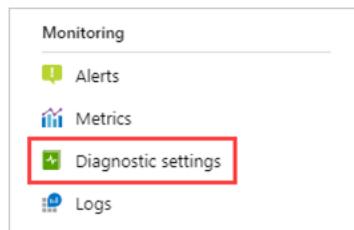
Stage 2: In Azure Monitor set up monitoring with the VNET's Resource Group as source, and Log Analytics workspace as destination

Create diagnostic settings

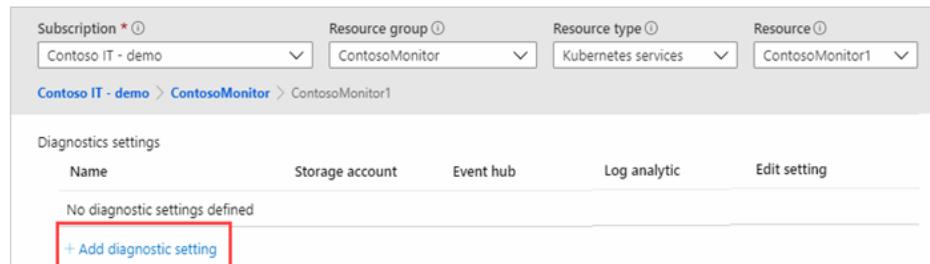
Step 2: You can configure diagnostic settings in the Azure portal either from the Azure Monitor menu or from the menu for the resource (XGroup in our case).

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

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



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



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

A screenshot of the 'Diagnostic setting' configuration page. At the top, there are buttons for Save, Discard, Delete, and Feedback. Below this, a descriptive text explains what a diagnostic setting is. The main form has fields for 'Diagnostic setting name \*' (empty), 'Logs' (with 'Category groups' for 'audit' and 'allLogs'), 'Metrics' (with 'AllMetrics' checked), and 'Destination details' (checkboxes for 'Send to Log Analytics workspace', 'Archive to a storage account', 'Stream to an event hub', and 'Send to partner solution').

Correct Answer:

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

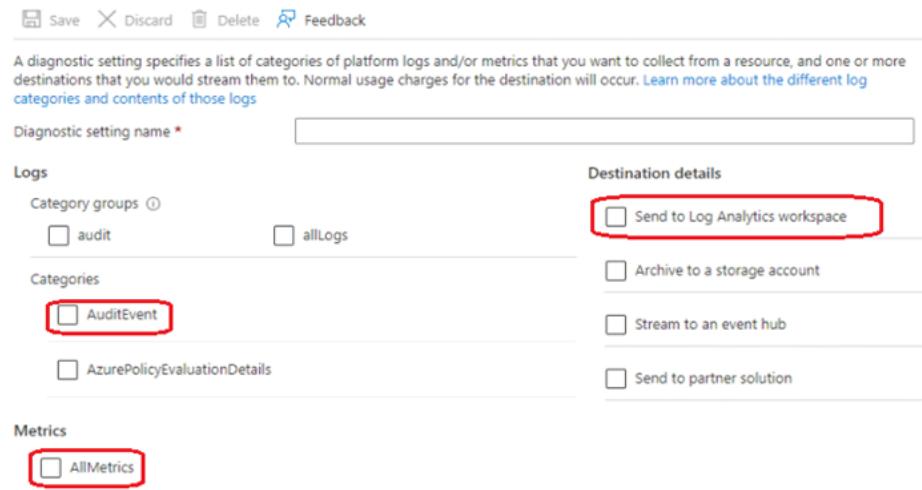
We do the following:

Categories: Select AuditEvent

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

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

Home > Monitor >  
**Diagnostic setting** ...



A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name \*

Logs

Category groups (radio button)

audit       allLogs

Categories

AuditEvent

AzurePolicyEvaluationDetails

Metrics

AllMetrics

Destination details

Send to Log Analytics workspace

Archive to a storage account

Stream to an event hub

Send to partner solution

Step 6: Destination details -skip

Step 7: Select Save.

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

Azure virtual network uses Azure Monitor.

#### Collection and routing

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

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

Sources: The type of metric and log data to send to the destinations defined in the setting.

The available types vary by resource type.

Destinations: One or more destinations to send to.

#### Destinations

Platform logs and metrics can be sent to the destinations listed in the following table.

\* Log Analytics workspace

Metrics are converted to log form. This option might not be available for all resource types. Sending them to the Azure Monitor Logs store (which is searchable via Log Analytics) helps you to integrate them into queries, alerts, and visualizations with existing log data.

\* Etc.

#### Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings>

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

  **Bbb78**  4 months, 2 weeks ago

This is not clearly explained. The solution would be from the VNET diagnostic settings and send to the Log Analytics workspace from there  
upvoted 10 times

  **JohnnyChimpo**  4 weeks ago

The solution shows "Azure Monitor" and it is incorrect. Other resources can be enabled for diagnostic settings in here, however vnets do not appear there for some reason. To configure vnet logging, do so directly from the "diagnostic settings" blade in the vnet itself.

upvoted 4 times

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**

 **ckyap** 2 months ago

Seems to be the right answer. Create an ASG and assign to each monitoring vm. Then in the NSG1, create an allow rule to allow the IP 131.107.1.15 to the ASG.

<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups>

upvoted 3 times

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

Name	Type	Description
VNet1	Virtual network	Contains a subnet named Subnet1
Subnet1	Virtual subnet	Part of VNet1
NSG1	Network security group (NSG)	Linked to Subnet1
ASG1	Application security group	Not linked

Subnet1 contains three virtual machines that host an app named App1. App1 is accessed by using the SFTP protocol.

From NSG1, you configure an inbound security rule named Rule2 that allows inbound SFTP connections to ASG1.

You need to ensure that the inbound SFTP connections are managed by using ASG1. The solution must minimize administrative effort.

What should you do?

- A. From NSG1, modify the priority of Rule2.
- B. From each virtual machine, associate the network interface to ASG1.
- C. From Subnet1, create a subnet delegation.
- D. From ASG1, modify the role assignments.

**Correct Answer: B**

✉️ user crypto700 1 month, 1 week ago

**Selected Answer: B**

B is correct

upvoted 2 times

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	<i>None</i>

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**

 **\_fvt** Highly Voted 2 months, 2 weeks ago

**Selected Answer: AB**

Seems correct.

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

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

upvoted 5 times

 **Rob\_G** Most Recent 1 month, 3 weeks ago

**Selected Answer: AB**

Correct A & B

The Firewall needs to be able to decrypt the traffic so the IDS can inspect the traffic. To do this TLS inspection needs to be enabled and a copy of the certificate needs to be stored.

upvoted 3 times

You have the Azure resources shown in the following table.

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

You configure storage1 to provide access to the subnet in Vnet1 by using a service endpoint.

You need to ensure that you can use the service endpoint to connect to the read-only endpoint of storage1 in the paired Azure region.

What should you do first?

- A. Fail over storage1 to the paired Azure region.
- B. Configure the firewall settings for storage1.
- C. Create a virtual network in the paired Azure region.
- D. Create another service endpoint.

**Correct Answer: B**

The Azure storage firewall provides access control for the public endpoint of your storage account. You can also use the firewall to block all access through the public endpoint when using private endpoints.

Note: By default, service endpoints work between virtual networks and service instances in the same Azure region. When using service endpoints with Azure

Storage, service endpoints also work between virtual networks and service instances in a paired region.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

✉️  **sapien45** Highly Voted 8 months, 3 weeks ago

**Selected Answer: C**

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal>

upvoted 13 times

✉️  **TJ001** 5 months ago

Answer C. Agreed

upvoted 1 times

✉️  **Zika69** Most Recent 4 days ago

**Selected Answer: B**

An answer is needed to the question "ensure that you can use the service endpoint to connect to the read-only endpoint of storage1 in the paired Azure region" - and only possible answer is B

Answer C is for the question - "What you should do to create a RA-GRS instance"

upvoted 1 times

✉️  **jarz** 1 month, 2 weeks ago

F#cking M\$ are sneaky mofo! You really got to RTFQ with these bastards!

It's asking what's the first thing you need to do. It's difficult to know exactly what's been done, and what needs to be done. Assuming nothing has been done, then configuring the vnets on the recovery site makes sense.

upvoted 2 times

✉️  **Apptech** 2 months, 3 weeks ago

Documentation says: "When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance." But in our case the service endpoint for the Azure Storage already is in place. So this question is pretty unclear. If the Vnet also already is in place (we do not know for sure) then Firewall should be the next step.

upvoted 1 times

✉️  **Neostar** 3 months ago

**Selected Answer: A**

"Service endpoints allow continuity during a regional failover and access to read-only geo-redundant storage (RA-GRS) instances. Network rules that grant access from a virtual network to a storage account also grant access to any RA-GRS instance."

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#available-virtual-network-regions>  
upvoted 2 times

 **Bbb78** 4 months, 2 weeks ago

**Selected Answer: B**

who is to say that the paired Azure region does not have a VNet yet ...maybe it just needs that firewall rule on the storage?  
upvoted 1 times

 **alkorkin** 5 months ago

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance.  
<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal>  
upvoted 1 times

 **varvare** 5 months, 3 weeks ago

This is the excerpt from the link above Service endpoints allow continuity during a regional failover and access to read-only geo-redundant storage (RA-GRS) instances. Network rules that grant access from a virtual network to a storage account also grant access to any RA-GRS instance.

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts.

if you read past the section that makes B the answer, you see the pre-requisite that makes C the answer  
upvoted 2 times

 **GohanF2** 7 months, 1 week ago

Answer is C.

By enabling Service Endpoint for access to our Azure resource, we are limiting the access to the "storage account" only to private IP address. So, we won't longer need the usage of a public IP address or NATting settings like in a firewall. So, the option of the firewall is no longer suitable in this case.

The first option about fail-over will work only if the primary "service point" fails, or for having active-active environment; but that will require too much effort. Plus, both "Subnet" and "Service endpoint" are located in the same region, it would be useful the "fail-over option if they are located in separated regions".

The other option about adding an additional "service endpoint" doesn't make sense due that the question says that we will need to grant access via the "Service endpoint" that was created.

upvoted 2 times

 **AjdIfasudfo0** 6 months, 2 weeks ago

this is wrong. Service endpoints go via the public ip. That's there very difference compared to private endpoint  
upvoted 4 times

 **Prutser2** 8 months, 1 week ago

**Selected Answer: C**

By default, service endpoints work between virtual networks and service instances in the same Azure region. When using service endpoints with Azure Storage, service endpoints also work between virtual networks and service instances in a paired region. If you want to use a service endpoint to grant access to virtual networks in other regions, you must register the AllowGlobalTagsForStorage feature in the subscription of the virtual network. This capability is currently in public preview.

Service endpoints allow continuity during a regional failover and access to read-only geo-redundant storage (RA-GRS) instances. Network rules that grant access from a virtual network to a storage account also grant access to any RA-GRS instance.

When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts.

upvoted 3 times

 **DevOpsJunior** 8 months, 3 weeks ago

B is correct, its clearly mentioned in the documentation.  
upvoted 2 times

 **sapien45** 8 months, 3 weeks ago

And which documentation is it , junior ?  
upvoted 4 times

 **Akodo\_Shado** 5 months ago

Answer is obviously B as DevOpsJunior pointed out.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal>  
"When using service endpoints with Azure Storage, service endpoints also work between virtual networks and service instances in a paired region."

Lab tested.

upvoted 3 times

✉️👤 **BlackZeros** 8 months, 3 weeks ago

Selected Answer: C

C is perhaps the right answer, you create a VNET on the paired region from where you will access the storage1

upvoted 1 times

✉️👤 **sapien45** 8 months, 3 weeks ago

and PERHAPS instead of conjecturing, you should look for official Azure litterature to docuement your arguments, This is whole point.

upvoted 2 times

**HOTSPOT -**

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

Your app is stopped. App Service plan charges still apply.

**Essentials**

Resource group (change) RG1	URL <a href="https://as12.azurewebsites.net">https://as12.azurewebsites.net</a>
Status Stopped	Health Check Configured
Location North Europe	App Service Plan ASP1 (P1v2:1)
Subscription (change) Subscription1	FTP/deployment user set No FTP/deployment user set
Subscription ID 846f6nnnt-nt8e-794i-k478-649ws1576487	FTP hostname <a href="ftp://waws-prod-db3-167.azurewebsites.windows.net/site/wwwroot">ftp://waws-prod-db3-167.azurewebsites.windows.net/site/wwwroot</a>
	FTPS hostname <a href="https://waws-prod-db3-167.azurewebsites.windows.net/site/wwwroot">https://waws-prod-db3-167.azurewebsites.windows.net/site/wwwroot</a>

Tags (change)  
Click here to add tags

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

**VNet Integration**

**VNet Configuration**

Securely access resources available in or through your Azure VNet. [Learn more](#)

**VNet Details**

VNet NAME	Vnet1
LOCATION	North Europe

**VNet Address Space**

Start Address	End Address
10.100.0.0	10.100.255.255

**Subnet Details**

Subnet NAME	Subnet1
-------------	---------

**Subnet Address Space**

Start Address	End Address
10.100.2.0	10.100.2.255

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

## Private Endpoint connections

+ Add Refresh | ✓ Approve ✗ Reject 🗑 Remove



### Private Endpoint connections

Private access to services hosted on the Azure platform, keeping your data on the Microsoft network [Learn more](#)

Filter by name or description All connection states

Connection name ↑ Connection state ↑↓ Private endpoint ↑↓ Description

No results.

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
Subnet2 can contain only App Service apps in the ASP1 App Service plan	<input type="radio"/>	<input type="radio"/>
As12 will use an IP address from Subnet2 for network communications	<input type="radio"/>	<input type="radio"/>
Computers in Vnet1 will connect to a private IP address when they connect to as12	<input type="radio"/>	<input type="radio"/>

Correct Answer:

#### Answer Area

Statements	Yes	No
Subnet2 can contain only App Service apps in the ASP1 App Service plan	<input checked="" type="radio"/>	<input type="radio"/>
As12 will use an IP address from Subnet2 for network communications	<input checked="" type="radio"/>	<input type="radio"/>
Computers in Vnet1 will connect to a private IP address when they connect to as12	<input type="radio"/>	<input checked="" type="radio"/>

Reference:

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

Geo13AZ Highly Voted 1 year, 5 months ago

1. Yes: Virtual Network Integration supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can use the same virtual network integration. <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration> under section “How regional virtual network integration works”.
2. Yes: “When regional virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app.”. <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration> under section “How regional virtual network integration works”.
3. No: “you can't use virtual network integration to provide inbound access to your app.”, if you need Inbound access to the App you will need to setup a Service Endpoint or Private Endpoint. <https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration> under “Regional virtual network integration”.

upvoted 36 times

GohanF2 7 months, 1 week ago

Great Answer.

upvoted 2 times

GohanF2 7 months, 1 week ago

Well explained

upvoted 1 times

✉️ **Pradh** 8 months, 2 weeks ago

for 2nd question if you are saying this "The outbound addresses that are listed in the app properties portal are the addresses still used by your app" , then why is the answer yes ? it should be NO right ?

upvoted 1 times

✉️ **Bharat** Highly Voted 1 year, 8 months ago

Clearly Subnet2 in the question statements has to be Subnet1?

upvoted 27 times

✉️ **RandomUser** 1 year, 8 months ago

It is already fixed in the exam as of today. It shows Subnet2 in the picture, so it matches the question now.

upvoted 7 times

✉️ **laige** 1 year, 8 months ago

agreed, otherwise it going to be 3 no.

upvoted 13 times

✉️ **mrgreat** Most Recent 3 months, 1 week ago

YYN.

Same question: <https://www.examtopics.com/exams/microsoft/az-700/view/11/>

upvoted 1 times

✉️ **TJ001** 5 months ago

YYN - just ignore subnet name error as highlighted by others already :)

upvoted 2 times

✉️ **jellybiscuit** 8 months, 3 weeks ago

As written/pictured it's NNN

If the vnet integration is really with subnet2, the it's YYN

upvoted 3 times

✉️ **sapien45** 8 months, 3 weeks ago

If we replace Subnet1 by Subnet2 in the screenshot :

YYN

\*\*"Subnet1" is dedicated to vnet integration

\* as12 will use IP address from "subnet1" for outbound

\*If you need Inbound access to the App you will need to setup a Service Endpoint or Private Endpoint.

upvoted 3 times

✉️ **nakul115** 9 months, 2 weeks ago

it should be NNN

The App service status is "stopped"

upvoted 2 times

✉️ **Skankhut** 4 months, 2 weeks ago

Lol where's the downvote button

upvoted 2 times

✉️ **Cristoicach91** 9 months, 3 weeks ago

There is no private endpoint configured. NNN

upvoted 3 times

✉️ **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22. Exam shows Subnet2 in the pictures.

upvoted 4 times

✉️ **Fearless90** 11 months, 4 weeks ago

Subnet1 can contain only App Service apps in the ASP1 App Service plan > Yes

"Subnet1" is dedicated to vnet integration

Virtual Network Integration supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can use the same virtual network integration.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional-virtual-network-integration-works>

The feature supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can only use the same virtual network integration to a specific subnet. If you need an app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan. The virtual interface used isn't a resource that customers have direct access to.

upvoted 1 times

✉️ **Fearless90** 11 months, 4 weeks ago

as12 will use an IP address from Subnet1 for network communications > Yes

as12 will use IP address from "subnet1" for outbound

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional-virtual-network-integration-works>

When regional virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app. However, if your outbound call is to a virtual machine or

private endpoint in the integration virtual network or peered virtual network, the outbound address will be an address from the integration subnet. The private IP assigned to an instance is exposed via the environment variable, WEBSITE\_PRIVATE\_IP.

upvoted 2 times

✉️ **Fearless90** 11 months, 4 weeks ago

Computers in Vnet1 will connect to a private IP address when they connect to as12 > No

"You can't use virtual network integration to provide inbound access to your app.", if you need Inbound access to the App you will need to setup a Service Endpoint or Private Endpoint.

The exhibit for private endpoints is empty.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual-network-integration>

When you use regional virtual network integration, you can use the following Azure networking features:

Network security groups (NSGs): You can block outbound traffic with an NSG that's placed on your integration subnet. The inbound rules don't apply because you can't use virtual network integration to provide inbound access to your app.

upvoted 1 times

✉️ **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

✉️ **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

✉️ **sleekdunga** 1 year, 4 months ago

1. Yes

2. Yes. When regional virtual network integration is enabled, your app makes outbound calls through your virtual network. The outbound addresses that are listed in the app properties portal are the addresses still used by your app.

3. No. Virtual network integration doesn't enable your apps to be accessed privately

upvoted 4 times

✉️ **sleekdunga** 1 year, 4 months ago

2. However, if your outbound call is to a virtual machine or private endpoint in the integration virtual network or peered virtual network, the outbound address will be an address from the integration subnet.

upvoted 1 times

✉️ **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022

upvoted 1 times

✉️ **Pravda** 1 year, 5 months ago

Variant on exam 1/6/2022

upvoted 2 times

✉️ **whatzapp95** 1 year, 6 months ago

Yes: "Subnet2" is dedicated to vnet integration

Yes: As12 will use ip address from "subnet 2" for outbound

Yes: Computer will use private endpoint for inbound to communicate to as12

upvoted 4 times

✉️ **Prutser2** 8 months, 1 week ago

box3: there is no private endpoint, exhibit has empty pr. endpoint, just saying, YYN

upvoted 2 times

✉️ **dusty\_dev** 1 year, 6 months ago

why is 3 Yes? It should be No. The exhibit for private endpoints is empty.

upvoted 12 times

**DRAG DROP -**

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

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

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

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

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

Select and Place:

**Actions**

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

**Answer Area****Correct Answer:****Actions**

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

**Answer Area**

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

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

Reference:

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

✉ **kerberos999** Highly Voted 1 year, 7 months ago

The order is wrong. If you need to avoid service interruption "Deny Public Access and Private Endpoint" should be configured at last  
upvoted 46 times

✉ **waqas** 1 year, 5 months ago

So plz guide what should be the right sequence and answer then????

upvoted 5 times

✉ **ChrisCrown** 9 months, 1 week ago

Deploy VM --> Install DNS Server role --> Configure On-prem to fwd blob.core.windows.net --> disable public access.

upvoted 25 times

✉ **Pravda** Highly Voted 1 year, 5 months ago

Think through the steps and this is an easy question to answer.

+ 5 Deploy VM This VM is for DNS.

+ 1 Install DNS Role and create DNS forward entry DNS server in Azure has blob.core mapped to IP address 168.63.129.16

+ 2 ON-prem DNS to VM The on-prem DNS server lookup requests for blob need to be forwarded to the DNS server in Azure with the blob.core to IP address mapping.

+ 3 Private-endpoint creation and disable public access – With DNS settings complete users can connect to blob, without interruption. Public access can be disabled.

Not sure why 4 could not be used in place of creating VM and installing DNS role. I suspect is has something to do with interruption of service. But since we aren't told how they are accessing the blob now who knows.

upvoted 42 times

✉️ **ian2387** 1 year, 2 months ago

I agree with this

upvoted 2 times

✉️ **Zeppoonstream** Most Recent 2 months ago

From where do i get the info what the ip is ?!

upvoted 1 times

✉️ **GohanF2** 7 months, 1 week ago

Answers are as following:

1. Deploy a virtual machine to a subnet in Vnet1
2. Install DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
3. Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine (This is assuming that there is an IPsec connection from your on-premises to your Azure Virtual Environment).
4. Configure a private endpoint on storageaccount1 and disable public access to the account. (This option is done on last due that a storage account can only have one type of access mode at a time, if we set this option by first, we will be interrupting the access publicly and the question says that we need to avoid service interruption.)

The option of: Configure on-premises DNS server to forward blob.core.windows.net to 168.63.129.16 is wrong due that the ip address: 168.63.129.16 exists only in Azure Environment and our On-premises network won't know any route of how to get to that network.

upvoted 10 times

✉️ **jellybiscuit** 8 months, 3 weeks ago

This is what I was doing, without really thinking about the disruption. After seeing the comments and thinking back on my answer, I think the key is to simply pause between enabling the private endpoint and disabling public access to allow DNS to propagate after you add the PE.

- deploy vm
- install dns
- on-prem dns forwards to vm
- configure private endpoint on storage account - [ insert pause here] then disable public access

upvoted 3 times

✉️ **sapien45** 8 months, 3 weeks ago

Very similar setup described here :

<https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#on-premises-workloads-using-a-dns-forwarder>

upvoted 2 times

✉️ **Jamesat** 10 months, 1 week ago

To avoid service disruption you would have to do the Private Endpoint last.

Otherwise you've lost access until you have finished building the VMs and installing DNS etc.

upvoted 1 times

✉️ **zerocool114** 11 months, 2 weeks ago

on exam today

upvoted 1 times

✉️ **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 1 times

✉️ **Fearless90** 11 months, 4 weeks ago

5. Deploy a virtual machine to a subnet in Vnet1
5. Deploy VM. This VM is for DNS.

1. Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
  1. Install DNS Role and create DNS forward entry. DNS server in Azure has blob.core.windows.net mapped to IP address 168.63.129.16
  2. Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine
  2. ON-prem DNS to VM The on prem DNS server lookup requests for blob need to be forwarded to the DNS server in Azure with the blob.core.windows.net to IP address mapping.
  3. Configure a private endpoint on storageaccount1 and disable public access to the account
  3. Private-endpoint creation and disable public access
- With DNS settings complete users can connect to blob, without interruption. Public access can be disabled.  
Avoid service interruption "Deny Public Access and Private Endpoint" should be configured at last

upvoted 1 times

✉️ **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

✉ **kogunribido** 11 months, 4 weeks ago

Appeared on exam 6/27/2022

upvoted 1 times

✉ **Pravda** 1 year, 5 months ago

Variant on exam 1/6/2022

upvoted 3 times

✉ **AidenYoukhana** 1 year, 5 months ago

Correct Order:

5

1

2

3

upvoted 13 times

✉ **vivert** 1 year, 6 months ago

VM>DNSRole

+FwdtoAzureDNA+

ON-premDNS to FwdtoAzureVM

+Private-endpoint creation

upvoted 5 times

✉ **Pravda** 1 year, 6 months ago

What is the correct answer?

upvoted 1 times

✉ **Mat\_212223** 1 year, 7 months ago

Correct!

upvoted 1 times

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

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

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

What should you do first?

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

**Correct Answer:** D

Reference:

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

✉️ **christianpageqc** Highly Voted 1 year, 8 months ago

I think answer should be B. Create a new subnet, since both Vnet and App Service are in the same region.

<https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet#enable-vnet-integration>

Regional VNet Integration = "If the VNet is in the same region, either create a new subnet or select an empty pre-existing subnet"

upvoted 79 times

✉️ **Bharat** 1 year, 8 months ago

You are correct. Thanks for the reference link.

upvoted 5 times

✉️ **dpinlaguna** Highly Voted 1 year, 8 months ago

I think it should be B since resources are in the same region (Regional VNet Integration), new subnet does not incur cost. The VPN Gateway solution incurs a cost (Gateway-required VNet Integration...When you connect directly to VNet in other regions or to a classic virtual network in the same region, you need an Azure Virtual Network gateway provisioned in the target VNet.)

upvoted 8 times

✉️ **RandomUser** 1 year, 8 months ago

But don't forget VNet integration is only available from Premium onwards. That might also be quite an increase in cost.

upvoted 2 times

✉️ **RandomUser** 1 year, 8 months ago

My bad, VNet integration is already available in smaller SKUs as well. I fucked up this question in the exam so I though I'd better fix my comment here.

upvoted 17 times

✉️ **breakpoint0815** Most Recent 2 months, 3 weeks ago

**Selected Answer: B**

Answer D suggests creating a gateway subnet and deploying a virtual network gateway, which is used for connecting virtual networks across different regions or connecting to on-premises networks. While it would provide access to resources in Vnet1, it would incur additional costs and is not necessary for connecting an App Service app to a virtual network in the same region. Therefore, creating a new subnet (answer B) is the correct and more cost-effective solution in this scenario.

upvoted 1 times

✉️ **samir111** 4 months ago

B should be the answer

upvoted 1 times

✉️ **ragav21** 8 months ago

**Selected Answer: B**

B should be the right answer

upvoted 1 times

✉️ **sapien45** 8 months, 3 weeks ago

**Selected Answer: B**

Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network. Private site access refers to making an app accessible only from a private network, such as from within an Azure virtual network. Virtual network integration is used only to make outbound calls from your app into your virtual network.

Regional virtual network integration: When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

The virtual network integration feature:

Requires a supported Basic or Standard, Premium, Premium v2, Premium v3, or Elastic Premium App Service pricing tier.

upvoted 3 times

 **wetraining123** 9 months, 4 weeks ago

it should be B.

Create a subnet and Integrate it with the App1

upvoted 1 times

 **Pradh** 8 months, 2 weeks ago

existing subnet already seems empty. why need new subnet ?

upvoted 1 times

 **Jamesat** 10 months, 1 week ago

**Selected Answer: B**

B is correct as the resources are in the same region.

Why would you even think about a VPN gateway? Odd answer. Exam Topics should review this one!

upvoted 1 times

 **Goseu** 10 months, 3 weeks ago

**Selected Answer: B**

Answer is B

upvoted 2 times

 **rac\_sp** 11 months, 1 week ago

**Selected Answer: B**

create a new subnet because both resources are in the same region, no need to a gateway that is only required when resources are in different regions.

upvoted 5 times

 **Pradh** 8 months, 2 weeks ago

existing subnet already seems empty. why need new subnet ?

upvoted 1 times

 **rac\_sp** 11 months, 1 week ago

**Selected Answer: B**

In the same region there is no need of a Virtual Network Gateway

upvoted 3 times

 **zerocool114** 11 months, 2 weeks ago

on exam today, answer B

upvoted 1 times

 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 2 times

 **kinder2** 1 year ago

**Selected Answer: B**

"B"

Regional virtual network integration supports connecting to a virtual network in the same region and doesn't require a gateway.  
<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual-network-integration>

upvoted 2 times

 **Pradh** 8 months, 2 weeks ago

existing subnet already seems empty. why need new subnet ?

upvoted 1 times

 **borekbp** 1 year, 3 months ago

but there is info in question that you have already one subnet, can we use it for gateway or vnet-integration? why create new one?

upvoted 1 times

 **Payday123** 11 months, 3 weeks ago

Because we need to provide access to resources in this one subnet. If this subnet is integrated with App Service we will not be able to create any other resources

upvoted 1 times

 **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

 **nitinkumarmca** 1 year, 4 months ago

**Selected Answer: B**

Subnet as it doesn't incur additional cost. VPN Gateway is required for cross region integration or Classic VNET in same region.  
upvoted 2 times

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

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

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

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

What should you provide?

- A. app1.contoso.onmicrosoft.com
- B. app1.private.contoso.com
- C. app1privatelink.azurewebsites.net
- D. app1.contoso.com

**Correct Answer: C**

✉  **Sahildange** Highly Voted 1 year, 8 months ago

When you use Private Endpoint for Web App, the requested URL must match the name of your Web App. By default mywebappname.azurewebsites.net.

By default, without Private Endpoint, the public name of your web app is a canonical name to the cluster. For example, the name resolution will be:

DNS

Name Type Value

mywebapp.azurewebsites.net CNAME clustername.azurewebsites.windows.net  
 clustername.azurewebsites.windows.net CNAME cloudservicename.cloudapp.net  
 cloudservicename.cloudapp.net A 40.122.110.154

When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net. For example, the name resolution will be:

DNS

Name Type Value Remark

mywebapp.azurewebsites.net CNAME mywebapp.privatelink.azurewebsites.net  
 mywebapp.privatelink.azurewebsites.net CNAME clustername.azurewebsites.windows.net  
 clustername.azurewebsites.windows.net CNAME cloudservicename.cloudapp.net  
 cloudservicename.cloudapp.net A 40.122.110.154 <https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint> Hence answer is C

upvoted 15 times

✉  **GohanF2** 7 months, 1 week ago

Well explained

upvoted 1 times

✉  **AzureLearner01** Most Recent 3 months, 1 week ago

For me the provided answer is correct. I've done a few tests in the lab and we only need to provide the dns record that is registered automatically in DNS to the developer. this is app1.privatelink.azurewebsite.net. My first opinion was app1.azurewebsites.net (which is not existing) that would be translated to app1.privatelink.azurewebsite.net. By default the app is not registered in the "custom" private DNS Zone private.contoso.com. It is auto registered only in privatelink.azurewebsites.net. I'm not 100% sure but i don't think there is no way to not register it in the privatelink.azurewebsites.net and instead register it in private.contoso.com by default.

upvoted 1 times

✉  **samir111** 4 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

✉  **DeepMoon** 5 months, 1 week ago

Be mindful of group think; making you see this the wrong way and voting for the wrong answer. @zenithcsa1 pointed to the correct answer. Use the same connection string to connect to your App Configuration store using private endpoints as you would use for a public endpoint. Don't connect to the store using its privatelink subdomain URL.

<https://learn.microsoft.com/en-us/azure/azure-app-configuration/concept-private-endpoint#connecting-to-private-endpoints>

upvoted 1 times

✉ **Skankhunt** 4 months, 2 weeks ago

The link you provided is specifically for Azure App Configuration.

Rather use the below article:

<https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint>

upvoted 1 times

✉ **TJ001** 5 months ago

yes it does not connect with private end point URL.. however there is no better option in the available list. I dont agree with option B unless there is custom domain created for the App Service it does not make sense.. This question should have been phrased better.

upvoted 1 times

✉ **mingorad** 8 months, 4 weeks ago

C is correct

Expl : <https://learn.microsoft.com/en-us/azure/app-service/networking/private-endpoint>

"When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net."

upvoted 1 times

✉ **zenithcsa1** 9 months, 2 weeks ago

**Selected Answer: B**

Not sure what's the purpose of giving name to developers. Just be aware that you can NOT connect to the App Service through xxx.privatelink.azurewebsite.net. Azure DNS uses the name, not us.

<https://docs.microsoft.com/en-us/azure/azure-app-configuration/concept-private-endpoint#connecting-to-private-endpoints>

upvoted 1 times

✉ **phoenix14** 5 months, 3 weeks ago

Key to this question here is you need to provide hostname registered in Azure DNS and not your private zone. Hence answer is C.

upvoted 1 times

✉ **pinchocr** 1 year ago

**Selected Answer: C**

Correct

upvoted 1 times

✉ **rockethack** 1 year, 3 months ago

This question was on the exam on 18th Feb 2022.

upvoted 1 times

✉ **Kimimoto** 1 year, 4 months ago

Appeared in exam on 11/Feb/2022

upvoted 1 times

✉ **kjfdzkkbsm** 1 year, 4 months ago

**Selected Answer: C**

From the docs: When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net.

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

upvoted 3 times

✉ **Contactfornitish** 1 year, 5 months ago

Appeared in exam on 17/01/2022 and I ended up putting A instead :(

upvoted 1 times

✉ **Pravda** 1 year, 5 months ago

Much more complicated variant on the exam 1/6/2022

upvoted 3 times

✉ **AidenYoukhana** 1 year, 5 months ago

Answer: app1.privatelink.azurewebsites.net

upvoted 3 times

✉ **dpinlaguna** 1 year, 8 months ago

<https://docs.microsoft.com/en-us/learn/modules/introduction-azure-private-link/3-how-azure-private-link-works>:

Clients that connect to a Private Link resource don't need to use the Private Endpoint's assigned IP address in the connection string. Instead, if you configure the Private Endpoint to integrate with your private DNS zone, then Azure automatically assigns a FQDN to the endpoint. For example, if the Private Link resource is an Azure Storage table, the FQDN will be something like mystorageaccount1234.table.core.windows.net.

upvoted 3 times

✉ **Bharat** 1 year, 8 months ago

Correct answer is A not C, i.e., app1.contoso.onmicrosoft.com

upvoted 1 times

✉ **christianpageqc** 1 year, 8 months ago

VNet DNS auto-registration won't create any DNS for private link according to this article : <https://docs.microsoft.com/en-us/azure/dns/private-dns-autoregistration#restrictions>

"Auto registration works only for virtual machines"

As for private link auto DNS, it seems bound to public Microsoft domains.. I think we would need to deploy DNS forwarder and CNAME to resolve something other then A.

upvoted 3 times

✉ **Bharat** 1 year, 8 months ago

So what should be the answer then?

upvoted 1 times

✉ **Bharat** 1 year, 8 months ago

Given answer is correct and I was wrong. @christianpageqc, thanks for the thoughtful answer. Here is an article that helped me clarify the answer: <https://blog.baeke.info/2021/06/22/azure-app-services-with-private-link/>

upvoted 2 times

✉ **Prutser2** 8 months, 1 week ago

great link, well explained!

upvoted 1 times

You have Azure App Service apps in the West US Azure region as shown in the following table.

Name	App Service Plan	Number of instances
App1	ASP1	3
App2	ASP1	3
App3	ASP2	2
App4	ASP3	1

You need to ensure that all the apps can access the resources in a virtual network named VNet1 without forwarding traffic through the internet.

How many integration subnets should you create?

- A. 0
- B. 1
- C. 3
- D. 4
- E. 6

**Correct Answer: C**

One integration subnet is required per App Service Plan regardless of how many apps are running in the App Service Plan.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration>

 **pinchocr** Highly Voted 1 year ago

**Selected Answer: C**

one per App Service Plan: The feature supports only one virtual interface per worker. One virtual interface per worker means one regional virtual network integration per App Service plan. All the apps in the same App Service plan can only use the same virtual network integration to a specific subnet. If you need an app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan. The virtual interface used isn't a resource that customers have direct access to.

<https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#how-regional-virtual-network-integration-works>

upvoted 8 times

 **TJ001** Most Recent 5 months ago

one per App Service Plan make sense..multiple apps with in the same plan can use the same subnet provided it has enough IP space....I will go with C

upvoted 2 times

 **jkklim** 1 year, 1 month ago

all azure app service apps in the same region, so we use regional virtual network integration.

All the apps in the same App Service plan can only use the same virtual network integration to a specific subnet. If you need an app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan

upvoted 1 times

 **jkklim** 1 year, 1 month ago

therefore 3 subnets = C

upvoted 3 times

 **FabioS** 1 year, 1 month ago

Subnet requirements

Virtual network integration depends on a dedicated subnet. When you create a subnet, the Azure subnet loses five IPs from the start. One address is used from the integration subnet for each plan instance. If you scale your app to four instances, then four addresses are used. Answer = D

upvoted 1 times

 **pinpin06** 1 year, 1 month ago

there is 3 plan instances ASP1, ASP2, ASP3, I would say this is response C

upvoted 3 times

 **sapien45** 8 months, 3 weeks ago

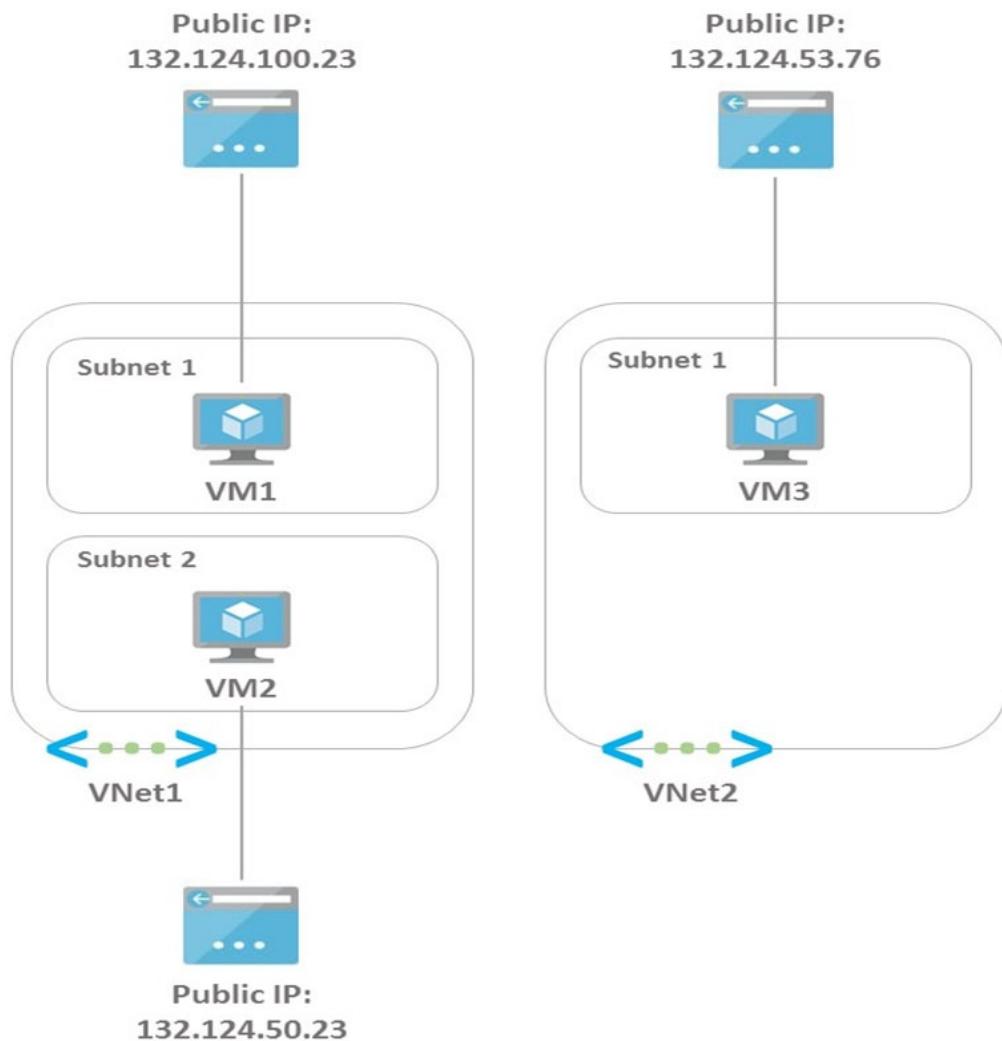
That is some weird logic here. If you need an app to connect to another virtual network or another subnet in the same virtual network, you need to create another App Service plan

1+1+1=3

upvoted 1 times

HOTSPOT -

You have the Azure environment shown in the Azure Environment exhibit.



The settings for each subnet are shown in the following table.

Subnet	Service endpoint
Vnet1/Subnet1	Storage
Vnet1/Subnet2	Storage
Vnet2/Subnet1	None

The Firewalls and virtual networks settings for storage1 are configured as shown in the Storage1 exhibit.

The screenshot shows the 'storage1 | Networking' blade in the Azure portal. The left sidebar lists 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', 'Storage Explorer (preview)', 'Containers', 'File shares', 'Queues', 'Tables', 'Networking' (which is selected), and 'Azure CDN'. The main area has tabs for 'Firewalls and virtual networks' (selected), 'Private endpoint connections', and 'Custom domain'. Under 'Firewalls and virtual networks', there are sections for 'Allow access from' (set to 'Selected networks'), 'Virtual networks' (listing 'VNet1' with subnet 'Subnet1' and address range '172.20.0.0/24' in 'Enabled' status), and 'Firewall' (with IP ranges '132.100.53.0/25' and '132.124.53.0/26' listed). Buttons for 'Save', 'Discard', and 'Refresh' are at the top.

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
VM1 can access storage1.	<input type="radio"/>	<input type="radio"/>
VM2 can access storage1 by using a service endpoint.	<input type="radio"/>	<input type="radio"/>
VM3 can access storage1 by using the public IP address.	<input type="radio"/>	<input type="radio"/>

**Correct Answer:**

## Answer Area

Statements	Yes	No
VM1 can access storage1.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can access storage1 by using a service endpoint.	<input type="radio"/>	<input checked="" type="radio"/>
VM3 can access storage1 by using the public IP address.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

The firewall allows VNet1\Subnet1 through the service endpoint.

Box 2: No -

The firewall does not allow VNet1\Subnet2 through the service endpoint.

Box 3: No -

The firewall allows 132.124.53.0/26 which means it allows all IP addresses between 132.124.53.0 and 132.124.53.63. The public IP of VM3 is 132.124.53.76 which is outside the allowed range.

 **Jamesat** Highly Voted 10 months, 1 week ago

Correct tested in my lab.

Yes, No, No

For question 2 Subnet2 has a service endpoint but is not present in the Firewall settings so would be denied.

upvoted 19 times

 **Goofier** 5 months ago

IP network rules can't be used in the following cases:

To restrict access to clients in same Azure region as the storage account.

IP network rules have no effect on requests originating from the same Azure region as the storage account. Use Virtual network rules to allow same-region requests.

Source: <https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range>

Yes, Yes, No

upvoted 2 times

 **flurgen248** 2 months, 3 weeks ago

I think it's Yes, No, No.

IP network rules have no effect on requests originating from the same Azure region as the storage account. Use Virtual network rules to allow same-region requests.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-an-internet-ip-range>

The service endpoint routes traffic from the VNet through an optimal path to the Azure Storage service. Administrators can then configure network rules for the storage account that allow requests to be received from specific subnets in a VNet.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-a-virtual-network>

If you look at the storage1 networking image, there are separate sections for IP addresses and virtual networks. The section with IP addresses is the "IP Network rules" section, but since it's also using the "Virtual Network" section then you can only access storage1 using service endpoints that are explicitly listed.

upvoted 1 times

 **JulienYork** Highly Voted 1 year, 1 month ago

Box 1: Yes -

The firewall allows VNet1\Subnet1 through the service endpoint.

This is wrong in the answer

Box 2: YES

It is already accessing with service endpoint no need to access via firewall

Box 3: No -

The firewall allows 132.124.53.0/26 which means it allows all IP addresses between 132.124.53.0 and 132.124.53.63. The public IP of VM3 is 132.124.53.76 which is outside the allowed range.

upvoted 10 times

 **jellybiscuit** 8 months, 3 weeks ago

I would agree with you if we were discussing private endpoints, as they bypass public access and firewall rules. Service Endpoints do not. VM2 can pass through subnet 1 to get to the endpoint, but its source address is still subnet 2 which has not been granted access on the storage account.

If a storage account has a Private Endpoint and no rules you can connect to it.

If a storage account has a Service Endpoint and no rules you cannot connect to it.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal#grant-access-from-a-virtual-network>

"You can enable a Service endpoint for Azure Storage within the VNet. The service endpoint routes traffic from the VNet through an optimal path to the Azure Storage service. The identities of the subnet and the virtual network are also transmitted with each request. Administrators can then configure network rules for the storage account that allow requests to be received from specific subnets in a VNet. Clients granted access via these network rules must continue to meet the authorization requirements of the storage account to access the data."

upvoted 7 times

 **sapien45** 8 months, 3 weeks ago

YYN, I concur

upvoted 3 times

 **sapien45** 8 months, 2 weeks ago

I stand corrected by jellybiscuit YNN

upvoted 6 times

 **Ajdifasudfo0** 6 months, 2 weeks ago

you better go do AZ-900. seems to be more fitting your skill level

upvoted 1 times

 **Takloy** 5 months, 3 weeks ago

the fact that you're using dumps to review is also not something to be proud of. everybody here is an AZ900 skill level.

upvoted 4 times

 **TJ001** (Most Recent) 5 months ago

Agree with Yes No No

upvoted 5 times

 **chatlisi** 5 months, 1 week ago

According this, it should be Y, Y, N

"With service endpoints, the source IP addresses of the virtual machines in the subnet for service traffic switches from using public IPv4 addresses to using private IPv4 addresses. Existing Azure service firewall rules using Azure public IP addresses will stop working with this switch."

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

upvoted 1 times

 **\_fvt** 2 months, 2 weeks ago

Yes you are well explaining why the public allowed IP range will not allow the connection from VM2 and why the private IP addresses from VNet1/Subnet2 should be allowed instead (only VNet1/subnet1 is allowed if you look on the storage account configuration)

So, Y,N,N.

upvoted 1 times

 **unclegrandfather** 11 months, 3 weeks ago

A version of this appeared on the exam Jun/28/22. Make sure you understand the concepts here

upvoted 1 times

 **pinchocr** 1 year ago

You cannot filter public IPs when de vnet and the storage accounts are in the same regions. The answer is correct YES-NO-NO

upvoted 5 times

 **Jun\_AZ500** 1 year ago

Correct me if I'm wrong on Q2, the answer still No according to this

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal>

IP network rules can't be used in the following cases:

To restrict access to clients in same Azure region as the storage account.

IP network rules have no effect on requests originating from the same Azure region as the storage account. Use Virtual network rules to allow same-region requests.

upvoted 1 times

 **jpetix** 1 year ago

But the Firewall in question is on the Service endpoint, and it only allows Vnet1, Subnet1.

upvoted 1 times

 **wsrudmen** 1 year ago

It's YES-YES-NO

But I'm disagree with you Julien for Box2.

VM2 is in Subnet2 that is not linked to the storage account like Subnet1.

So VM2 can only access through Internet using its public IP. And in The Firewall table VM2 is allowed.

NB: Please correct me if I'm wrong

upvoted 2 times

 **Payday123** 11 months, 3 weeks ago

Question is if it access using service endpoint not public IP

upvoted 3 times

**DRAG DROP -**

You have two Azure subscriptions named Subscription1 and Subscription2. Subscription1 contains a virtual network named Vnet1. Vnet1 contains an application server. Subscription2 contains a virtual network named Vnet2.

You need to provide the virtual machines in Vnet2 with access to the application server in Vnet1 by using a private endpoint.

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

Select and Place:

**Actions**

In Subscription 1, accept the private endpoint connection request.

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

Enable virtual network peering between Vnet1 and Vnet2.

Deploy an Azure Standard Load Balancer in front of the application server.

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

**Answer Area****Correct Answer:****Actions**

Enable virtual network peering between Vnet1 and Vnet2.

**Answer Area**

Deploy an Azure Standard Load Balancer in front of the application server.



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

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

In Subscription 1, accept the private endpoint connection request.

Step 1: Deploy an Azure Load Balancer in front of the application server

Configure your application to run behind a standard load balancer in your virtual network.

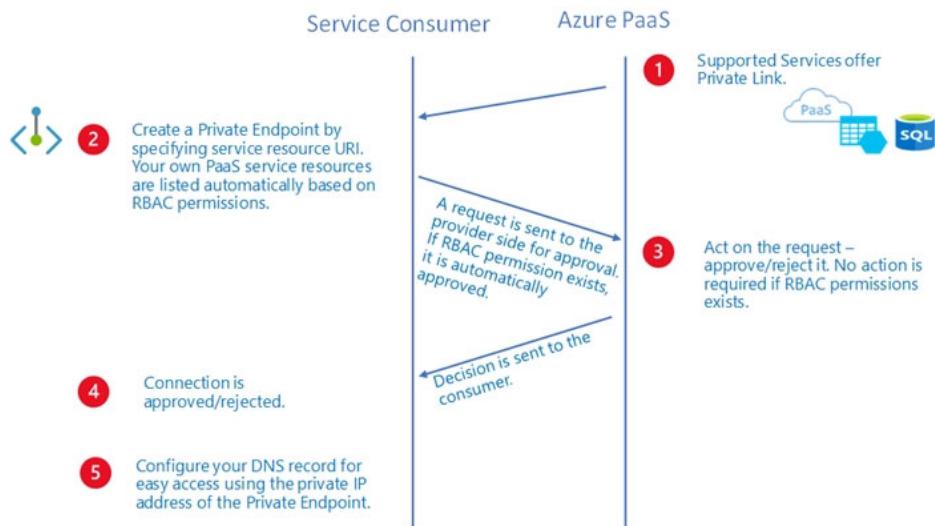
Step 2: In Subscription 1, create a private link service and attach the service to the frontend IP configuration of the load balancer.

Create a Private Link Service referencing the load balancer above.

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

Private Link service can be accessed from approved private endpoints in any public region. The private endpoint can be reached from the same

virtual network, regionally peered VNets, globally peered VNets and on premises using private VPN or ExpressRoute connections.



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

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

Not:

Incorrect: Enable virtual network peering between Vnet1 and Vnet2.

Reference:

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

**jellybiscuit** Highly Voted 8 months, 3 weeks ago

I spent the entire time wondering why I'm creating a load balancer.  
Finally realized it's an "application server" and not an "app service"

Answer is correct.

upvoted 8 times

**TJ001** Most Recent 5 months ago

Answer is correct  
Please note peering is not required .. the whole point of Private Link is to provide connectivity without peering..  
upvoted 1 times

**alexGv** 5 months, 4 weeks ago

I see something a little confused, maybe the question itself is "wrong" because how is possible to use a LoadBalancer that I assume as "Internal" to publish a Private Endpoint "attaching the service private IP of the Private Endpoint as frontend IP of the Load Balancer" and not "as the Backend pool of it".

Then why we need a NLB if the Private Endpoint itself is capable to "hear" connections through his own private IP address?  
Can somebody else try to explain me...Thanks!

upvoted 1 times

**alexGv** 5 months, 4 weeks ago

Sorry, reviewed,  
<https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview#workflow>  
upvoted 1 times

**GohanF2** 7 months, 1 week ago

Answer is correct.  
upvoted 1 times

**ragav21** 8 months ago

Why is peering not sufficient ?  
upvoted 2 times

**tfktfk** 2 weeks, 6 days ago

we use private link service to avoid ips overlap  
upvoted 1 times

**Leib** 8 months ago

it is but, you need to use private endpoint.  
upvoted 4 times

**Cristoicach91** 9 months, 3 weeks ago

correct  
upvoted 3 times

Question #9

Topic 5

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

- ☞ A virtual network named Vnet1
  - ☞ An App Service plan named ASP1
  - ☞ An Azure App Service named webapp1
- An Azure private DNS zone named private.contoso.com

- ☞ Virtual machines on Vnet1 that cannot communicate outside the virtual network

You need to ensure that the virtual machines on Vnet1 can access webapp1 by using a URL of <https://www.private.contoso.com>.

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

NOTE: Each correct selection is worth one point.

- A. Create a CNAME record that maps www.private.contoso.com to webapp1.contoso.onmicrosoft.com.
- B. Create a CNAME record that maps www.private.contoso.com to webapp1.private.contoso.com.
- C. Create a service endpoint for webapp1.
- D. Register an enterprise application in Azure AD for webapp1.
- E. Create a private endpoint for webapp1.
- F. Create a CNAME record that maps www.private.contoso.com to webapp1privatelink.azurewebsites.net.

**Correct Answer: EF**

E: You can use private DNS zones to override the DNS resolution for a private endpoint. A private DNS zone can be linked to your virtual network to resolve specific domains.

When you use Private Endpoint for Web App, the requested URL must match the name of your Web App. When you deploy a Private Endpoint, we update the

DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net. For example, the name resolution will be (Name, Type, Value): mywebapp.azurewebsites.net CNAME mywebapp.privatelink.azurewebsites.net

Reference:

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

 **TJ001** 5 months ago  
EF, only assumption custom domain is added for App Service already  
upvoted 3 times

 **Prutser2** 8 months, 1 week ago  
**Selected Answer: EF**  
correct  
upvoted 2 times

 **jellybiscuit** 8 months, 3 weeks ago  
**Selected Answer: EF**  
correct  
upvoted 1 times

 **StephenKDS** 9 months ago  
**Selected Answer: EF**  
correct - makes sense  
upvoted 1 times

You have an Azure Front Door instance named FD1 that is protected by using Azure Web Application Firewall (WAF).

FD1 uses a frontend host named app1.contoso.com to provide access to Azure web apps hosted in the East US Azure region and the West US Azure region.

You need to configure FD1 to block requests to app1.contoso.com from all countries other than the United States.

What should you include in the WAF policy?

- A. a custom rule that uses a match rule
- B. a frontend host association
- C. a custom rule that uses a rate limit rule
- D. a managed rule set

**Correct Answer: A**

✉️  **StephenKDS** Highly Voted 9 months ago

\*host = host

upvoted 9 times

✉️  **sapien45** Highly Voted 8 months, 2 weeks ago

**Selected Answer: A**

Custom rules allow you to create tailored rules to suit the exact needs of your applications and security policies. Now, you can restrict access to your web applications by country/region. As with all custom rules, this logic can be compounded with other rules to suit the needs of your application.

To create a geo-filtering custom rule in the Azure portal, simply select Geo location as the Match Type, and then select the country/region or countries/regions you want to allow/block from your application.

upvoted 6 times

✉️  **omgMerrick** Most Recent 4 months ago

**Selected Answer: A**

Answer is correct.

- A. a custom rule that uses a match rule

Source:

<https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-geo-filtering>

upvoted 1 times

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

- A. Azure DDoS Protection for virtual networks
- B. private endpoints
- C. Azure Virtual Network NAT
- D. service endpoint policies

**Correct Answer:** B

 **omgMerrick** 4 months ago

**Selected Answer: B**

B. private endpoints

Private endpoints require IP addresses in the subnets. Other resources such as Azure DDoS Protection for virtual networks, Azure Virtual Network NAT, and service endpoint policies do not require IP addresses in the subnets.

upvoted 2 times

 **lambdaCarre** 4 months, 3 weeks ago

Private endpoint is the correct answer. Indeed each private endpoint is associated with a network interface card which has a private IP

upvoted 2 times

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

✉  **JennyHuang36** 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 2 times

✉  **omgMerrick** 4 months ago

**Selected Answer: D**

Answer is correct.

D. a private DNS zone named privatelink.database.windows.net

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

Source:

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

upvoted 4 times

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

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

You need to ensure that VM1 and VM2 can connect only to storage1. The solution must meet the following requirements:

- Prevent VM1 and VM2 from accessing any other storage accounts
- Ensure that storage1 is accessible from the internet.

What should you use?

- a network security group (NSG)
- a service endpoint policy
- a private link
- a private endpoint

**Correct Answer: B**

✉ **omgMerrick** Highly Voted 4 months ago

**Selected Answer: B**

Answer appears to be correct.

B. a service endpoint policy

Virtual Network (VNet) service endpoint policies allow you to filter egress virtual network traffic to Azure Storage accounts over service endpoint, and allow data exfiltration to only specific Azure Storage accounts. Endpoint policies provide granular access control for virtual network traffic to Azure Storage when connecting over service endpoint.

Source:

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

upvoted 8 times

✉ **roshingrg** Most Recent 2 weeks, 6 days ago

B. a service endpoint policy

A service endpoint policy can be used to control the access to Azure Storage accounts from virtual networks. By creating a service endpoint policy, you can specify which storage accounts are allowed to be accessed from the virtual network, while blocking access to other storage accounts.

In this case, you can create a service endpoint policy that allows access to storage1 and associate it with the virtual network containing VM1 and VM2. This will ensure that VM1 and VM2 can only connect to storage1 and will be prevented from accessing any other storage accounts.

Additionally, to ensure that storage1 is accessible from the internet, you can configure the storage account's networking settings to allow public access. This can be done by enabling the appropriate settings such as allowing public access to blobs or enabling a public endpoint.

Using a network security group (NSG) would not provide the required granular control over specific storage accounts. A private link or private endpoint would enable private access to the storage account but would not allow access from the internet, which is a requirement in this scenario. Therefore, the best option is to use a service endpoint policy.

upvoted 3 times

✉ **tomtom2022** 1 month, 2 weeks ago

**Selected Answer: A**

The answer is A.

NSG only can filter whether the VMs can access the storage accounts via the service tag, but can't filter which storage account can be accessed.

upvoted 1 times

✉ **MrBlueSky** 2 months ago

**Selected Answer: A**

I believe the answer is A. NSG

Storage accounts are accessible from the internet by default so all we need to worry about is restricting the VMs access to all other storage accounts. This is only doable with an NSG from the options listed.

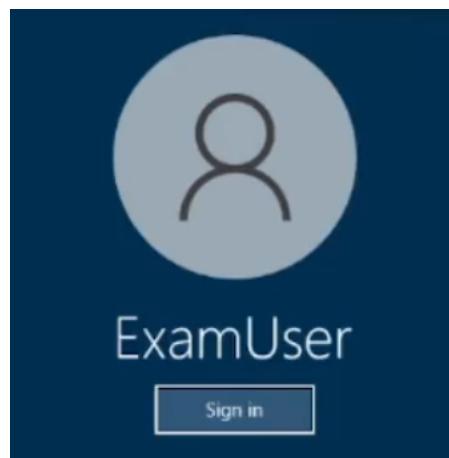
upvoted 1 times

 **TheBigMan** 1 week, 2 days ago

With NSG/service tags you can only limit the region. Like sql.EastUs .

Only viable in my opinion B

upvoted 1 times

**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: xxxxxxxxxxx

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 connections to the storage12345678 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name storage12345678.privatelink.blob.core.windows.net.

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

**Correct Answer:**

## Use private endpoints for Azure Storage

You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service.

Plan:

- Stage 1: Create a virtual network and subnet
- Stage 2: Create a private endpoint

Stage 1: Create a virtual network and subnet

Step 1: Sign in to the Azure portal.

Step 2: In the search box at the top of the portal, enter Virtual network. In the search results, select Virtual networks.

Step 3: Select + Create in Virtual networks.

Step 4: In the Basics tab of Create virtual network, enter or select the following information.

Subscription -Select your subscription.

Resource group - Select Create new.

Enter SomeName in Name and select OK.

Instance details

Name - Enter myVNet for example

Region - Select West Europe.

Step 5: Select Next: IP Addresses or the IP Addresses tab.

Step 6: Select the IP Addresses tab or select Next: IP Addresses at the bottom of the page.

Step 7: In the IP Addresses tab, enter the following information:

\* IPv4 address space - Enter 10.1.0.0/16

Step 8: Select Add subnet. In Edit subnet, enter the following information:

Subnet name - Enter mySubnet

Subnet address range - Enter 10.1.1.0/24 (as specified in the question)

Step 9: For the subnet: Select the Review + create tab or select the Review + create button.

Step 10: For the Virtual network: Select the Review + create tab or select the Review + create button.

Stage 2: Create a private endpoint

Step 1: In the search box at the top of the portal, enter Private endpoint. Select Private endpoints.

Step 2: Select + Create in Private endpoints.

Step 3: In the Basics tab of Create a private endpoint, enter or select the following information.

\* Storage subresource - storage12345678.privatelink.blob.core.windows.net

\* Private DNS integration.

Integrate with private DNS zone - Leave the default Yes.

\* Private DNS Zone

Leave the default (New) privatelink.blob.core.windows.net.

Step 4: Select Next: Resource.

Step 5: In the Resource pane, leave the defaults.

Step 6: Select Next: Virtual Network.

Step 7: In Virtual Network, enter or select the following information.

Virtual network - Select the virtual network you created in stage 1.

Subnet - Select the subnet you created in stage 1.

Step 8: Select Next: DNS.

Step 9: Leave the defaults in DNS. Select Next: Tags, then Next: Review + create.

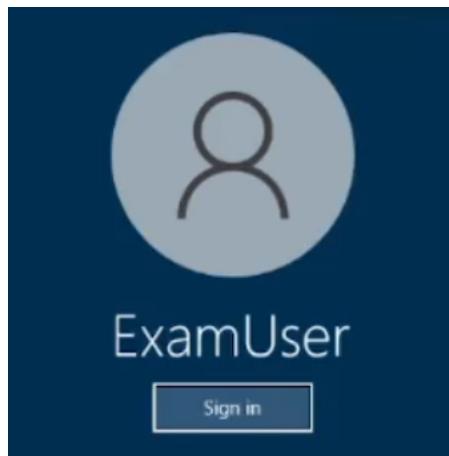
Step 10: Select Create.

Reference:

<https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>

<https://learn.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal>



**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: xxxxxxxxx

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](http://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.

**Correct 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>

✉  **JohnnyChimpo** 2 weeks ago

For anyone saying you have to use a public DNS - you are wrong. You need to create a virtual network links to the vnets in order for them to resolve the CNAME of www.relecloud.com to frontdoor1.azurefd.net - you cannot create vnet links to public DNS zones, only private DNS

upvoted 1 times

✉  **hal01** 2 months ago

To ensure that requests for www.relecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net, you can follow these steps:

Go to the Azure portal and navigate to the Relecloud DNS zone.

Create a new CNAME record by clicking on the "+ Record set" button.

In the "Name" field, enter "www".

In the "Type" field, select "CNAME".

In the "Alias" field, enter "frontdoor1.azurefd.net".

Save the record set by clicking the "Save" button.

This will create a CNAME record that maps the hostname "www.relecloud.com" to "frontdoor1.azurefd.net". Once this DNS change propagates to your virtual networks, requests to www.relecloud.com will resolve to frontdoor1.azurefd.net.

Note that you may need to update any firewall rules or network security groups to allow traffic to flow to frontdoor1.azurefd.net.

upvoted 2 times

✉  **Cabelen** 2 months, 3 weeks ago

You forgot to add the virtual networks links to the subnet that will use that private DNS zone.

upvoted 2 times

✉  **breakpoint0815** 2 months, 3 weeks ago

Only Azure networks are needed to resolve the address. Therefore -> private DNS zone

upvoted 2 times

✉  **Aziza\_Adam** 3 months, 4 weeks ago

It should be a public DNS not private

upvoted 1 times

 **cypkir** 4 months ago

You Have to use An Azure DNS zone and not a An Azure private DNS zone

upvoted 2 times

 **tzatziki** 4 months, 1 week ago

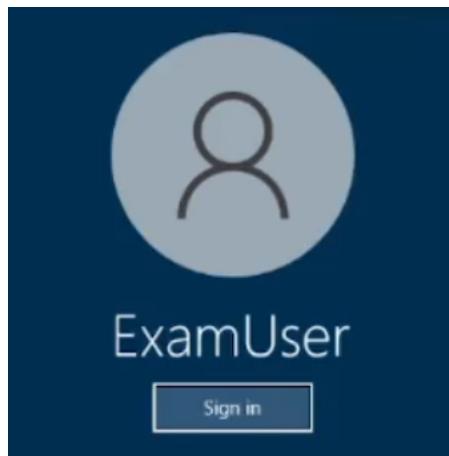
Excuse my, perhaps, silly question but why private.relecloud.com and not simply relecloud.com as concerns the naming of the private dns zone?  
would typing www.private.relecloud.com or www.releceloud.com would resolve the same way or smt???

upvoted 4 times

 **hal01** 2 months ago

it's a way to differentiate between the publicly accessible domain and the privately accessible domain. This naming convention may help prevent confusion and ensure that requests for private resources are directed to the correct DNS zone.

upvoted 1 times

**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: xxxxxxxxxxx

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 the storage12345678 storage account will only accept connections from the hosts on VNET1.

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

**Correct Answer:**

Azure storage account accepts connections from Virtual network.

Use private endpoints for Azure Storage

You can use private endpoints for your Azure Storage accounts to allow clients on a virtual network (VNet) to securely access data over a Private Link. The private endpoint uses a separate IP address from the VNet address space for each storage account service. Network traffic between the clients on the VNet and the storage account traverses over the VNet and a private link on the Microsoft backbone network, eliminating exposure from the public internet.

Link the private endpoint to the existing storage account

Step 1: In the search box at the top of the portal, enter Storage account. Select Storage accounts in the search results.

Step 2: Select or Search&find storage account storage12345678

Step 3: Select the Networking tab or select Next: Advanced then Next: Networking.

Step 4: In the Networking tab, under Network connectivity select Disable public access and use private access.

Step 5: In Private endpoint, select + Add private endpoint.

Step 6: In the Basics tab of Create a private endpoint, enter or select basic information for the endpoint.

Step 7: Select Next: Resource.

Step 8: In the Resource pane, enter or select basic information for the resource.

Step 9: Select Next: Virtual Network.

Step 10: In Virtual Network, enter or select:

\* Virtual network: VNET1.

Step 11: Select Next: DNS.

Step 12: Leave the defaults in DNS. Select Next: Tags, then Next: Review + create.

Step 13: Select Create.

Back in the setting of settings of the Storage Account.

Step 14: Save.

Reference:

<https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal>

<https://learn.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal>

✉️  **Bbb78**  4 months, 2 weeks ago

This seems incorrect - the question only asks to accept connections only from VNET1 hosts!

This can be done with the Storage Network/Firewall settings.

upvoted 18 times

✉️  **wooyourdaddy** 3 months, 1 week ago

Agree, this one seems easier to do with Service Endpoints rather than Private Endpoints. Change Public network access on the storage account to 'Enabled from selected virtual networks and IP addresses'. Under Virtual Networks, choose VNET1 and its subnets.

On the subnets in VNET1, edit and add the Microsoft.Storage service under Service Endpoints.

upvoted 4 times

✉️  **Ws1234** 1 month, 3 weeks ago

You'd have to add every new subnet of VNET1 to the 'selected virtual networks' manually. When using a private endpoint, all subnets in the VNET automatically have access. Both will work, Private endpoint seems like the better option to me.

upvoted 3 times

✉️  **Aziza\_Adam**  3 months, 4 weeks ago

Private endpoint is correct as it ensures that there is no connection except to the linked vnet

upvoted 4 times

✉️  **barte** 3 months, 3 weeks ago

you also have to remember to disable public access for storage  
upvoted 3 times

**HOTSPOT**

You have two Azure subscriptions named Subscription1 and Subscription2.

There are no connections between the virtual networks in the two subscriptions.

You configure a private link service as shown in the privatelinkservice1 exhibit. (Click the privatelinkservice1 tab.)

**privatelinkservice1** ...

**Essentials**

Resource group ( <a href="#">move</a> )	: rg1	Alias	: privatelinkservice1.955063e0-3b92-468a-a054-22c729f62297.eastus2.azure.privatelinkservice
Status	: Succeeded	NAT subnet	: vnet2/subnet1
Location	: East US 2	NAT IPs	: 10.3.0.7
Subscription ( <a href="#">move</a> )	: subscription1	Load balancer	: lb1
Subscription ID	: c40e35e3-7605-4f12-ba4c-90d200425073	Visibility	: All
Tags ( <a href="#">edit</a> )	: <a href="#">Click here to add tags</a>		

You create a load balancer name in Subscription1 and configure the backend pool shown in the lb1 exhibit. (Click the lb1 tab.)

**lb1** ...

**Overview**

**Essentials**

Resource group ( <a href="#">move</a> )	: rg1	Backend pool	: backendpool1 (1 virtual machine)
Location	: East US 2	Loading balancing rule	: rule1 (Tcp/80)
Subscription ( <a href="#">move</a> )	: subscription1	Health probe	: probe1 (Http:80)
Subscription ID	: c40e35e3-7605-4f12-ba4c-90d200425073	NAT rules	: 0 inbound
SKU	: Standard	Tier	: Regional
Tags ( <a href="#">edit</a> )	: <a href="#">Click here to add tags</a>	Private IP address	: 10.3.0.6
<a href="#">See less</a>			

You create a private endpoint in Subscription2 as shown in the privateendpoint4 exhibit. (Click the privateendpoint4 tab.)

**Private Link Center**

**Private endpoints**

Name	Private IP	Resource	Subnet	Connection State
privateendpoint4	10.5.0.7	privatelinkservice1.955063e0-3b92-468a-a054-22c729f62297.eastus2.azure.privatelinkservice	vnet5/subnet1	Pending

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
	The resources that will be accessed by using privatelinkservice1 must be added to backendpool1 on LB1.	<input type="radio"/>	<input type="radio"/>
	Users in Subscription2 can connect to the resources published by privatelinkservice1 by using IP address 10.3.0.7.	<input type="radio"/>	<input type="radio"/>
	The private endpoint must be approved by an administrator in Subscription1.	<input type="radio"/>	<input type="radio"/>

Answer Area	Statements	Yes	No
	The resources that will be accessed by using privatelinkservice1 must be added to backendpool1 on LB1.	<input checked="" type="checkbox"/>	<input type="radio"/>
Correct Answer:	Users in Subscription2 can connect to the resources published by privatelinkservice1 by using IP address 10.3.0.7.	<input type="radio"/>	<input checked="" type="checkbox"/>
	The private endpoint must be approved by an administrator in Subscription1.	<input checked="" type="checkbox"/>	<input type="radio"/>

 **occupatissimo** 1 month, 1 week ago  
NNY, backendpool already have a VM in  
upvoted 1 times

 **Apptech** 1 month, 1 week ago  
we do not know if VM hosts the resources that should be access. For that reason we can state: Yes, generally speaking, we must add resources to the load balancer  
upvoted 1 times

 **\_fvt** 2 months, 2 weeks ago  
Y.N.Y, seems good.  
<https://learn.microsoft.com/en-us/azure/private-link/create-private-link-service-portal>  
<https://learn.microsoft.com/en-us/azure/private-link/private-link-overview>  
upvoted 4 times

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: B**

✉ **Ben\_88** 1 week ago

**Selected Answer: A**

if you follow this procedure

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

upvoted 1 times

✉ **AppTech** 1 month, 1 week ago

In my opinion it should be a private endpoint. See here: <https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/how-to-enable-private-link-web-app#approve-azure-front-door-premium-private-endpoint-connection-from-app-service>

upvoted 2 times

✉ **khksoma** 1 month, 1 week ago

It should be A

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

upvoted 2 times

✉ **AppTech** 1 month, 1 week ago

If you follow your own link under headline access restrictions you also can find a link that states that a private endpoint is needed:

<https://learn.microsoft.com/de-de/azure/app-service/networking-features#access-restrictions>

upvoted 2 times

✉ **occupatissimo** 1 month, 1 week ago

A, access comes from internet

<https://learn.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions?tabs=azurecli>

upvoted 2 times

**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 <b>Vault access policy</b>
KeyVault2	Azure Key Vault	Key vault with Permission model set to <b>Azure role-based access control</b>

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:

Store the certificate in:

**Answer Area****Correct Answer:**

DNS record type:

Store the certificate in:

 **crypto700** Highly Voted 1 month, 2 weeks ago

The Right answers are:

1-CNAME

2- Key Vault 1

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

Key Vault access policy permission model.

upvoted 7 times

 **jonav94** Highly Voted 1 month, 2 weeks ago

I disagree with proposed answers, they must be:

DNS: CNAME (When you added a custom domain to your Front Door's frontend hosts, you created a CNAME record in the DNS table of your domain registrar to map it to your Front Door's default .azuredfd.net hostname)

Store certificate in: KeyVault1 (Your key vault must be configured to use the Key Vault access policy permission model.)

There you have a link with all explained <https://learn.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https>.

upvoted 7 times

Question #20

Topic 5

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**

 **Apptech** 1 month, 1 week ago

True, in the health probe settings you can configure the interval of health probe. The amount of time (in seconds) between consecutive health check attempts to the virtual machines

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

upvoted 3 times

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the following subnets:

- AzureFirewallSubnet
- GatewaySubnet
- Subnet1
- Subnet2
- Subnet3

Subnet2 has a delegation to the Microsoft.Web/serverfarms service.

The subscription contains the resources shown in the following table.

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

You need to implement an Azure application gateway named AG1 that will be integrated with an Azure Web Application Firewall (WAF). AG1 will be used to publish VMSS1.

To which subnet should you connect AG1?

- A. GatewaySubnet
- B. AzureFirewallSubnet
- C. Subnet2
- D. Subnet1
- E. Subnet3

**Correct Answer: E**

✉  **khksoma** 1 month, 1 week ago

An application gateway is a dedicated deployment in your virtual network. Within your virtual network, a dedicated subnet is required for the application gateway. You can have multiple instances of a given application gateway deployment in a subnet. You can also deploy other application gateways in the subnet. But you can't deploy any other resource in the application gateway subnet.

Subnet 3

upvoted 3 times

✉  **crypto700** 1 month, 2 weeks ago

what about Subnet2?

upvoted 1 times

✉  **JackCoole95** 1 month, 1 week ago

Because Subnet2 is delegated to Microsoft.Web/serverfarms and therefore is not eligible to deploy an AppGW in to.

upvoted 3 times

✉  **jonav94** 1 month, 2 weeks ago

**Selected Answer: E**

It's ok, it cannot use the others subnets because they've already have another services deployed on them.

upvoted 3 times

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	<i>None</i>

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**

 **tfkfk** 3 weeks, 1 day ago

**Selected Answer: B**

provided answer is correct !

a dedicated subnet is required for the application gateway. You can have multiple instances of a given application gateway deployment in a subnet. You can also deploy other application gateways in the subnet. But you can't deploy any other resource in the application gateway subnet. You can't mix v1 and v2 Azure Application Gateway SKUs on the same subnet.

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

upvoted 2 times

 **jonav94** 1 month, 2 weeks ago

**Selected Answer: B**

Subnet2 is the only one that doesn't have any resources and it is not a gateway subnet.

upvoted 2 times

**HOTSPOT**

You have an Azure subscription that contains multiple virtual machine scale sets and multiple Azure load balancers. The load balancers balance traffic across the scale sets.

You plan to deploy Azure Front Door to load balance traffic across the load balancers.

You need to identify which Front Door SKU to configure, and what to use to route the traffic to the load balancers. The solution must minimize costs.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

SKU:

Classic  
 Premium  
 Standard

Use:

Azure Private Link  
 Azure Route Server  
 A service endpoint

**Answer Area**

Correct Answer:

SKU:

Classic  
 Premium  
 Standard

Use:

Azure Private Link  
 Azure Route Server  
 A service endpoint

  **Apptech** 1 month, 1 week ago

Premium SKU is the only tier which includes private link. <https://learn.microsoft.com/en-us/azure/frontdoor/standard-premium/tier-comparison>  
upvoted 3 times

  **khksoma** 1 month, 1 week ago

Not sure if the question is framed right. Found this in the FAQ.  
Azure Front Door Standard, Premium and (classic) tier requires a public IP or publicly resolvable DNS name to route traffic to backend resources. Azure resources such as Application Gateways or Azure Load Balancers can enable routing to resources within a virtual network. If you're using a Front Door Premium tier, you can enable Private Link to connect to origins behind an internal load balancer over a private endpoint.  
upvoted 3 times

You have an Azure subscription that contains the following resources:

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

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

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

What should you do?

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

**Correct Answer: C**

 **Annie1210** 1 month, 2 weeks ago

Repeated  
upvoted 2 times

**Introductory Info**

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 -

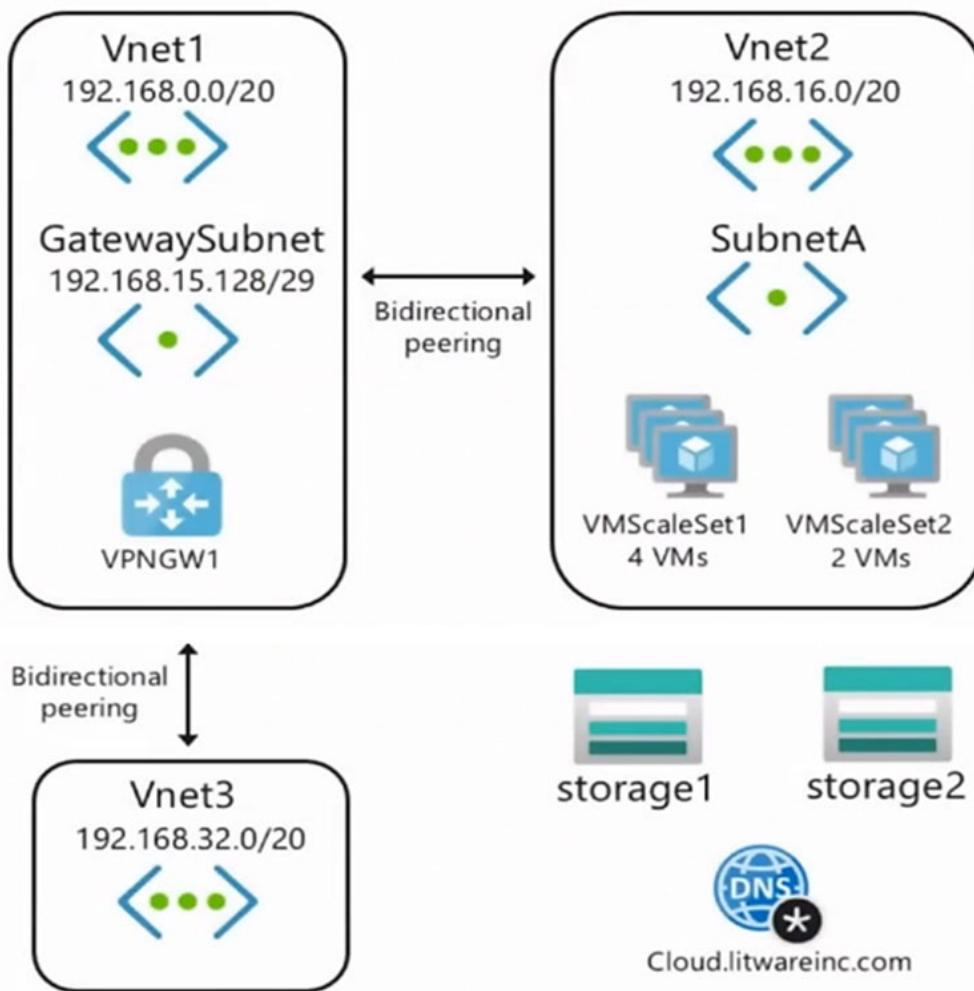
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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 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.

### Question

HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Set the ExpressRoute gateway type to:

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

To minimize latency of traffic to Vnet2:

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

### Correct Answer:

### Answer Area

Set the ExpressRoute gateway type to:

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

To minimize latency of traffic to Vnet2:

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

 **JennyHuang36**  3 months, 3 weeks ago

In exam Feb, 2023

upvoted 5 times

 **alfonzo47**  5 months ago

Correct answers are:

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

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

upvoted 4 times

 **GohanF2** 7 months, 1 week ago

This is a tricky question on regard of the second option. It's true that FastPath now can send traffic directly to the VM including the peered networks. But , this is talking about if we have only in place express route Direct. For the other options express route, it's not available yet and still it on public review. The case study says that they want to minimize costs..so having an express route direct circuit is not the best idea. However, by adding express route Ultra performance gateway , we can say that we can afford express route direct .. . cheapest solution would be to add the vm2 traffic directly through the express route circuit... But , once again it's tricky... I will take the Risk and select the option of enabling gateway transit .

upvoted 3 times

 **GohanF2** 7 months, 1 week ago

Here is the updated link of fastpath new availability just in case u guys don't have it : <https://learn.microsoft.com/en-us/azure/expressroute/about-fastpath>

upvoted 3 times

 **Prutser2** 8 months, 1 week ago

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

so in box 2: peering with transit gateway, leveriging off the fastpath feature in vnet1

upvoted 2 times

✉ **sapien45** 8 months, 3 weeks ago

FastPath now supports virtual network peering . FastPath will send traffic directly to any VM deployed in a spoke virtual network peered to the virtual network where the ExpressRoute virtual network gateway is deployed.

<https://azure.microsoft.com/en-ca/updates/general-availability-expressroute-fastpath-support-for-virtual-network-vnet-peering-and-user-defined-routes-udrs-2/>

upvoted 2 times

✉ **A\_A\_AB** 8 months, 3 weeks ago

First answer is correct as FastPath only works with Ultra Performance SKU.

The second answe must be the dedicated ER:

If you have other virtual networks peered with the one that is connected to ExpressRoute, the network traffic from your on-premises network to the other virtual networks (i.e., the so-called "Spoke" VNets) will continue to be sent to the virtual network gateway. The workaround is to connect all the virtual networks to the ExpressRoute circuit directly.

upvoted 1 times

✉ **wwwww** 8 months, 4 weeks ago

FastPath doesn't work for peered VNets, thus Vnet2 needs a direct connection to the ExpressRoute as well. The data can still flow through Vnet1: Vnet 2 > ExpressRoute > Vnet 1 -> ExpressRoute > ...

upvoted 2 times

✉ **hom3sick** 8 months, 4 weeks ago

I agree:

VNet Peering: If you have other virtual networks peered with the one that is connected to ExpressRoute, the network traffic from your on-premises network to the other virtual networks (i.e., the so-called "Spoke" VNets) will continue to be sent to the virtual network gateway. The workaround is to connect all the virtual networks to the ExpressRoute circuit directly.

upvoted 1 times

✉ **tkcltoh** 9 months ago

but there is a condition that Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

i thinkthe gateway transit in vnet1 is correct.

upvoted 1 times

✉ **ChinkSantana** 5 months, 3 weeks ago

Traffic between VNET2 and 3 and not traffic between VNET2 and On-Prem

upvoted 1 times

✉ **Cristoicach91** 9 months, 3 weeks ago

correct

upvoted 1 times

✉ **Cristoicach91** 9 months, 3 weeks ago

Correcting myself here. Should be Ultra for the first box and the second box since it mentions FastPath it needs to have Vnet2 directly connected to ExpressRoute.

upvoted 6 times

**Introductory Info**

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 -

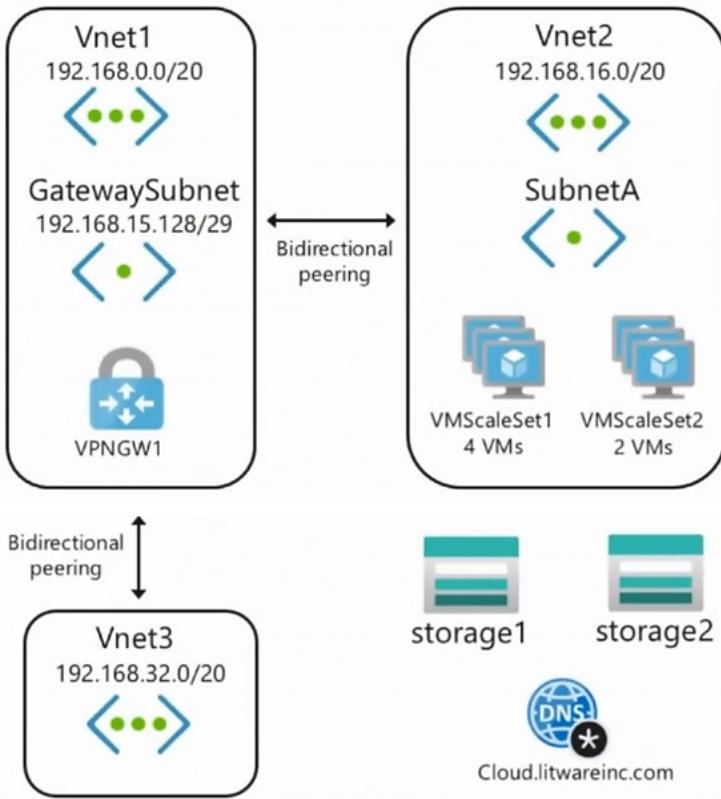
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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	<b>None</b>
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

You need to provide access to storage1. The solution must meet the PaaS networking requirements and the business requirements.

What should you include in the solution?

- A. a private endpoint
- B. Azure Traffic Manager
- C. Azure Front Door
- D. a service endpoint

**Correct Answer: D**

✉  **Cristoicach91** Highly Voted 9 months, 3 weeks ago

**Selected Answer: A**

The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.  
upvoted 19 times

✉  **tkcltoh** Highly Voted 9 months ago

**Selected Answer: A**

service endpoint limitation  
Endpoints are enabled on subnets configured in Azure virtual networks. Endpoints can't be used for traffic from your premises to Azure services  
upvoted 8 times

✉  **JohnnyChimpo** 1 month, 2 weeks ago

NICE! Thanks for this  
upvoted 1 times

✉  **sapien45** 8 months, 3 weeks ago

Good catch Sir  
upvoted 4 times

✉  **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023  
upvoted 2 times

✉  **jtvdw** 2 months, 4 weeks ago

What was your answer in the exam, A or D? I see a lot of people is in favor of A.  
upvoted 2 times

✉  **TJ001** 5 months ago

private endpoint for on-premise access ..  
Correct Answer A  
upvoted 1 times

✉  **chatlisi** 5 months, 2 weeks ago

**Selected Answer: A**

Service Endpoints Limitations:  
"Endpoints can't be used for traffic from your premises to Azure services."  
<https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview#limitations>  
upvoted 1 times

✉  **GohanF2** 7 months, 1 week ago

It's A.  
Service endpoints are used when we want to call data from our Apps in Azure to our on premise services .  
upvoted 3 times

✉  **ragav21** 8 months ago

**Selected Answer: A**

Matches the requirement for private endpoint  
upvoted 1 times

✉  **jellybiscuit** 8 months, 3 weeks ago

**Selected Answer: A**  
Private endpoint fulfills all the requirements and is the current "microsoft way".  
upvoted 2 times

✉  **khanwoo** 8 months, 4 weeks ago

<https://jeffbrown.tech/azure-private-service-endpoint/>  
Answer should be A  
upvoted 1 times

✉  **zenithcsa1** 9 months, 2 weeks ago

**Selected Answer: A**

private endpoint, 100%

upvoted 3 times

✉️👤 **erima21** 9 months, 2 weeks ago

Correct!

- Service endpoints does not remove public endpoint.

- Private endpoints remove public access.

upvoted 7 times

✉️👤 **Azuriste** 9 months, 3 weeks ago

i think is correct

upvoted 3 times

## Introductory Info

### 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 -

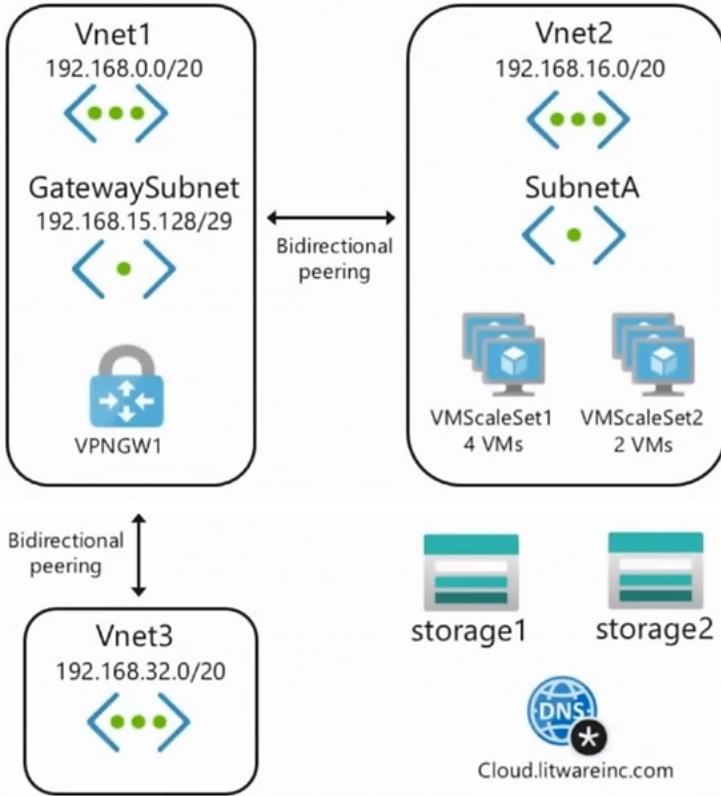
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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	<b>None</b>
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 VMSScaleSet1 to VMSScaleSet2 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

You need to provide access to **storage2**. The solution must meet the PaaS networking requirements and the business requirements.

Which connectivity method should you use?

- A. a private endpoint

- B. Azure Firewall
- C. Azure Front Door
- D. a service endpoint

**Correct Answer: D**

Reference:

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

 **wsrudmen** Highly Voted 1 year ago

**Selected Answer: A**

Azure Service Endpoint provides secure and direct connectivity to Azure PaaS services over an optimized route over the Azure backbone network.

Traffic still left your VNet and hit the public endpoint of PaaS service. ==> Then it can't meet the goal because of the public IP

Azure Private Link (or Private Endpoint) allows you to access Azure PaaS services over Private IP address within the VNet. It's then OK

A is the answer

upvoted 24 times

 **erima21** 9 months, 2 weeks ago

Correct!

- Service endpoints does not remove public endpoint.
- Private endpoints remove public access.

upvoted 7 times

 **jeffangel28** 10 months, 2 weeks ago

Perfectly explained!

upvoted 1 times

 **Payday123** Highly Voted 11 months, 3 weeks ago

**Selected Answer: D**

"Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet."

And it is cheaper

upvoted 11 times

 **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 4 times

 **energie** 4 months ago

**Selected Answer: A**

"Virtual Network (VNet) Service Endpoint provides secure and direct connectivity to (native)Azure services"(NOT the private services provisioned by you).

Private Endpoint brings the private services provisioned by you(like Azure Storage, Azure SQL Database etc.) to the VNet.

upvoted 1 times

 **staffo** 4 months, 2 weeks ago

Both answers are technically correct (As the public ip is already blocked) except when it comes to costs. Service Endpoints are free and private endpoints include additional costs. So to minimise costs use Service Endpoints.

upvoted 3 times

 **TJ001** 5 months ago

Service end point still connect to public IP of the storage account ...The question should have been better phrased to have proper use case for service endpoint..!

upvoted 2 times

 **chatlisi** 5 months, 2 weeks ago

**Selected Answer: D**

Storage 1 can be accessed from on prem via Private Endpoint only (Service Endpoint does not support on prem access)

Storage 2 should be via Service Endpoint since the communication is within Azure only.

upvoted 5 times

 **jellybiscuit** 8 months, 2 weeks ago

**Selected Answer: A**

A - private endpoint

- a service endpoint does not remove the public endpoint. The storage account could be accessed both through the service endpoint and publicly.

I have a hard time imagining that service endpoint is the correct answer to any question that would appear on the test today.  
upvoted 1 times

✉️ **hom3sick** 8 months, 4 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

✉️ **promto** 9 months ago

**Selected Answer: A**

private ip - no public access

upvoted 2 times

✉️ **zenithcsa1** 9 months, 2 weeks ago

**Selected Answer: D**

private / service endpoint both meet the goal, providing private connectivity from specific vNet.

However, private endpoint needs more conditions such as firewall that blocking traffic from on-premises to the private endpoint or NSG for vNet1. More conditions also include more money.

Moreover, public IP address of xxx.blob.core.windows.net is always visible through nslookup even though you disabled public access in Storage-Firewall setting, adding private endpoint or private DNS zone to vNet, etc.

upvoted 1 times

✉️ **zenithcsa1** 6 months, 4 weeks ago

Ignore my answer, just confused what 'exposing the public endpoint' really means. The answer is A - private endpoint.

upvoted 1 times

✉️ **examtaker20398** 11 months ago

**Selected Answer: A**

Service Endpoints expose a Public IP address still

upvoted 2 times

✉️ **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22. There were two separate questions, one about storage1 and one about storage2. Understand the concepts behind both.

upvoted 3 times

✉️ **Fearless90** 11 months, 4 weeks ago

**Selected Answer: A**

A. a private endpoint

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

What is Azure Private Link?

Azure Private Link enables you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network.

Traffic between your virtual network and the service travels the Microsoft backbone network. Exposing your service to the public internet is no longer necessary. You can create your own private link service in your virtual network and deliver it to your customers. Setup and consumption using Azure Private Link is consistent across Azure PaaS, customer-owned, and shared partner services.

upvoted 2 times

✉️ **Fearless90** 11 months, 4 weeks ago

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

Virtual Network service endpoints

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

Note

Microsoft recommends use of Azure Private Link for secure and private access to services hosted on Azure platform. For more information, see Azure Private Link.

upvoted 1 times

✉️ **Fearless90** 11 months, 4 weeks ago

<https://docs.microsoft.com/en-us/azure/private-link/private-link-overview#key-benefits>

Key benefits

Azure Private Link provides the following benefits:

Privately access services on the Azure platform: Connect your virtual network to services in Azure without a public IP address at the source or destination. Service providers can render their services in their own virtual network and consumers can access those services in their local virtual network. The Private Link platform will handle the connectivity between the consumer and services over the Azure backbone network.

upvoted 1 times

✉️ **Fearless90** 11 months, 4 weeks ago

<https://www.techtarget.com/searchcloudcomputing/tip/Compare-Azure-Private-Link-vs-service-endpoints#:~:text=What%20are%20the%20differences%3F,them%20directly%20into%20your%20VNet.>

What are the differences?

The primary difference between these methods to restrict access is that while service endpoints keep PaaS resources outside your VNet, Private Link brings them directly into your VNet.

<https://samcogan.com/service-endpoints-and-private-link-whats-the-difference/>

The key difference between Private Link and Service Endpoints is that with Private Link you are injecting the multi-tenant PaaS resource into your virtual network. With Service Endpoints, traffic still left your vNet and hit the public endpoint of the PaaS resource, with Private Link the PaaS resource sits within your vNet and gets a private IP on your vNet. When you send traffic to the PaaS resource, it does not leave the virtual network.

upvoted 1 times

 **kinder2** 12 months ago

**Selected Answer: A**

Azure Private Link provides the following benefits:

On-premises and peered networks: Access services running in Azure from on-premises over ExpressRoute private peering, VPN tunnels, and peered virtual networks using private endpoints. There's no need to configure ExpressRoute Microsoft peering or traverse the internet to reach the service. Private Link provides a secure way to migrate workloads to Azure.

upvoted 2 times

 **HTD** 1 year, 1 month ago

also need access from onsite ...so private point is right

upvoted 2 times

 **Jorex** 1 year, 1 month ago

That's a requirement for storage1.

upvoted 4 times

 **RVR** 1 year, 1 month ago

Considering they want to meet business requirements as well which says

"Litware wants to minimize costs whenever possible, as long as all other requirements are met" - a service endpoint will be fine

upvoted 6 times

## Introductory Info

### 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 -

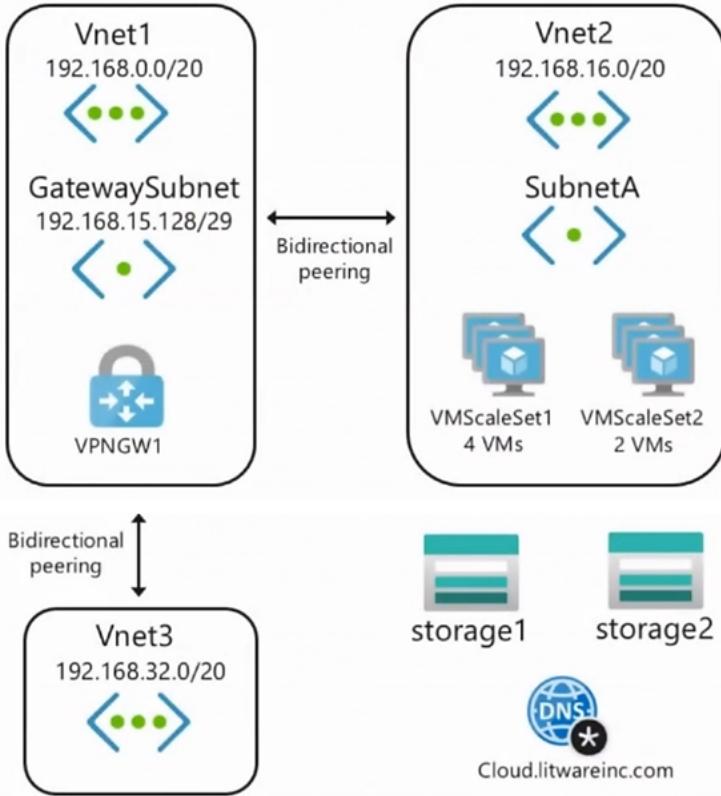
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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	<b>None</b>
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

##### HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

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

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

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

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

Correct Answer:

### Answer Area

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

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

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

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

Reference:

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

✉️  **GhostMan135710** Highly Voted 10 months ago

Congratulations making it to the end!  
upvoted 24 times

✉️  **jellybiscuit** Highly Voted 8 months, 3 weeks ago

- Typically, the test answer to this type of scenario is to build a DNS server. That does work.  
- DNS proxy would also work.

If you already had a firewall, I'd go with the proxy option.  
You don't though, and VMs are cheaper than firewalls.

I'm sticking with:

- virtual network link
- build a DNS server (and the implied forwarder steps that follow)

DNS Proxy

<https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>  
upvoted 7 times

✉️  **mammoot** 4 months ago

And this has all changed since Private DNS Resolver was introduced.. which isn't even in the exam  
<https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-overview>  
upvoted 2 times

✉️  **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023  
upvoted 2 times

✉️  **GohanF2** 7 months, 1 week ago

We cannot use DNS proxy due that there is not a firewall in place in the case, so yeah I will stick with the answer of adding a VM and add the DNS role to that server.

upvoted 3 times

✉️  **sapien45** 8 months, 3 weeks ago

Firewall as a DNS Proxy would have been a great option, if there was a Firewall deployed ...

Second best option, is to deploy a dedicated VM acting as a DNS forwarder, as proposed

upvoted 1 times

✉️  **jeffangel28** 10 months, 2 weeks ago

Create virtual network links -> Right

Deploy azure virtual machine.... -> False because one simplest way to do is using firewall dns proxy (<https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/>)

upvoted 2 times

✉️  **JNishant** 10 months ago

case study as no mention about use of Firewall.

upvoted 7 times

✉️  **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 3 times

✉️  **WickedMJ** 10 months ago

Can you please be more helpful and tell us the answer instead?

upvoted 3 times

✉️  **Aunehwet79** 5 months, 3 weeks ago

Personally, I do find it helpful to know if it turns up in the exam. Don't expect answers to be given. Use these to test your knowledge

upvoted 2 times

**Introductory Info**

Case Study -

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

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

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

To start the case study -

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

Overview -

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

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

Existing Environment -

Azure Network Infrastructure -

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

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

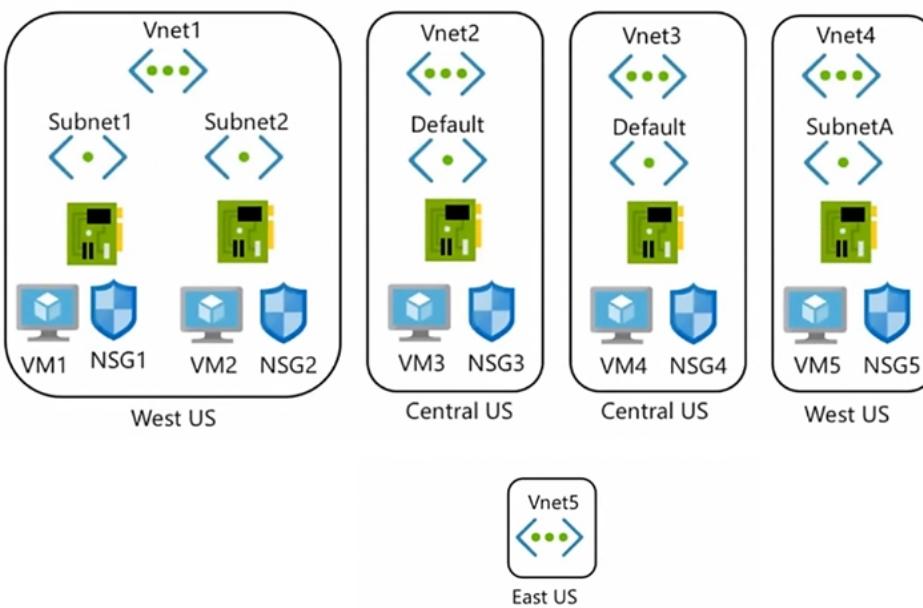
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	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

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

Reference:

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

✉  **wsrudmen** Highly Voted 1 year ago

Azure AD authentication is supported for OpenVPN® protocol connections only and requires the Azure VPN Client.

And also SSTP and IKEv2 don't support all client devices:  
 SSTP limited to Windows  
 IKEv2 limited to Mac devices  
 upvoted 20 times

✉  **derrp** Highly Voted 11 months ago

mnemonic device:  
 If you try to read this very long case study during the exam, you're going to run out of time and open up a can of worms.  
 open.  
 openVPN.  
 upvoted 14 times

✉  **Prutser2** Most Recent 8 months, 1 week ago

Selected Answer: D

openVPN, has been asked many times before  
 upvoted 1 times

✉  **jellybiscuit** 8 months, 3 weeks ago

Selected Answer: D

P2S + AD authentication = OpenVPN

Recurring question in multiple tests.  
<https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#authenticate-using-native-azure-active-directory-authentication>  
 upvoted 1 times

**Introductory Info**

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 -

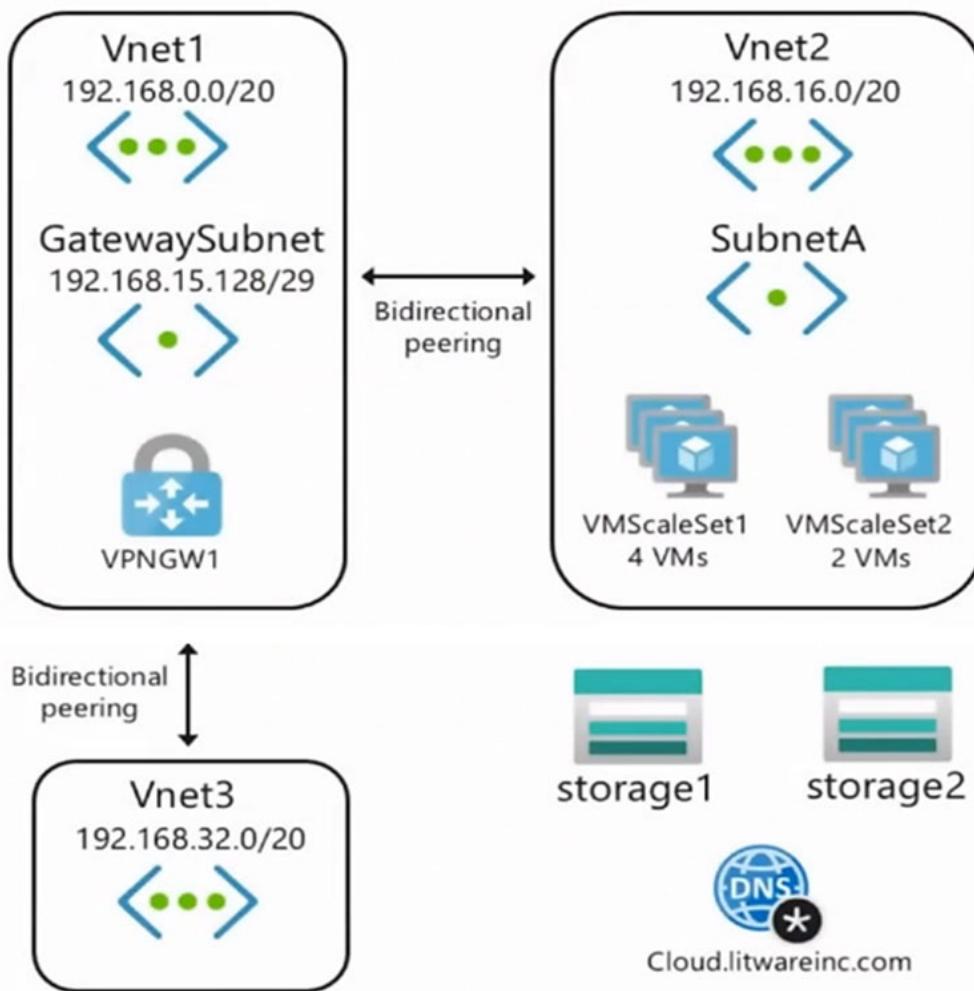
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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 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.

### Question

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.	

Correct 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.	

Step 1: Delete the VPN GW1.

The existing VPN GW1 GatewaySubnet is too small with /29.

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.

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

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

Step 2: Create a VPN gateway by using Basic SKU.

Basic SKU is good enough.

Note -

The Basic gateway SKU does not support IKEv2 or RADIUS authentication. If you plan on having Mac clients connect to your virtual network, do not use the Basic SKU.

Step 3: Set the subnet mask of Gateway Subnet to /27.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed

depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We [Microsoft] recommend that you create a gateway subnet that uses a /27 or /28.

It's best to specify /27 or larger (/26,/25 etc.). This allows enough IP addresses for future changes, such as adding an ExpressRoute gateway.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

✉  **zenithcsa1** Highly Voted 9 months, 1 week ago

1. Delete VPN GW1.
2. Set the subnet mask of Gateway Subnet to /27.
3. Create a VPN gateway by using the VPN GW1 SKU.

Basic VPN Gateway does not support P2S.

If the gateway subnet is /29, you've to first delete the virtual network gateway and increase the gateway subnet size.

<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>

upvoted 20 times

✉  **hom3sick** 8 months, 3 weeks ago

I agree, but basic VPN gateway does support P2S (SSTP Connections) but not P2S IKEv2/OpenVPN Connections. And openVPN is needed for AzureAD.

So basic can't be used here

upvoted 3 times

✉  **Alessandro365** Highly Voted 8 months, 3 weeks ago

1. Delete VPN GW1.
2. Set the subnet mask of Gateway Subnet to /27.
3. Create a VPN gateway by using the VPN GW1 SKU.

<https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal>

"To configure coexisting connections for an already existing VNet:

- 1- Delete the existing ExpressRoute or Site-to-site VPN gateway.
- 2 - Delete and recreate the GatewaySubnet to have prefix of /27 or shorter.
- 3- Configure a VNet with a Site-to-Site connection and then Configure the ExpressRoute gateway.
- 4 - Once the ExpressRoute gateway is deployed, you can link the virtual network to the ExpressRoute circuit."

upvoted 10 times

✉  **Prutser2** 8 months, 1 week ago

also to reaffirm VPN gateway type:

ExpressRoute-VPN Gateway coexist configurations are not supported on the Basic SKU.

as per <https://learn.microsoft.com/en-us/azure/expressroute/how-to-configure-coexisting-gateway-portal> s. so concur

upvoted 1 times

✉  **Apptech** Most Recent 2 months, 3 weeks ago

About the Gateway Subnet:

"When you're planning your gateway subnet size, refer to the documentation for the configuration that you're planning to create. For example, the ExpressRoute/VPN Gateway coexist configuration requires a larger gateway subnet than most other configurations. Further more, you may want to make sure your gateway subnet contains enough IP addresses to accommodate possible future configurations. While you can create a gateway subnet as small as /29, we recommend that you create a gateway subnet of /27 or larger (/27, /26 etc.). If you plan on connecting 16 ExpressRoute circuits to your gateway, you must create a gateway subnet of /26 or larger. If you're creating a dual stack gateway subnet, we recommend that you also use an IPv6 range of /64 or larger. This set up will accommodate most configurations."

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

upvoted 1 times

✉  **sellamibassem** 3 months, 1 week ago

Sorry. VPN GW basic sku should not work as we have Azure AD authentication

upvoted 1 times

✉  **sellamibassem** 3 months, 1 week ago

VPN GW Basic sku is enough as we have only 10 devices.

upvoted 1 times

✉  **JennyHuang36** 3 months, 3 weeks ago

In exam Feb 2023

upvoted 1 times

✉  **magikmarcus** 4 months, 2 weeks ago

Also as they need to auth on the VPN PS2 with Azure AD. It needs to be OpenVPN  
OpenVPN is not supported on basic SKU

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

upvoted 1 times

✉️ **jellybiscuit** 8 months, 3 weeks ago

Once you realize you need to resize the subnet, the first two should be obvious.

- 1) delete gw
- 2) set subnet mask

3) I personally went with the "what's there is probably fine" assumption, but as others have pointed out, Basic would not work.

Sometimes you get lucky.

upvoted 4 times

✉️ **smosmo** 9 months, 2 weeks ago

Following this documentation Basic Gateway is not enough for P2S Connection, but there is no other option to choose. Any comments/ideas? Should we create based on the VPN GW 1 SKU instead?

upvoted 1 times

✉️ **tdienst** 9 months, 2 weeks ago

1. Delete GW1
2. Create VPN GW with GW1 SKU
3. Edit subnet mask to /27

ExpressRoute-VPN Gateway coexist configurations are not supported on the Basic SKU.

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

although i feel that 2-3 are interchangable.

upvoted 5 times

✉️ **Cristoicach91** 9 months, 3 weeks ago

You need to prepare Vnet1 for the deployment of an ExpressRoute gateway.

You need to have a standard SKU VPN gate for express route p2s and s2s.

upvoted 4 times

## Introductory Info

### 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 -

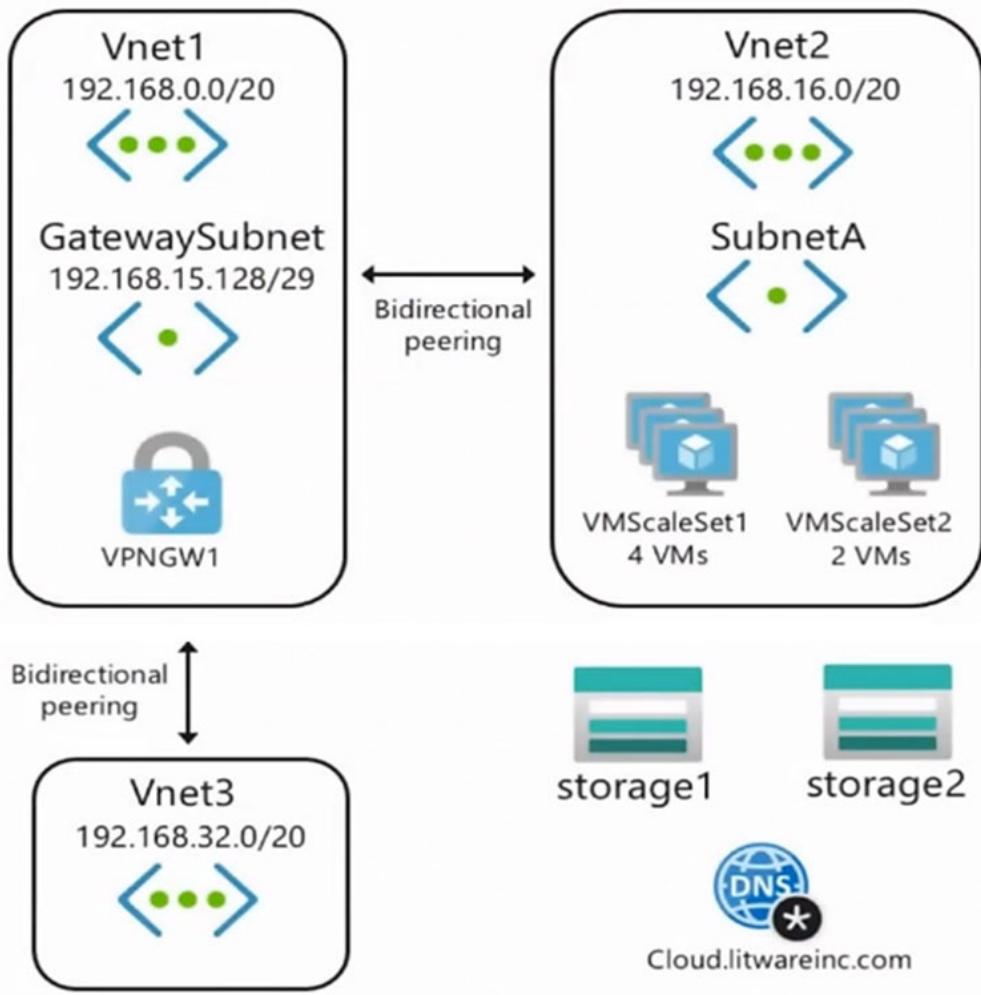
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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	<b>None</b>
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.

## Question

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.

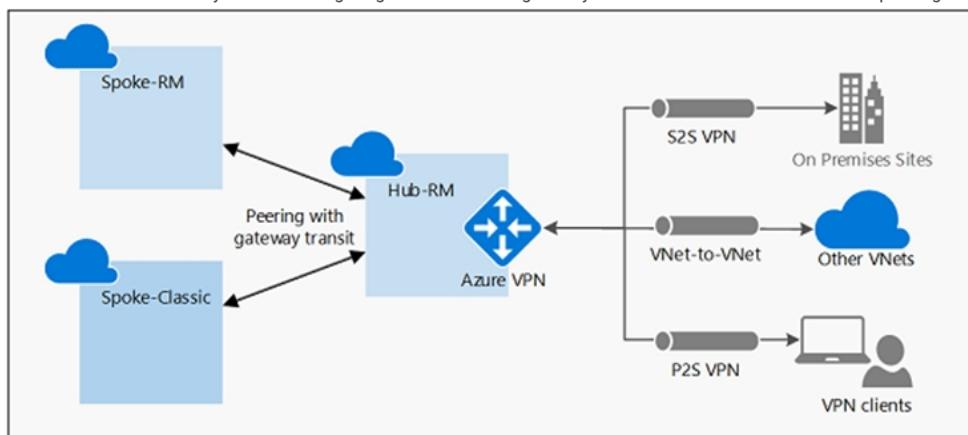
NOTE: Each correct selection is worth one point.

- A. On the peering from Vnet1, select Allow gateway transit.
- B. On the peerings from Vnet2 and Vnet3, select Use remote gateways.
- C. On the peerings from Vnet2 and Vnet3, select Allow gateway transit.
- D. On the peering from Vnet1, select Use remote gateways.
- E. On the peering from Vnet1, select Allow forwarded traffic.

### Correct Answer: AB

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

Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity. The following diagram shows how gateway transit works with virtual network peering.



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

Reference:

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

✉️ **Zika69** 3 days, 22 hours ago

**Selected Answer: BE**

You cannot select Gateway transit on peering on vnet1 - only allow traffic forwarded from remote virtual network  
upvoted 1 times

✉️ **JennyHuang36** 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 3 times

✉️ **TJ001** 5 months ago

AB correct however from peering perspective .. There is no mention of FW/RouteServer/NVA in the Vnet 1...so assume the VNET2 and VNET3 will learn the route from the GW

upvoted 1 times

✉️ **alkorkin** 5 months ago

There's no option "gateway transit." in the peering configuration.

Three's only "traffic forwarded from remote virtual network"

upvoted 2 times

✉️ **alkorkin** 5 months ago

We can use "AllowGatewayTransit" in PowerShell command for peering configuration

upvoted 2 times

✉️ **vivikar** 5 months, 3 weeks ago

The sentence should be modified without creating confusion

upvoted 1 times

✉️ **Prutser2** 8 months, 1 week ago

**Selected Answer: AB**

vnets 2 and 3 need to peer with vnet1.  
upvoted 3 times

 **Alessandro365** 8 months, 2 weeks ago

**Selected Answer: AB**

A and B are the correct answer  
upvoted 2 times

 **sapien45** 8 months, 3 weeks ago

**Selected Answer: DE**

There is no such thing as gateway transit option in VPC peering  
gateway transit is the feature  
upvoted 1 times

 **MariusKas** 8 months, 2 weeks ago

VPC is in GCP cloud  
upvoted 2 times

 **abdx** 3 months ago

AWS as well  
upvoted 1 times

## Introductory Info

### 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 -

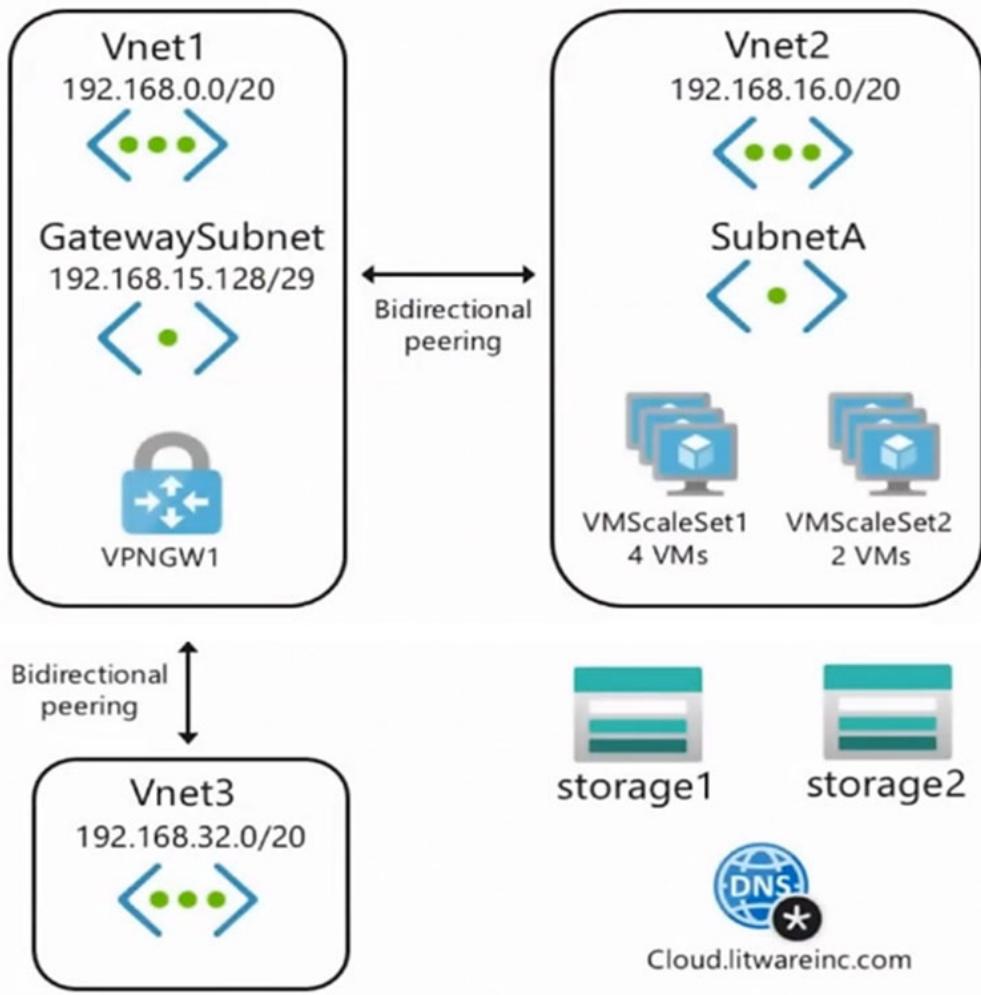
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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	<b>None</b>
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.

## Question

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.

Hot 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

Correct 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

Reference:

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

✉ **wsrudmen** Highly Voted 1 year ago

Correct

OpenVPN because there's many device type (Users have Android, iOS, and Windows 10 devices). It's the only one configuration suitable for this.

To enable Azure AD authentication on the VPN Gateway, as Global admin you have to give consent to Azure VPN (listed as an Enterprise application)

upvoted 16 times

✉ **Prutser2** Highly Voted 8 months, 1 week ago

the way i do these exhibit questions, that usually contain a multitude of information (some of which is useless), is to go straight to the question. sometime the question does not require you to read all the exhibit info, but if it doesn't, then based on the question you can filter out the relevant exhibit info, this will save you time!

upvoted 9 times

✉ **JennyHuang36** Most Recent 3 months, 3 weeks ago

In exam Feb, 2023

upvoted 2 times

✉ **Prutser2** 8 months, 1 week ago

correct

upvoted 1 times

✉ **hogs** 10 months ago

Appeared on exam Aug2022

upvoted 1 times

✉ **derrp** 11 months ago

From the Microsoft Support Documentation:

"Sign in to the Azure portal as a user that is assigned the Global administrator role. Next, grant admin consent for your organization. This allows the Azure VPN application to sign in and read user profiles."

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

upvoted 1 times

 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 1 times

**Introductory Info**

Case Study -

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

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

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

To start the case study -

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

Overview -

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

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

Existing Environment -

Azure Network Infrastructure -

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

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

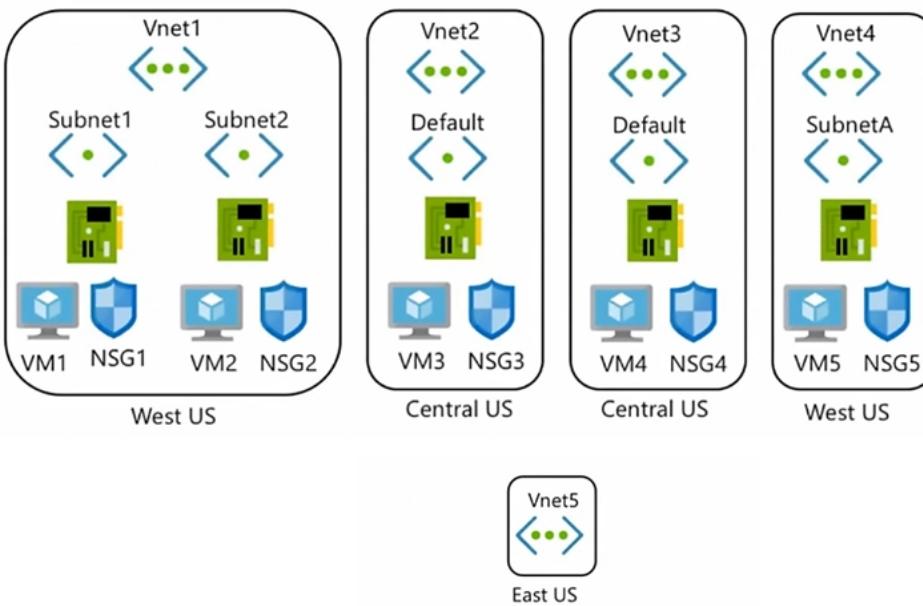
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

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

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"/>

Correct 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"/>

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.

✉  **derrp** Highly Voted 11 months ago

No:

Zone 2 is not linked to any VNets therefor no VMs can resolve names in Zone 2.

Yes:

VM4 is in VNET3 which has autoregistration enabled with a Link to Zone 1

No:

VNETs can only be linked to one Zone. VNET3 is already linked to Zone 1.

All answers can be interpreted by analysis of the above information without any surprises.

upvoted 22 times

✉  **Madball** 4 months, 2 weeks ago

You can have two private DNS zones linked to the same vnet, however only 1 private DNS zone can have auto-registration enabled, this is why the final question is no.

upvoted 4 times

✉  **Prutser2** 8 months, 1 week ago

zone 2 is not explicitly "not linked", so therefore assuming it is not linked at all.

they way these questions are written up popen for suggestions/assumptions, is just mind baffling

upvoted 2 times

✉  **Dimetrodon** 8 months, 1 week ago

To clarify point 3, yes you are right about a VNET can be linked to only 1 zone. However this is if the zone is set to auto-registration. ie. Registration virtual network

If the vnet is linked to a private DNS zone and has auto registration turned off i.e. A Resolution virtual network, then the vnet can have multiple virtual network links from that vnet, however only one of those links can be a Registration virtual network. i.e. - set for auto registration.

upvoted 2 times

✉  **wsrudmen** Highly Voted 1 year ago

CORRECT

upvoted 5 times

✉  **TJ001** Most Recent 5 months ago

Correct No Yes No

upvoted 2 times

### Introductory Info

Case Study -

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

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

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

To start the case study -

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

Overview -

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

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

Existing Environment -

Azure Network Infrastructure -

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

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

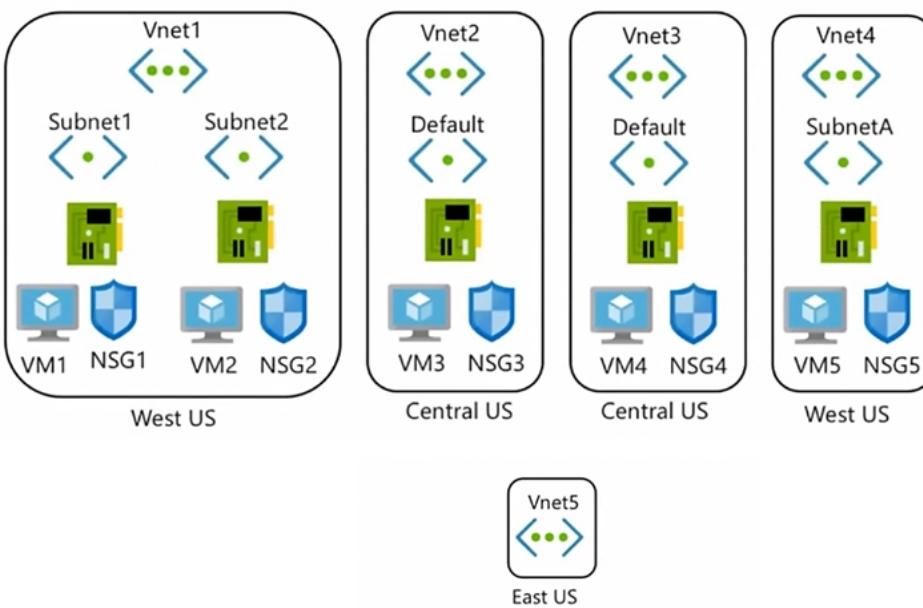
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	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

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 Area

VM1:

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

Correct Answer:

VM4:

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

Box 1: VM2, VM3 and VM4.

VM1 is in VNet1/Subnet1. VNet1 is peered with VNet2 and VNet3.

There are no NSGs blocking outbound ICMP from VNet1. There are no NSGs blocking inbound ICMP to VNet1/Subnet2, VNet2 or VNet3.

Therefore, VM1 can ping VM2 in VNet1/Subnet2, VM3 in VNet2 and VM4 in VNet3.

Box 2:

VM4 is in VNet3. VNet3 is peered with VNet1 and VNet2. There are no NSGs blocking outbound ICMP from VNet3. There are no NSGs blocking inbound ICMP to VNet1/Subnet1, VNet1/Subnet2 or VNet2 from VNet3 (NSG10 blocks inbound ICMP from VNet4 but not from VNet3).

Therefore, VM4 can ping VM1 in VNet1

Subnet1, VM2 in VNet1/Subnet2 and VM3 in VNet2.

✉  **derrrp** Highly Voted  11 months ago

Been cramming on this one all week. Reviewed this question so many times now, it's muscle memory: The sequence is 234 then 123

Write that sequence down several times on your keyboard and you'll never forget it:

234123 234123 234123

Hope this helps!

upvoted 14 times

✉  **Ayokun** 3 months, 3 weeks ago

I think just excluding VM5 is simpler lol

upvoted 5 times

✉  **Aunehwet79** 5 months, 3 weeks ago

Thanks this does help

upvoted 1 times

✉  **Ajdifasudfo0** 6 months, 2 weeks ago

big IQ brain that tries to just remember it

upvoted 1 times

✉  **wooyourdaddy** 10 months ago

Nice memory association tip ;-)

upvoted 1 times

✉  **ejml** Most Recent  4 months, 3 weeks ago

There is a peering between VN2 and VN5, why is not reachable VM4 from VM1 and VM4?

upvoted 1 times

✉  **MrBlueSky** 2 months ago

There is not a peering between Vnet2 and Vnet5.

upvoted 2 times

✉  **dsmurray88** 4 months, 3 weeks ago

Default NSG rule allows all ports inbound and outbound for the VirtualNetwork service tag. This encompasses any peered networks  
The VM Firewalls allow ICMP

So any VMs in peered VNets can ping

The answer is 1234 (1 > 2,3,4) (4 > 1,2,3)

upvoted 1 times

✉  **TJ001** 5 months ago

correct answer

upvoted 1 times

✉  **TJ001** 5 months ago

It is not hard ...only two things to be checked ...

1) Is there a peering in place ?

2) Is there a NSG rule blocking ?

Do that is order and we are good with the answers

upvoted 1 times

✉  **DeepMoon** 5 months, 1 week ago

Default Inbound or Outbound rule doesn't allow ICMP.

VM1 can only ping VM2. Default rule for inside vnet will allow it.

VM4 cannot ping anything. Default Outbound rule will block it.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#default-security-rules>

upvoted 1 times

✉  **Anandan** 8 months, 2 weeks ago

They ask from which VM's can ping VM1 and VM4 successfully... We can ping VM1 from VM2,VM3,VM4 and VM4 from VM1,VM2,VM3...

Because

NSG Inbound rule deny the RDP port from 10.1.x.x to any destination...

NSG Inbound rule deny the ICMP from 10.10.x.x to any destination

10.0.0.0/16 is Vnet4 address space..so VM5 only is available in this Vnet..

NSG outbound rule deny the RDP port from 10.1.x.x to any destination...

By default outbound rule for any to any virtual network is enabled..  
Already peering is enabled between Vnet1,vnet2,vnet3... obviously ping will happen successfully...  
Please correct me if anything wrong in my understanding

upvoted 1 times

 **GeorgeMilev91** 4 months, 4 weeks ago

no mate, they are not asking this, please read the question again, they are asking from vm1 and vm4 which hosts you can ping i.e. vm1, vm4 -> vm2 and etc, not vice-versa..

upvoted 1 times

 **lobswort** 11 months ago

Answer is correct, appeared in exam 22-July-2022.

upvoted 2 times

## Introductory Info

### Case Study -

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

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

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

### To start the case study -

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

### Overview -

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

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

### Existing Environment -

#### Azure Network Infrastructure -

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

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

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

Vnet1 contains a virtual network gateway named GW1.

#### Azure Virtual Machines -

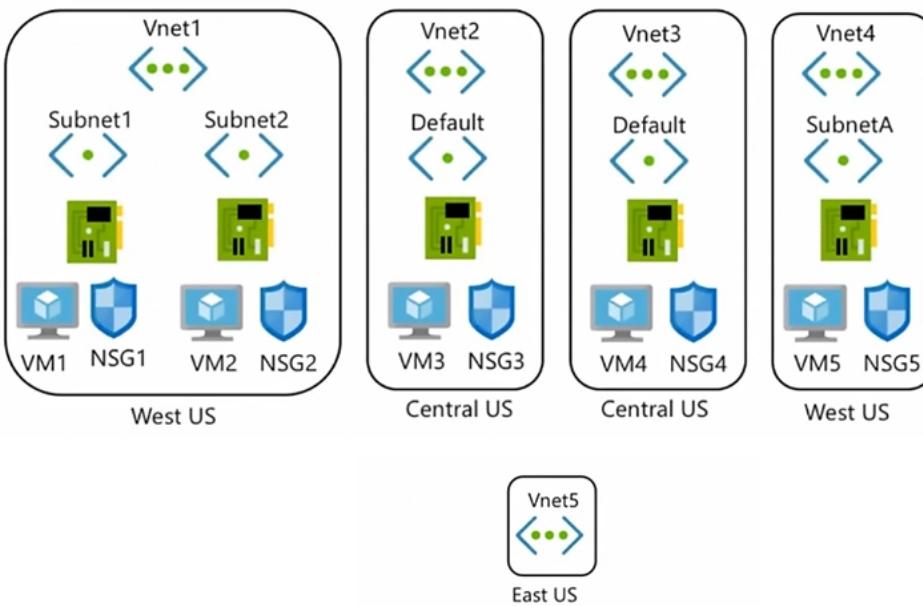
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	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

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

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.

 **letteris\_k** 3 months, 2 weeks ago

**Selected Answer: E**

Vnet Peering with no doubt

upvoted 2 times

 **omgMerrick** 3 months, 3 weeks ago

**Selected Answer: E**

Answer is correct: E. virtual network peering

Virtual network peering connects two Azure virtual networks. Once peered, the virtual networks appear as one for connectivity purposes. Traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, through private IP addresses only. No public internet is involved.

Source:

<https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vnet-peering#virtual-network-connection-types>

upvoted 1 times

 **Prutser2** 8 months, 1 week ago

**Selected Answer: E**

correct

upvoted 1 times

 **GhostMan135710** 10 months ago

**Selected Answer: E**

Correct

upvoted 2 times

**Introductory Info**

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 -

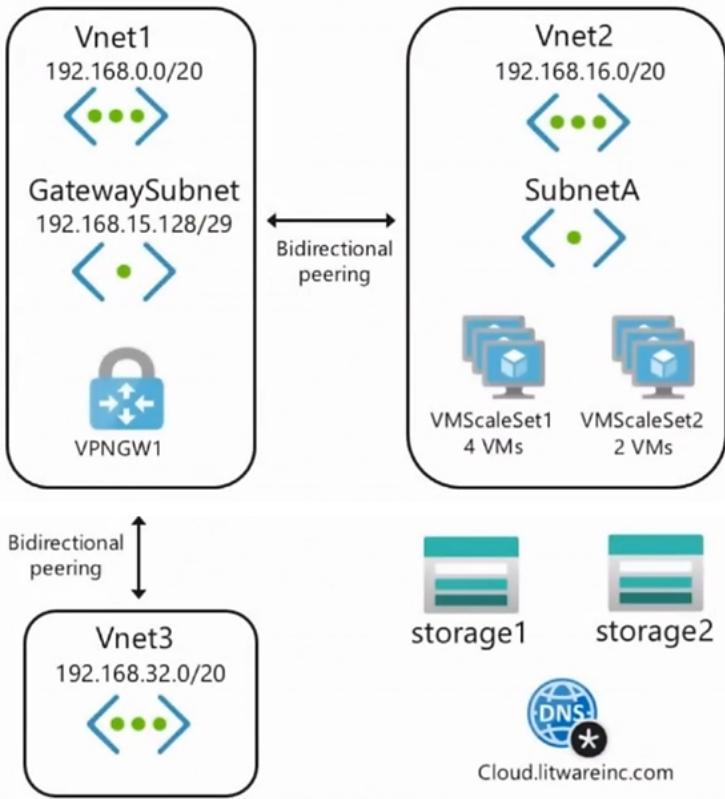
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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.

### Question

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

What should you use to configure the default route?

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

**Correct Answer: B**

Reference:

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

✉️  **Fearless90** Highly Voted 11 months, 4 weeks ago

**Selected Answer: B**

B. BGP route exchange

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.

upvoted 11 times

✉️  **Fearless90** 11 months, 4 weeks ago

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#border-gateway-protocol>  
Border gateway protocol

An on-premises network gateway can exchange routes with an Azure virtual network gateway using the border gateway protocol (BGP). Using BGP with an Azure virtual network gateway is dependent on the type you selected when you created the gateway. If the type you selected were:

- ExpressRoute: You must use BGP to advertise on-premises routes to the Microsoft Edge router. You can't create user-defined routes to force traffic to the ExpressRoute virtual network gateway if you deploy a virtual network gateway deployed as type: ExpressRoute. You can use user-defined routes for forcing traffic from the Express Route to, for example, a Network Virtual Appliance.

upvoted 2 times

✉️  **Fearless90** 11 months, 4 weeks ago

Repeated question

<https://www.examtopics.com/discussions/microsoft/view/74497-exam-az-700-topic-10-question-3-discussion/>

upvoted 2 times

✉️  **Fearless90** 11 months, 4 weeks ago

Repeated question

<https://www.examtopics.com/discussions/microsoft/view/64711-exam-az-700-topic-9-question-2-discussion/>

upvoted 2 times

✉️  **Fearless90** 11 months, 4 weeks ago

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

Virtual network gateway: Specify when you want traffic destined for specific address prefixes routed to a virtual network gateway. The virtual network gateway must be created with type VPN. You can't specify a virtual network gateway created as type ExpressRoute in a user-defined route because with ExpressRoute, you must use BGP for custom routes. You can't specify Virtual Network Gateways if you have VPN and ExpressRoute coexisting connections either. You can define a route that directs traffic destined for the 0.0.0.0/0 address prefix to a route-based virtual network gateway. On your premises, you might have a device that inspects the traffic and determines whether to forward or drop the traffic. If you intend to create a user-defined route for the 0.0.0.0/0 address prefix, read 0.0.0.0/0 address prefix first. Instead of configuring a user-defined route for the 0.0.0.0/0 address prefix, you can advertise a route with the 0.0.0.0/0 prefix via BGP, if you've enabled BGP for a VPN virtual network gateway.

upvoted 2 times

✉️  **mrgreat** Most Recent 2 months, 3 weeks ago

To configure the default route on Vnet2 and Vnet3, we can use BGP route exchange. This would allow us to advertise the default route of 0.0.0.0/0 from the Boston datacenter over an ExpressRoute circuit to Vnet2 and Vnet3. This meets the requirement to direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.

Option A, route filters, are used to allow or deny routes based on a set of defined rules. They are not used to configure the default route.

Option C, a user-defined route assigned to GatewaySubnet in Vnet1, would only affect traffic within Vnet1, and not traffic from Vnet2 and Vnet3 to the Boston datacenter.

Option D, a user-defined route assigned to GatewaySubnet in Vnet2 and Vnet3, would only affect traffic within Vnet2 and Vnet3, and not traffic from Vnet2 and Vnet3 to the Boston datacenter.

Therefore, the correct answer is B. BGP route exchange.

upvoted 1 times

✉️  **JennyHuang36** 3 months, 3 weeks ago

In exam Feb 2023

upvoted 2 times

✉️  **mhmyz** 5 months, 3 weeks ago

I think D is Ans.

If you enable BGP and 0.0.0.0/0 is propagated from on-premises,  
Works like a request.

However, this question does not have information that confirms that it is propagated from on-premises.

No.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-forced-tunneling>

There is also a method of setting a forced tunnel with UDR without using BGP as follows,

There is a possibility that D is the correct answer

In that case, the nexthop will be the gateway.

upvoted 2 times

 **cypher9** 11 months, 1 week ago

B is correct.

upvoted 1 times

 **Payday123** 11 months, 3 weeks ago

All answers are wrong :) BGP will not help to propagate default route? VNet2 and VNet3 don't know that they have to send default traffic (0.0.0.0/0) to Vnet1

upvoted 4 times

 **sapien45** 8 months, 2 weeks ago

You are wrong homie.

BGP enables multiple gateways to learn and propagate prefixes from different networks, whether they are directly or indirectly connected. This can enable transit routing with Azure VPN gateways between your on-premises sites or across multiple Azure Virtual Networks.

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-overview#transitrouting>

upvoted 1 times

 **sapien45** 8 months, 3 weeks ago

<https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-bgp-resource-manager-ps?toc=%2Fazur%2Fvirtual-network%2Ftoc.json#part-3---establish-a-vnet-to-vnet-connection-with-bgp>

VNet2 and VNet3 will exchange route informations through vnet to vnet connection via bgp with vnet1

upvoted 1 times

 **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 1 times

 **wsrudmen** 1 year ago

**Selected Answer: B**

It's correct.

You can create custom routes by either creating user-defined routes, or by exchanging border gateway protocol (BGP) routes between your on-premises network gateway and an Azure virtual network gateway.

As it's mentionned "Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit." then UDR doesn't match, we need BGP protocol

upvoted 1 times

 **Kay04** 1 year, 1 month ago

is the answer B or C?

upvoted 1 times

 **RVR** 1 year, 1 month ago

the action on vnet 1 is c, but the question is what needs to be done on vnet2 &3, so i guess enabling bgp is required.

upvoted 1 times

## Introductory Info

### 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 -

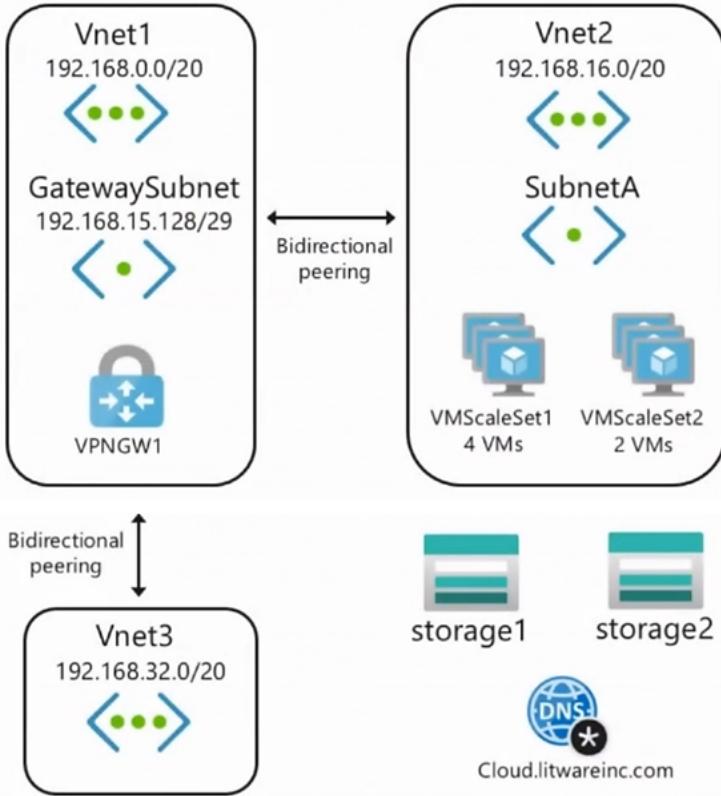
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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	<b>None</b>
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 VMSScaleSet1 to VMSScaleSet2 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

DRAG DROP -

You need to implement outbound connectivity for VMSScaleSet1. The solution must meet the virtual networking requirements and the business requirements.

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

arrange them in the correct order.

Select and Place:

Actions	Answer Area
Create a health probe	
Create a public load balancer in the Standard SKU	
Create a public load balancer in the Basic SKU	
Create a backend pool that contains VMScaleSet1	>
Create a NAT rule	<
Create an outbound rule	

Correct Answer:

Actions	Answer Area
Create a health probe	Create a public load balancer in the Standard SKU
Create a public load balancer in the Basic SKU	Create a backend pool that contains VMScaleSet1
	> Create an outbound rule
Create a NAT rule	

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/skus>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections#outboundrules>

 **Fearless90** Highly Voted 11 months, 4 weeks ago

Answer

Create a public load balancer in the Standard SKU

Create a backend pool that contains VMScaleSet1

Create an outbound rule

upvoted 10 times

 **Fearless90** 11 months, 4 weeks ago

Repeat

<https://www.examtopics.com/discussions/microsoft/view/68612-exam-az-700-topic-9-question-1-discussion/>

upvoted 1 times

 **roshingrg** Most Recent 2 weeks, 4 days ago

public Standard Load Balancer with an HTTPS configuration, along with a backend pool, health probe, and outbound rule, you can follow the steps outlined in the Microsoft Learn module you provided. However, I can provide you with a high-level overview of the steps involved:

Create a Standard Load Balancer:

Specify the load balancer's name, SKU (Standard), and public frontend IP configuration.

Configure the HTTPS protocol for the frontend IP configuration.

Set up the SSL certificate if required.

Create a Backend Pool:

Create a backend pool that includes the virtual machines in VMScaleSet1.

Associate the backend pool with the frontend IP configuration of the load balancer.

Configure Health Probe:

Create a health probe with the required settings, such as the port (443) and probe interval.

Associate the health probe with the backend pool.

Create Outbound Rule:

Define an outbound rule for the load balancer.

Specify the backend pool and health probe to use for outbound traffic.

upvoted 1 times

✉️ **Crazysaffer** 3 weeks, 5 days ago

As far as i know, if you don't create a health probe, then the LB is not going to work. I think it should be in this order

1 - Create a public load Standard balancer (HTTPS = Standard)

2 - Create a backend pool that contains VMSSet1

3 - Create a Health probe (port 443)

4 - Create a Outbound rule (needs a backend pool and a Health Probe)

upvoted 1 times

✉️ **TJ001** 5 months ago

correct answer

upvoted 1 times

✉️ **Goofer** 5 months, 1 week ago

1 - Create a public load Standard balancer (HTTPS = Standard)

2 - Create a backend pool that contains VMSSet1

3 - Create a Health probe (port 443)

4 - Create a Outbound rule (needs a backend pool and a Health Probe)

<https://learn.microsoft.com/en-us/training/modules/load-balancing-non-https-traffic-azure/4-exercise-create-configure-azure-load-balancer>

upvoted 3 times

✉️ **Goofer** 5 months, 1 week ago

1 - Create a public Standard Load balancer (HTTPS = Standard)

<https://learn.microsoft.com/en-us/training/modules/load-balancing-non-https-traffic-azure/3-design-implement-azure-load-balancer-using-azure-portal>

upvoted 1 times

✉️ **unclegrandfather** 11 months, 3 weeks ago

Appeared on exam Jun/28/22

upvoted 2 times

✉️ **Fearless90** 11 months, 4 weeks ago

<https://docs.microsoft.com/en-us/azure/load-balancer/skus>

SKU comparison

Azure Load Balancer has 3 SKUs - Basic, Standard, and Gateway. Each SKU is catered towards a specific scenario and has differences in scale, features, and pricing.

To compare and understand the differences between Basic and Standard SKU, see the following table.

Outbound Rules

Standard Load Balancer - Declarative outbound NAT configuration

Basic Load Balancer - Not available

upvoted 3 times

✉️ **Fearless90** 11 months, 4 weeks ago

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>

Create the virtual network

In this section, you'll create a virtual network, subnet, and Azure Bastion host. The virtual network and subnet contains the load balancer and virtual machines. The bastion host is used to securely manage the virtual machines and install IIS to test the load balancer.

upvoted 1 times

✉️ **Fearless90** 11 months, 4 weeks ago

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>

Create virtual machines

In this section, you'll create two VMs (myVM1 and myVM2) in two different zones (Zone 1, and Zone 2).

These VMs are added to the backend pool of the load balancer that was created earlier.

upvoted 1 times

✉️ **Fearless90** 11 months, 4 weeks ago

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>

Note

Azure provides a default outbound access IP for VMs that either aren't assigned a public IP address or are in the back-end pool of an internal basic Azure load balancer. The default outbound access IP mechanism provides an outbound IP address that isn't configurable.

For more information, see Default outbound access in Azure.

The default outbound access IP is disabled when either a public IP address is assigned to the VM or the VM is placed in the back-end pool of a standard load balancer, with or without outbound rules. If an Azure Virtual Network network address translation (NAT) gateway resource is assigned to the subnet of the virtual machine, the default outbound access IP is disabled.

VMs that are created by virtual machine scale sets in flexible orchestration mode don't have default outbound access.

For more information about outbound connections in Azure, see Use source network address translation (SNAT) for outbound connections.

upvoted 1 times

✉️ **Fearless90** 11 months, 4 weeks ago

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal>

Create NAT gateway

In this section, you'll create a NAT gateway for outbound internet access for resources in the virtual network.  
upvoted 1 times

 **wsrudmen** 1 year ago

It's correct.

Outbound rules is not available for Basic Load Balancer then Standard SKU is required.

After it's a backend pool to link VMScaleSet and the LB. And it's an outbound rule as there's no address translation in this case.

upvoted 1 times

**Introductory Info**

Case Study -

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

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

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

To start the case study -

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

Overview -

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

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

Existing Environment -

Azure Network Infrastructure -

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

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

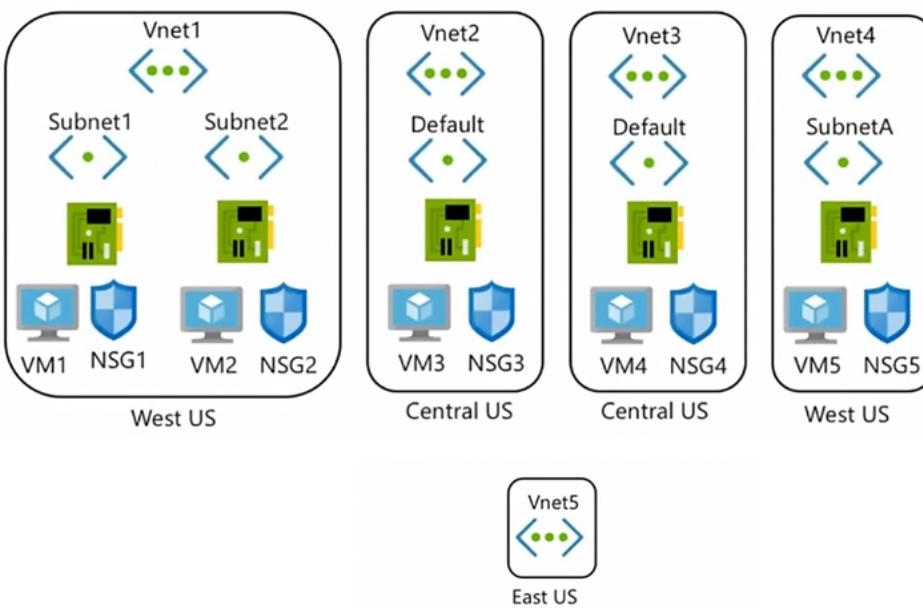
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

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

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 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

Correct Answer:

Next hop type:

None
Internet
Virtual appliance
Virtual network
Virtual network gateway

Reference:

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

✉  **tng69**  10 months, 1 week ago

If I understand this correctly, we create a Route Table with a UDR that points 0.0.0.0/0 to a Virtual Appliance and assign it to Subnet2.

The IP of the virtual appliance (not asked for here) would then be VM-Analyze which then inspects the traffic. In my opinion then, the answers should be fine.

upvoted 16 times

✉  **jeffangel28**  10 months, 2 weeks ago

Given answer is correct!

upvoted 8 times

✉  **TJ001**  5 months ago

classic use case for Hub NVA/Firewall

upvoted 1 times

✉  **Bbb78** 4 months, 2 weeks ago

or a web proxy

upvoted 1 times

**Introductory Info**

Case Study -

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

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

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

To start the case study -

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

Overview -

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

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

Existing Environment -

Azure Network Infrastructure -

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

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

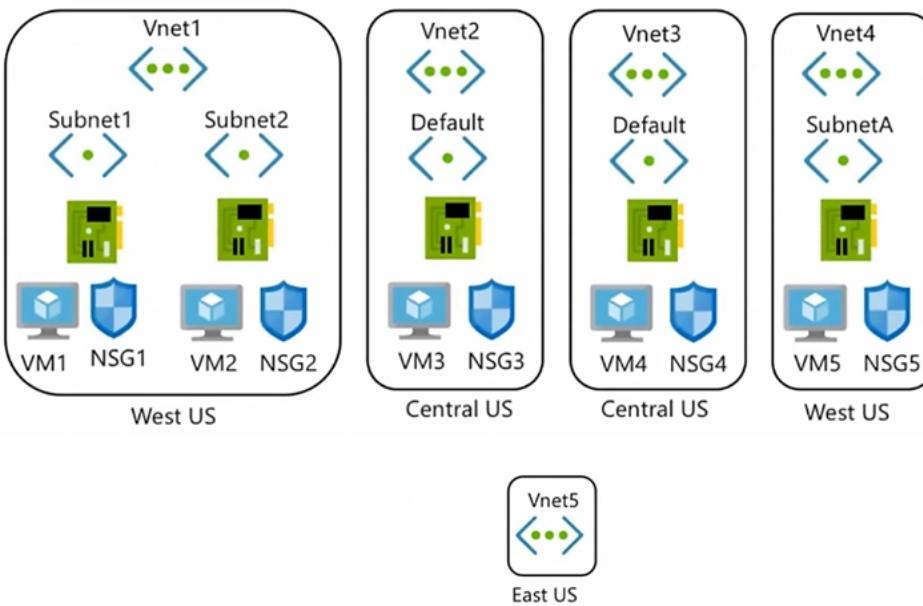
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

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

HOTSPOT -

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

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
From VM1, you can establish a Remote Desktop session with VM2	<input type="radio"/>	<input type="radio"/>
From VM2, you can ping VM1	<input type="radio"/>	<input type="radio"/>
From VM2, you can establish a Remote Desktop session with VM1	<input type="radio"/>	<input type="radio"/>

Correct Answer:

#### Answer Area

Statements	Yes	No
From VM1, you can establish a Remote Desktop session with VM2	<input type="radio"/>	<input checked="" type="radio"/>
From VM2, you can ping VM1	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can establish a Remote Desktop session with VM1	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No -

NSG10 which is attached to VM1's subnet blocks RDP (port TCP 3389) to 'Any' which means the port is blocked to all destinations.

Box 2: Yes -

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

Box 3: No -

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

 **pinpin06**  1 year, 1 month ago

I thin the response should be YES, YES, NO

1) VM1 can establish a RDP session to VM as the filtering is set to inbound even if the rule would have matched ( it would have required outbound)

2) as stated already, this is for vnet4, so no problem, the traffic will be granted

3) the traffic will be dropped by NSG11 set as abound and from the subnet 10.1.0.0/16 to the vnet, so it matches and is dropped.

upvoted 39 times

 **Prutser2** 8 months, 1 week ago

agreed

upvoted 1 times

✉ **jeffangel28** 10 months, 2 weeks ago

You are right!

upvoted 5 times

✉ **Bon\_** Highly Voted 9 months, 3 weeks ago

Yes, Yes, No is correct. Make sure you double-check each of the NSG rules, so it's clear!

1. From VM1 to inbound RDP VM2, there are no NSGs blocking this. There is only a custom inbound NSG for VM1, and a custom outbound NSG for VM2-- neither of which will block our connection

2. VM2 outbound NSG has no rules blocking ping (ICMP). Next review the inbound NSG for VM1. There is an priority rule 1000 -- inbound ICMP deny, but the source is pointing to VNET4 (tricky!)

3. Blocked. VM2 NSG has an outbound deny for 3389 RDP.

upvoted 14 times

✉ **Apptech** Most Recent 2 months, 2 weeks ago

Some basics:

1. NSG on NIC always takes precedence over NSG on Subnet.

2. Default setting for NSG is DenyAllInbound. There is one rule for all NSG linked to NIC which says RDP from Internet is allowed, which indicates that default setting for Inbound is active.

What does ist mean? It means that VM1 cannot establish RDP to VM2 which NSG2 only allows RDP from Internet.

Q1: No

For outbound traffic default setting is Allow All. NSG10 (VNET1/Subnet2) denies ICMP only to Vnet4.

Q2: YES

NSG 11 on Vnet1/Subnet2 does not allow outbound for Virtual Network

Also Default for NSG of Vm3 (NIC) is DenyAllInbound.

Q3: NO

So, in my opinion NYN is correct.

<https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works>

upvoted 1 times

✉ **JennyHuang36** 3 months, 3 weeks ago

In exam Feb 2023

upvoted 2 times

✉ **TJ001** 5 months ago

yes yes no

upvoted 3 times

✉ **TJ001** 5 months ago

same vnet so route is present ...only check NSG rules....

upvoted 2 times

✉ **Mahakal\_123** 5 months, 2 weeks ago

Answer is correct, it will be NYN.

No - Traffic will be dropped by NSG10. Subnet NSG will take precedence over VM interface NSG.

Yes - ICMP is allowed.

No - Traffic will be dropped by NSG11.

upvoted 1 times

✉ **wetraining123** 6 months, 3 weeks ago

check these two NSGS table

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.

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.

so the answer is NNN

upvoted 1 times

✉ **wetraining123** 6 months, 3 weeks ago

its NNN , AS THE custom nsg denies any communication from 10.1.0.0/16 which is the address space of vnet1 , and vm1 and vm2 uses that address space

upvoted 1 times

✉ **Gronow** 7 months, 2 weeks ago

What about the NSG's connected to the NIC's? There is only 1 rule (inbound), which is to allow RDP from Internet. Won't these block any VM/subnet RDP connections allowed via the subnet NSG?

'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'

upvoted 1 times

 **azeem0077** 9 months, 4 weeks ago

Yes, Yes, No  
upvoted 1 times

 **kinder2** 1 year ago

Y,Y,N.  
upvoted 3 times

 **Whatsamattr81** 1 year ago

NSG10 is an inbound rule attached to subnet 1... It doesn't prevent an outbound RDP to subnet 2. Its Yes, Yes, No  
upvoted 6 times

 **Kay04** 1 year, 1 month ago

I believe yes yes no, no outbound filter on subnet 1.  
upvoted 3 times

 **petermogaka91** 1 year, 1 month ago

I think YYN for the answers  
upvoted 4 times

**Introductory Info**

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 -

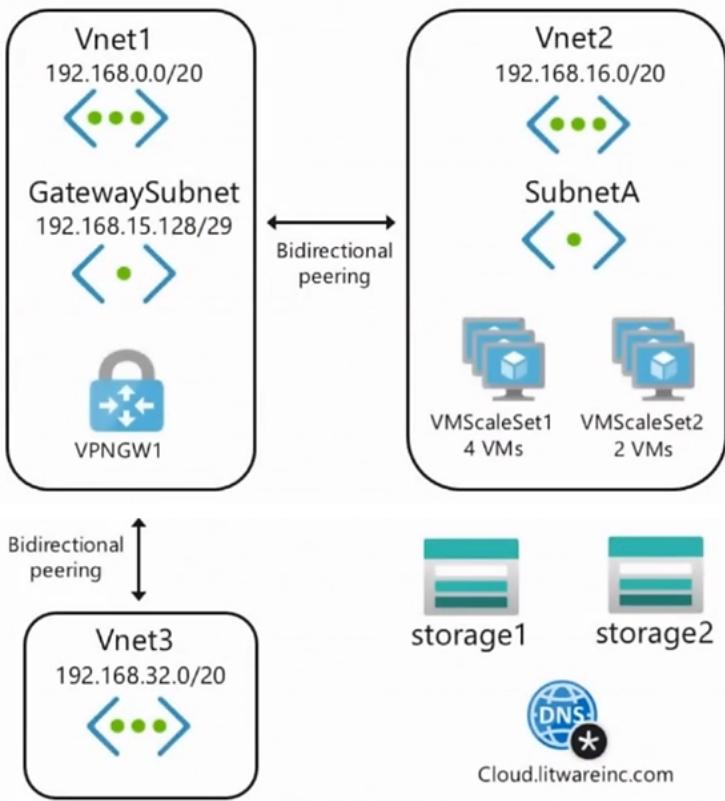
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

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.

## Question

### HOTSPOT -

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Minimum number of custom NSG rules:

1
2
3
4
5

Minimum number of NSG assignments:

1
2
3
4
5

## Answer Area

Minimum number of custom NSG rules:

1
2
3
4
5

Correct Answer:

Minimum number of NSG assignments:

1
2
3
4
5

Box 2: One NSG -

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

Box 1: Two custom rules -

With the NSG attached to VMScaleSet2, you would need to create a custom rule blocking all traffic from VMScaleSet1. Then you would need to create another custom rule with a higher priority than the first rule that allows traffic on port 443.

The default rules in the NSG will allow all other traffic to VMScaleSet2.

  **derrrp**  11 months ago

2 Rules 1 Assignment

Reminds me of an old video I once saw on the internet...

upvoted 20 times

  **sapien45** 8 months, 2 weeks ago

I saw a variant of that movie : 3 rHoles 1 Assgnment

I just saw a few minutes though

upvoted 2 times

  **MariusKas** 8 months, 2 weeks ago

I tested your movie in lab - got all Yesses

upvoted 1 times

  **jeffangel28** 10 months, 2 weeks ago

Right, validated!

upvoted 1 times

 **mrgreat** Most Recent 2 months, 3 weeks ago

To restrict traffic from VMScaleSet1 to VMScaleSet2 on TCP port 443, we need to create a custom NSG rule to allow traffic on port 443 and apply it to both VMScaleSet1 and VMScaleSet2. We also need to create a custom NSG rule to deny all traffic and apply it to VMScaleSet1.

So the minimum number of custom NSG rules and NSG assignments required would be:

2 custom NSG rules: 1 to allow traffic on TCP port 443 and 1 to deny all traffic

2 NSG assignments: 1 for VMScaleSet1 and 1 for VMScaleSet2

Therefore, the answer is:

Minimum number of custom NSG rules = 2

Minimum number of NSG assignments = 2

Note: It's important to note that we could potentially use an existing NSG that is already assigned to the virtual machines and add the necessary rules to it. In that case, the minimum number of NSG assignments would be 1.

upvoted 3 times

 **MrBlueSky** 2 months, 1 week ago

You could just apply the NSG to the subnet that both VMSS are in.

Min number of rules = 2

Min number of assignments = 1

upvoted 2 times

 **BenH** 1 year ago

Correct

upvoted 2 times

Question #1

Topic 15

**Introductory Info**

Case Study -

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

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

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

To start the case study -

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

Overview -

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

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

Existing Environment -

Azure Network Infrastructure -

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

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

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

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines -

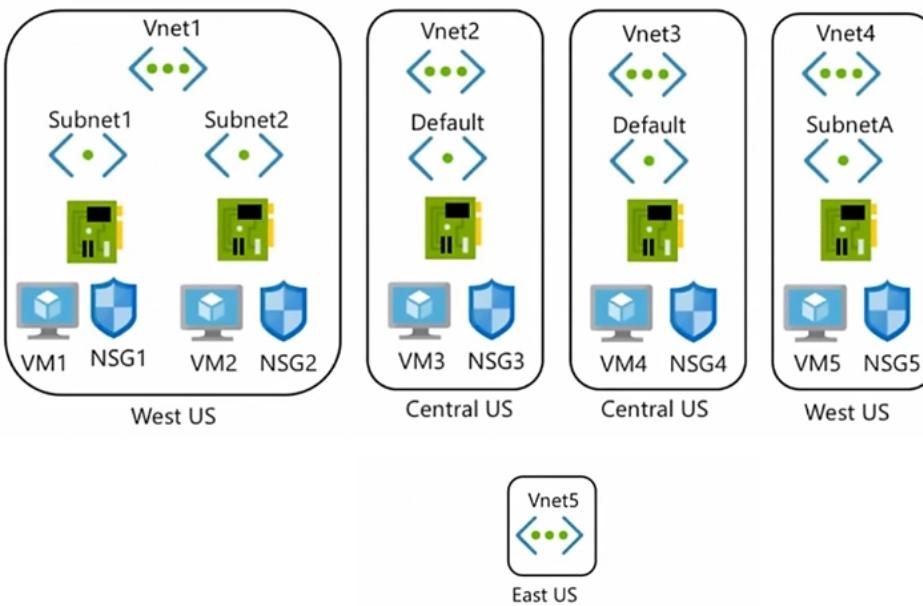
The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

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

HOTSPOT -

In which NSGs can you use ASG1 and to which virtual machine network interfaces can you associate ASG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

NSGs:

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

Virtual machines:

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

Correct Answer:

## Answer Area

NSGs:

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

Virtual machines:

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

✉  **leo87las2**  9 months, 1 week ago

NSG1,NSG2 same vnet  
VM2 only NIC in same Vnet  
<https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>  
upvoted 21 times

✉  **zenithcsa1**  9 months, 2 weeks ago

Tested  
NSG1, NSG2, and NSG5 only : ASG and NSG must be in the same region  
VM2 only : network interfaces attached to an ASG must be in the same vNet.  
<https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>  
upvoted 15 times

✉  **tdienst** 9 months, 2 weeks ago

NSG1 & NSG2  
VM2 Only

NSG5 also is out of the question:

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

upvoted 14 times

✉  **zenithcsa1** 6 months, 4 weeks ago

Please read the question again, and the next paragraph in the link. The question is about connection between ASG and NSG, not between ASG and NIC.  
upvoted 1 times

✉  **wooyourdaddy** 3 months, 1 week ago

I was initially only NSG1 & NSG2 only, but came across these 2 websites:

<https://medium.com/awesome-azure/azure-application-security-group-asg-1e5e2e5321c3>  
<https://petri.com/understanding-application-security-groups-in-the-azure-portal/>

Which both state:

Source and Destination in the new rule blade allow you to select any application security group in the same region.

So while their may be not practical use case for using ASG1 in NSG5 in this case, the ASG can be selected by any NSGs in the same region.

The only caveat being:

If you specify an application security group as the source and destination in a security rule, the network interfaces in both application

security groups must exist in the same virtual network.

So I would agree that NSG1, NSG2 and NSG5 can use ASG1. And only VM2 can be added to ASG1 due to the NICs needing to be in the same VNET.

upvoted 2 times

✉️👤 **wooyourdaddy** 2 months, 2 weeks ago

I set up this lab scenario. When I go to NSG5 and create an inbound rule, I am able to change the destination to application security group and ASG1 is visible as an option to select. When I try in NSG3 and NSG4, the Destination application security groups drop down is greyed out and says 'No application security groups found'.

When I go to Network under Settings on VM5, the ASG1 application security group is visible as an option to choose. However, when I click save, the operation fails indicating that the ASG is already attached to another device in a separate subnet.

I was successfully able to add VM2 to the ASG, but ASG1 was not even visible to VM3 and VM4.

The questions seems to want to drive home the point that NSGs and ASGs need to be in the same region if you intend to use the ASG in an NSG rule, while VM NICs added to an ASG need to be in the same VNET.

upvoted 1 times

✉️👤 **GiorgioLDN** 7 months, 4 weeks ago

Correct. ASG1 is applied on VM1. VM1's interface is the first network interface assigned to ASG1, thus all subsequent network interfaces assigned to ASG1 must exist in VNet1. NSG2 exists in VNet1.

upvoted 1 times

✉️👤 **wooyourdaddy** 3 months, 1 week ago

I set up this lab scenario. When I go to NSG5 and create an inbound rule, I am able to change the destination to application security group and ASG1 is visible as an option to select. When I try in NSG3 and NSG4, the Destination application security groups drop down is greyed out and says 'No application security groups found'.

When I go to Network under Settings on VM5, the ASG1 application security group is visible as an option to choose. However, when I click save, the operation fails indicating that the ASG is already attached to another device in a separate subnet.

I was successfully able to add VM2 to the ASG, but ASG1 was not even visible to VM3 and VM4.

The questions seems to want to drive home the point that NSGs and ASGs need to be in the same region if you intend to use the ASG in an NSG rule, while VM NICs added to an ASG need to be in the same VNET.

upvoted 1 times

✉️👤 **somenick** 3 months ago

NSG1, NSG2, and NSG5 only. Also tested and it's true. You can use ASG from another VNET in the same region.

upvoted 2 times

✉️👤 **JohnnyChimpo** Most Recent 1 month, 2 weeks ago

Congrats on making it to the last question. Godspeed and best of luck everyone :D

upvoted 2 times

✉️👤 **\_fvt** 2 months, 2 weeks ago

- All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

- If you specify an application security group as the source and destination in a security rule, the network interfaces in both application security groups must exist in the same virtual network. For example, if AsgLogic contained network interfaces from VNet1, and AsgDb contained network interfaces from VNet2, you could not assign AsgLogic as the source and AsgDb as the destination in a rule. All network interfaces for both the source and destination application security groups need to exist in the same virtual network.

So, you can apply the ASG to all NSG within the same region :

=> "NSG1, NSG2, and NSG5 only"

But, as VM1 NIC is already in the ASG, you cannot add another NIC from a different VNet:

=> "VM2 only"

upvoted 1 times

✉️👤 **Madball** 4 months, 1 week ago

I believe the answers are:

NSGS = NSG1, NSG2 and NSG5 only.

My reasoning for this is that an ASG can be used in NSG rules for any NSG within the same region.

Virtual Machines = VM2 only

The ASG can only be attached to NICs within the same virtual network.

I have tested this in my lab.

upvoted 3 times

 **TJ001** 5 months ago

Box 1: NSG 1 and NSG 2  
Box 2: VM2

upvoted 2 times

 **vivikar** 5 months, 3 weeks ago

NSG 1 and NSG2: As per All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

upvoted 1 times

 **winy** 6 months, 3 weeks ago

Box 1: NSG 1 and NSG 2  
Box 2: VM2 , VM1 only

This has been tested on the LAB.

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups#allow-database-businesslogic>

upvoted 4 times

 **winy** 6 months, 3 weeks ago

Box 1: NSG 1 and NSG 2  
Box 2: VM2

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.

<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups#allow-database-businesslogic>

upvoted 2 times

 **Prutser2** 8 months, 1 week ago

box1: only vnets 1 and 4 are in westUS, so only NSGs in this region can re-use the existing ASG1  
result: NSG1, NSG2 and NSG5

box2:

All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.  
source:<https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups>

result:Vm2 only (was already assigned to VM1, which is in vnet1)

upvoted 1 times

 **Pradh** 8 months, 2 weeks ago

These are correct answers !! Rest is your wish to opt for .

NSG1, NSG2, and NSG5 only

VM2 only

upvoted 1 times

 **Cristoicach91** 9 months, 3 weeks ago

Correct.

upvoted 2 times