AZ-700 Q&As

Designing and Implementing Microsoft Azure Networking Solutions

Pass Microsoft AZ-700 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/az-700.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You need to monitor the latency between your on-premises network and the Azure virtual machines.

What should you use?

A. Service Map

B. Connection troubleshoot

C. Network Performance Monitor

D. Effective routes

Correct Answer: C

Correct Answer(s):

Network Performance Monitor - Network Performance Monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor

network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.

You can monitor network connectivity across cloud deployments and on-premises locations, multiple data centers, and branch offices and mission-critical multitier applications or microservices. With Performance Monitor, you can detect

network issues before users complain.

https://docs.microsoft.com/en-us/azure/azure-monitor/insights/network-performance-monitor

Wrong Answers:

Service Map - Service Map automatically discovers application components on Windows and Linux systems.

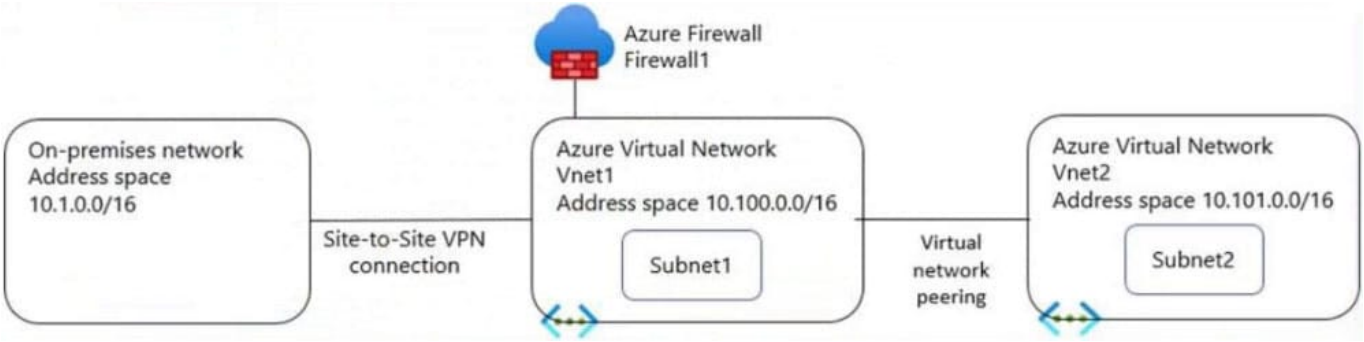
Connection troubleshoot - enable you to troubleshoot network performance and connectivity issues in Azure.

Effective routes You can use effective routes to determinewhy you can\\'t connect to the VM.

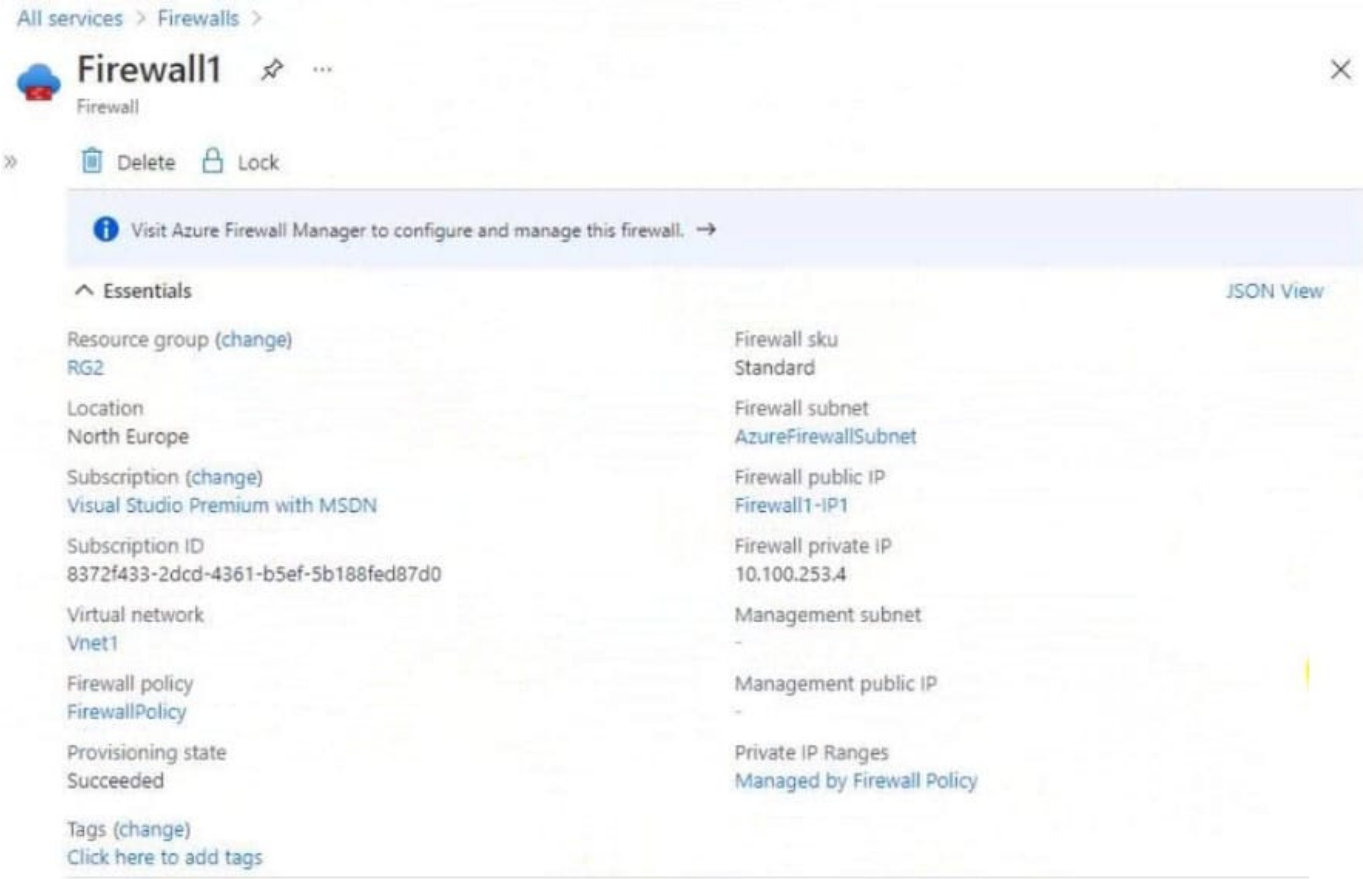
QUESTION 2

HOTSPOT

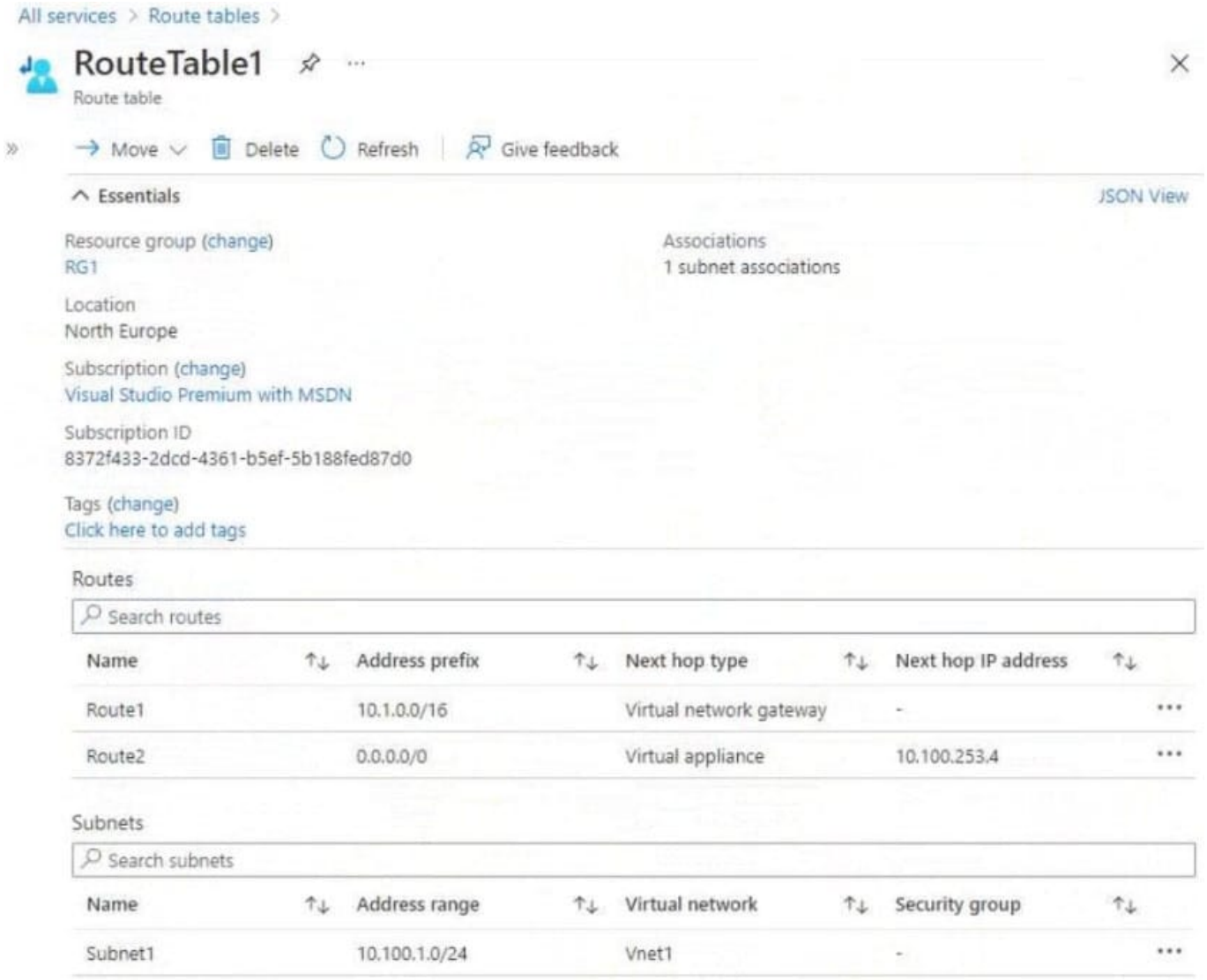
You have the network topology shown in the Topology exhibit. (Click the Topology tab.)



You have the Azure firewall shown in the Firewall 1 exhibit. (Click the Firewall tab.)

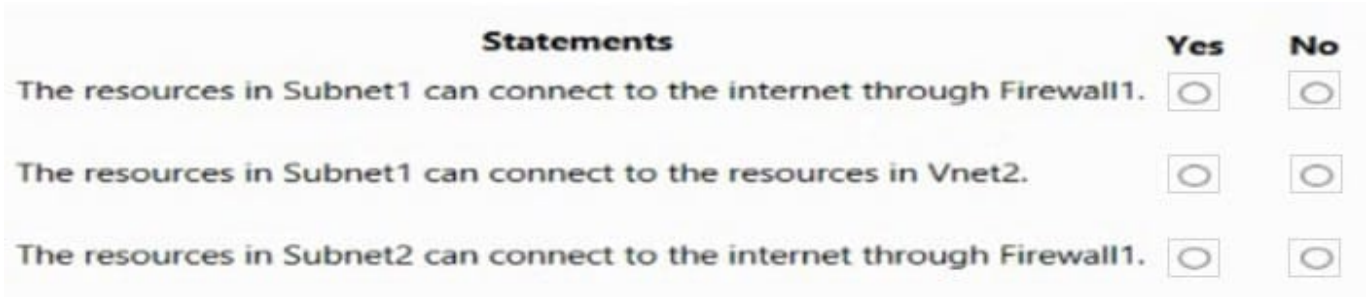


You have the route table shown in the RouteTable1 exhibit. (Click the RouteTable1 tab.)



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:



Correct Answer:

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

Box 1: Yes

Resources in Subnet1 will use the Route2 and its Next hop ID address to the Firewall 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

---

QUESTION 3

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.

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

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 Searchandfind 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

QUESTION 4

You have a web app named App1 that is hosted in on-premises servers and on four Azure virtual machines (VMs).

Each Azure region has one virtual machine.

You need to recommend a solution to ensure that users will always connect to the closest instance of App1.

The solution must prevent the users from attempting to connect to a failed instance of App1.

Which two possible should you recommendation achieve the goal?

A. Azure Front Door Service

B. Azure Load Balancer

C. round-robin DNS

D. Azure Traffic Manager

E. Azure Application Gateway

Correct Answer: AD

Correct Answers:

Azure Front Door Service - Front Door is an application delivery network that provides global load balancing and site acceleration service for web applications. It offers Layer 7 capabilities for your application like SSL offload, path-based

routing, fast failover, caching, etc. to improve performance and high-availability of your applications.

Azure Traffic Manager - Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

https://docs.microsoft.com/en-au/azure/architecture/guide/technology-choices/load-balancing-overview

Wrong Answers:

Azure Load Balancer - It is a regional load balancing solution.

round-robin DNS - Round-robin DNS is a load balancing technique where the balancing is done by a type of DNS server called an authoritative nameserver, rather than using a dedicated piece of load-balancing hardware.

Azure Application Gateway - It is a regional load balancing solution.

QUESTION 5

You need to implement name resolution for the cloud.healthengine.com.

The solution must meet the networking requirements.

What should you do to implement automatic DNS name registration in clould.healthengine.com?

A. Create virtual network links

B. Configure conditional forwarding

C. Create an SOA record in cloud.healthengine.com

Correct Answer: A

Scenario: Automatically register the DNS names of Azure virtual machines to the cloud.healthengine.com zone

After you create a private DNS zone in Azure, you\\'ll need to link a virtual network to it. Once linked, VMs hosted in that virtual network can access the private DNS zone. When creating a link between a private DNS zone and a virtual network. You have the option to enable autoregistration. With this setting enabled, the virtual network becomes a registration virtual network for the private DNS zone. A DNS record gets automatically created for any virtual machines you deploy in the virtual network. DNS records will also be created for virtual machines already deployed in the virtual network.

https://docs.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

---

QUESTION 6

Which rules should you configure in Azure firewall to allow inbound internet connections?

A. Application rules

B. Network rules

C. NAT rules

Correct Answer: C

Correct Answer(s):

NAT rules: Configure DNAT rules to allow incoming Internet connections.

https://docs.microsoft.com/en-us/azure/firewall/firewall-faq#what-are-some-azure-firewall-concepts

Wrong Answers:

Application rules - Configure fully qualified domain names (FQDNs) that can be accessed from a subnet.

Network rules - Configure rules that contain source addresses, protocols, destination ports, and destination addresses.

QUESTION 7

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

---

QUESTION 8

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 type of ExpressRoute gateway should you recommend?

A. High Performance (ERGw2AZ)

B. Standard Performance (ERGw1AZ)

C. Ultra-Performance (ERGw3AZ)

Correct Answer: C

Scenario: The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection. To configure FastPath, the virtual network gateway must be either: Ultra-Performance ErGw3AZ
https://docs.microsoft.com/en-us/azure/expressroute/about-fastpath#gateways

QUESTION 9

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.

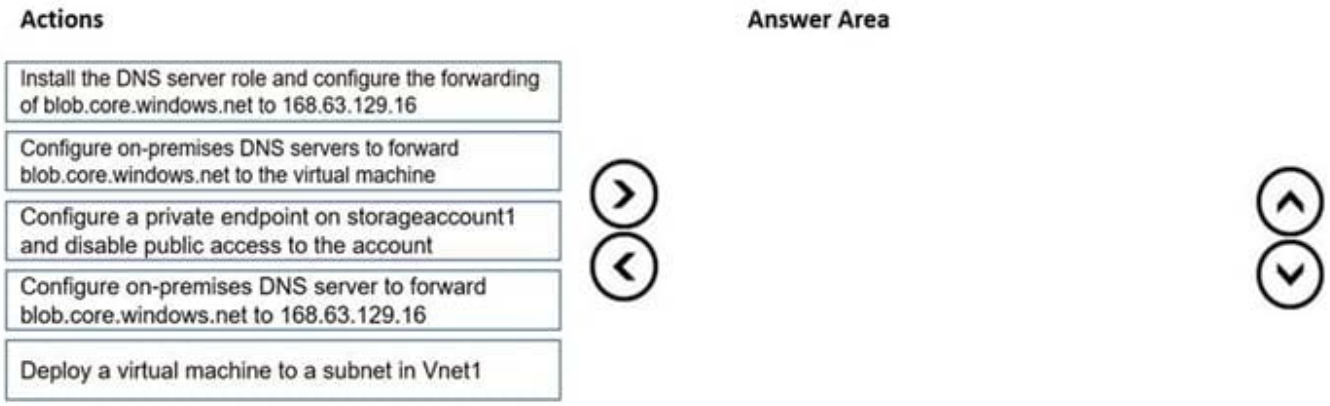
You need to configure a private endpoint for the blob storage. The solution must meet the following requirements:

Ensure that all on-premises users can access storageaccount1 through the private endpoint.

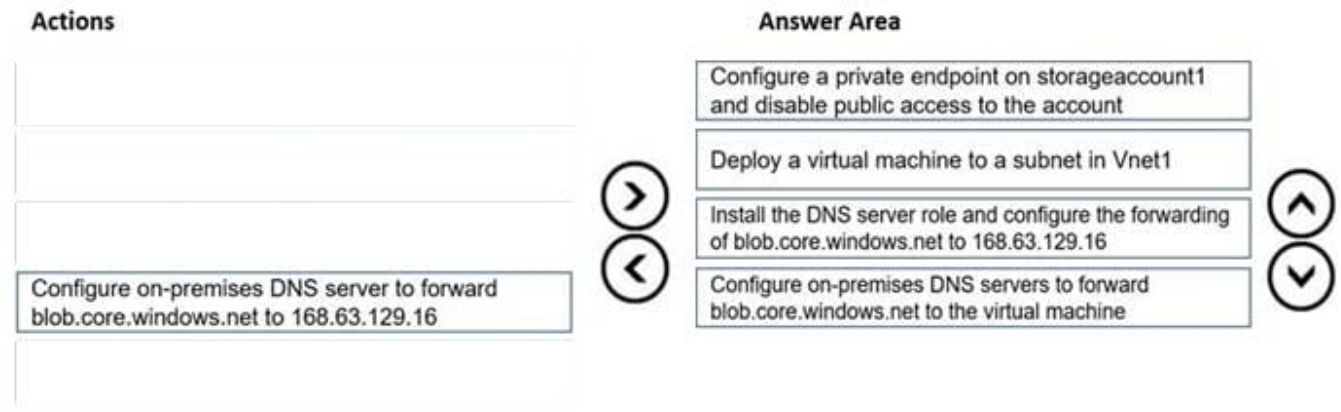
Prevent access to storageaccount1 from being interrupted.

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:



Correct Answer:



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

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

---

QUESTION 10

You have an Azure subscription that contains two virtual networks named VritualNetwork1 and VritualNetwork2.

You have a Windows 10 device that connects to VritualNetwork1 by using a Point-to-Site (P2S) IKEv2 VPN. You have implemented virtual network peering between VritualNetwork1 and VritualNetwork2.

VritualNetwork1 allows gateway transit. VritualNetwork2 can use the remote gateway. You discover that you cannot communicate with VritualNetwork2 from Windows 10 device. You need to ensure that you can communicate with

VritualNetwork2 from Windows 10 device.

To achieve the requirement, you enable BGP on the gateway of VritualNetwork1.

Did you achieve the requirement?

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. 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

---

QUESTION 11

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.

To achieve the requirement, you configure the firewall on storage1 to only accept connections from Vnet1.

Did you achieve the requirement?

A. Yes

B. No

Correct Answer: B

If you configure the firewall on storage1 to only accept connections from Vnet1, any virtual machine from Vnet1 will be able to connect to the storage1. VM1 can also access other storage accounts depending on the firewall settings on other storage accounts.

QUESTION 12

You plan to deploy five virtual machines to a subnet named Subnet1.

Each virtual machine requires the same inbound and outbound security rules.

What is the minimum number of network security groups that you require?

A. 1

B. 5

C. 10

Correct Answer: A

The rules are same for all virtual machines, so one NSG should suffice the requirement.

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

---

QUESTION 13

You have Azure virtual machines in three Azure regions.

Each virtual machine has a public IP address assigned to its network interface. An application named App1 is installed in each virtual machine.

You plan to implement Azure Front Door-based load balancing across all the virtual machines.

You need to ensure that App1 on the virtual machines will only accept traffic routed from Azure Front Door.

What should you implement?

A. Azure Private Link

B. Service endpoints

C. Network security groups (NSGs) with service tags

D. Network security groups (NSGs) with application security groups

Correct Answer: C

Correct Answer(s):

Network security groups (NSGs) with service tags - To lock down your application to accept traffic only from your specific Front Door, you will need to set up IP ACLs for your backend and then restrict the traffic on your backend to the specific

value of the header \\'X-Azure-FDID\\' sent by Front Door. These steps are detailed out as below:

Configure IP ACLing for your backends to accept traffic from Azure Front Door\\'s backend IP address space and Azure\\'s infrastructure services only.

The above step basically means configure NSGs with service tags.

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq

Wrong Answers:

Azure Private Link - Azure Private Link enables you to access Azure PaaS Services over a private endpoint in your

virtual network.

Service endpoints - Service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. It does not restrict traffic.

Network security groups (NSGs) with application security groups - ASG\\'s allow you to group virtual machines and define network security policies based on those groups. You must also use service tag AzureFrontDoor.Backend in the network

security groupsto restrict the traffic.

QUESTION 14

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:

1.

Log all connections from Australia.

2.

Deny all connections from New Zealand.

3.

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

QUESTION 15

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 minimizing latency of traffic to Vnet2?

A. Create a dedicated ExpressRoute circuit for Vnet2

B. Connect Vnet2 directly to the ExpressRoute circuit

C. Configure gateway transit for the peering between Vnet1 and Vnet2

Correct Answer: C

Scenario:

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

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.

Gateway transit allows you to share an ExpressRoute or VPN gateway with all peered VNets and lets you manage the connectivity in one place. Sharing enables cost-savings and reduction in management overhead.

https://azure.microsoft.com/en-us/blog/create-a-transit-vnet-using-vnet-peering/