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

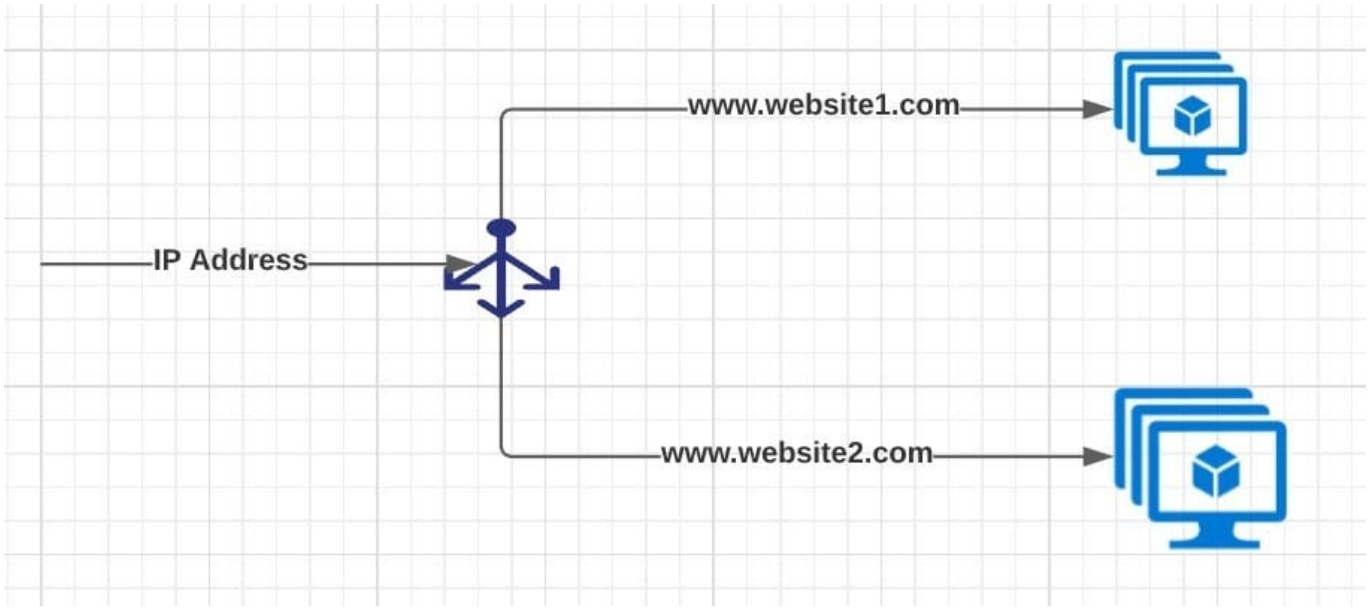
Following Questions and Answers are all new published by Microsoft Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

You have deployed multiple websites in Internet Information Server (IIS) by using Azure virtual machine scale sets (VMSS).

User sessions must be routed to the same server by using cookie-based session affinity. The below image depicts the network traffic flow for the websites to the VMSS.



What should you configure to make sure web traffic arrives at the appropriate server in the VMSS?

A. Routing rules and backend listeners

B. CNAME and A records

C. Routing method and DNS time to live (TTL)

D. Path-based redirection and websockets

Correct Answer: A

Correct Answer(s):

Routing rules and backend listeners - You can configure the hosting of multiple web sites when you create an application gateway. You need to define backend address pools using virtual machines. You then configure listeners and rules

based on domains that you own to make sure web traffic arrives at the appropriate servers in

the pools.

https://docs.microsoft.com/bs-latn-ba/azure//application-gateway/create-multiple-sites-portal

Wrong Answers:

CNAME and A records - These are used for domain registrations.

Routing method and DNS time to live (TTL) - DNS TTL (time to live) is a setting that tells the DNS resolver how long to cache a query before requesting a new one. This is nothing to do with routing.

Path-based redirection and websockets - Path Based Routing allows you to route traffic to back-end server pools based on URL Paths of the request.

QUESTION 2

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 3

You need to create an Azure Firewall instance named FW1 that meets the following requirements:

1.

Has an IP address from the address range of 10.1.255.0/24

2.

Uses a new Premium firewall policy named FW-policy1

3.

Routes traffic directly to the internet

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

A. See explanation below.

B. Placeholder

C. Placeholder

D. Placeholder

Correct Answer: A

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 -

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

---

QUESTION 4

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:

1.

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

2.

Minimize costs.

Which gateway SKU should you specify?

A. VpnGw1AZ

B. VpnGw2AZ

C. VpnGw4AZ

D. VpnGw5AZ

Correct Answer: C

VpnGw4AZ supports 90 Site-to-Site VPN connections at a lower cost than VpnGw5AZ. VpnGw1AZ, VpnGw2AZ, and VpnGw4AZ supports max 30.

Gateway SKUs by tunnel, connection, and throughput

VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP	Zone-redund
Generation1	Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported	No
Generation1	VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	No
Generation1	VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	No
Generation1	VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	No
Generation1	VpnGw1AZ	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	Yes
Generation1	VpnGw2AZ	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	Yes
Generation1	VpnGw3AZ	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	Yes
Generation2	VpnGw2	Max. 30	Max. 128	Max. 500	1.25 Gbps	Supported	No
Generation2	VpnGw3	Max. 30	Max. 128	Max. 1000	2.5 Gbps	Supported	No
Generation2	VpnGw4	Max. 100*	Max. 128	Max. 5000	5 Gbps	Supported	No
Generation2	VpnGw5	Max. 100*	Max. 128	Max. 10000	10 Gbps	Supported	No

Reference: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

QUESTION 5

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.

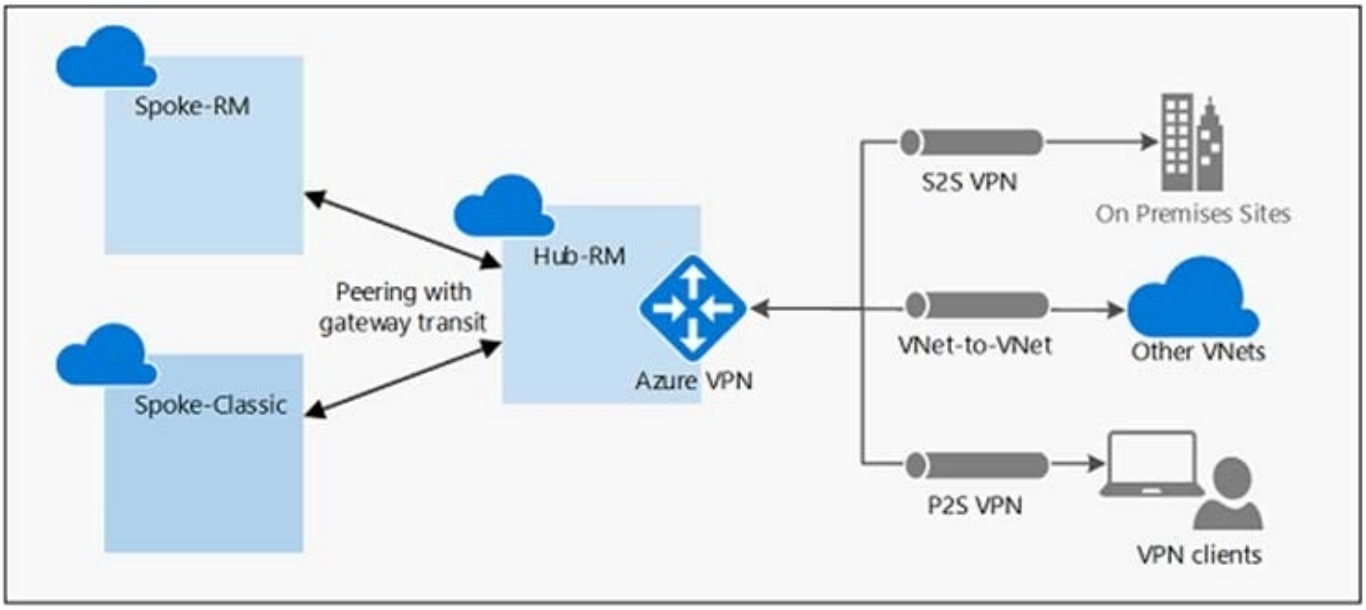
C. On the peerings from Vnet2 and Vnet3, select Allow gateway transit.

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

Latest AZ-700 Dumps AZ-700 VCE Dumps AZ-700 Exam Questions