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.geekcert.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

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 for each virtual machine?

A. Create an additional IP configuration

B. Create an additional NIC

C. Create a public IPv6 address

Correct Answer: A

You need to configure the VM NICs with an IPv6 address. https://docs.microsoft.com/en-us/azure/load-balancer/ipv6-add-to-existing-vnet-cli

QUESTION 2

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": "f7546159ylhjk7wal14568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


You need to ensure that the URL is accessible through the application gateway.

Solution: You disable the WAF rule that has a ruleld of 920300.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 3

You have an on-premises network that uses an IP address space of 172.16.0.0/16.

You plan to create a new Azure subscription and deploy 25 virtual machines.

The requirements are as follows:

All Azure virtual machines must be placed on the same subnet named Subnet1.

All the Azure virtual machines must be able to communicate with all on-premises servers.

The servers must be able to communicate between the on-premises network and Azure by using a site-to-site VPN.

What should you include in the recommendation for Subnet1 and Gateway subnet IP address space?

A. 172.16.0.0/16 and 172.16.1.0/28

B. 172.16.0.0/16 and 192.168.0.0/24

C. 172.16.1.0/28 and 192.168.0.0/24

D. 192.168.0.0/24 and 172.16.1.0/28

E. 192.168.0.0/24 and 192.168.1.0/28

Correct Answer: E

We cannot use these IP address spaces - 172.16.0.0/16 and 172.16.1.0/28 in Azure as these overlap with on- premises IP address space. The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part

of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

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 recommend that you create a gateway subnet that uses a /27 or /28.

So, the subnet1 IP address space must be 192.168.0.0/24 and Gateway subnet IP address space must be 192.168.1.0/28

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal#VNetGateway

Wrong Answers:

172.16.0.0/16 and 172.16.1.0/28 - Overlaps with on-premises IP address space.

172.16.0.0/16 and 192.168.0.0/24 - Overlaps with on-premises IP address space.

172.16.1.0/28 and 192.168.0.0/24 - Overlaps with on-premises IP address space.

192.168.0.0/24 and 172.16.1.0/28 - Overlaps with on-premises IP address space.

QUESTION 4

You plan to create a Point-to-Site (P2S) VPN connection for a remote user to connect to your Azure environment. Which of the following protocols should you use?

A. OpenVPN

B. IPSec

C. Secure Socket Tunneling Protocol (SSTP)

D. IKEv2 VPN

E. FTP

Correct Answer: ACD

Point-to-site VPN can use one of the following protocols:

OpenVPN?Protocol, an SSL/TLS based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. OpenVPN can be used to connect from Android, iOS (versions 11.0 and above), Windows, Linux, and Mac devices (macOS versions 10.13 and above).

Secure Socket Tunneling Protocol (SSTP), a proprietary TLS-based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. SSTP is only supported on Windows devices. Azure supports all versions of Windows that have SSTP and support TLS 1.2 (Windows 8.1 and later).

IKEv2 VPN, a standards-based IPsec VPN solution. IKEv2 VPN can be used to connect from Mac devices (macOS versions 10.11 and above). https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#protocol

---

QUESTION 5

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