**\*\*AZ-104 Networking MCQs\*\***

**\*\*Question 1:\*\***

**Which Azure networking component allows you to filter network traffic to and from Azure resources in an Azure Virtual Network (VNet)?**

A) Azure Load Balancer

B) Azure Application Gateway

C) Network Security Group (NSG)

D) Azure Firewall

**\*\*Question 2:\*\***

**You need to connect two Azure Virtual Networks (VNets) located in different Azure regions. Which of the following is the most suitable method?**

A) VNet Peering

B) VPN Gateway

C) ExpressRoute

D) Network Security Group

**\*\*Question 3:\*\***

**Which Azure service provides centralized network security control, logging, and inspection for all traffic flowing to and from Azure Virtual Networks?**

A) Azure Load Balancer

B) Azure Application Gateway

C) Azure Firewall

D) Network Watcher

**\*\*Question 4:\*\***

**You have a Virtual Machine (VM) in an Azure VNet. You want to ensure that the VM always gets the same private IP address. What should you configure?**

A) Dynamic IP address

B) Static IP address

C) Public IP address

D) Internal Load Balancer

**\*\*Question 5:\*\***

**Which type of Azure Load Balancer operates at Layer 7 (Application Layer) and supports URL-based routing and SSL termination?**

A) Azure Standard Load Balancer

B) Azure Basic Load Balancer

C) Azure Application Gateway

D) Azure Front Door

**\*\*Question 6:\*\***

**You need to establish a private, dedicated, high-bandwidth connection between your on-premises datacenter and Azure. Which service would you use?**

A) Site-to-Site VPN

B) Point-to-Site VPN

C) ExpressRoute

D) VNet Peering

**\*\*Question 7:\*\***

**Which component in Azure Network Watcher allows you to troubleshoot connectivity issues between a VM and another endpoint, showing the hop-by-hop path?**

A) IP flow verify

B) NSG flow logs

C) Connection troubleshoot

D) Packet capture

**\*\*Question 8:\*\***

**You want to enable two-factor authentication for administrative access to your Azure resources and require users to connect via a secure, encrypted tunnel from their individual client machines. Which VPN type is best suited for this?**

A) Site-to-Site VPN

B) Point-to-Site VPN

C) VNet Peering

D) ExpressRoute

**\*\*Question 9:\*\***

**What is the primary purpose of a Public IP address in Azure?**

A) To assign a private IP address to a VM

B) To enable communication with resources within the same VNet

C) To allow resources to communicate with the internet or other public endpoints

D) To provide internal load balancing for VMs

**\*\*Question 10:\*\***

**Which of the following is a key advantage of using Azure DNS for your domain names?**

A) It provides physical security for your DNS servers.

B) It integrates seamlessly with Azure Active Directory.

C) It allows you to host your DNS zones in Azure and manage DNS records.

D) It encrypts all DNS queries by default.

**\*\*Question 11:\*\***

**You are designing a solution where web traffic needs to be distributed across multiple backend web servers, and you also need to support sticky sessions and URL-based routing. Which Azure networking service should you choose?**

A) Azure Load Balancer

B) Azure Traffic Manager

C) Azure Application Gateway

D) Azure Front Door

**\*\*Question 12:\*\***

**Which of the following is NOT a valid scope for a Network Security Group (NSG)?**

A) Subnet

B) Network Interface Card (NIC)

C) Virtual Network (VNet)

D) Individual VM

**\*\*Question 13:\*\***

**You need to control inbound and outbound traffic to a subnet based on service tags (e.g., "AzureCloud", "Storage"). Where would you configure this?**

A) Azure Firewall rules

B) Network Security Group (NSG) rules

C) User Defined Routes (UDRs)

D) Azure DDoS Protection

**\*\*Question 14:\*\***

**What is the maximum number of NICs a single Azure VM can have?**

A) 2

B) 4

C) It depends on the VM size

D) 8

**\*\*Question 15:\*\***

**You want to implement a custom routing policy for traffic leaving an Azure subnet, directing it through a virtual appliance. What Azure networking component would you use?**

A) Network Security Group (NSG)

B) Service Endpoint

C) User Defined Route (UDR)

D) Azure Private Link

**\*\*Question 16:\*\***

**Which Azure service provides global routing to distribute user traffic to the most performant application endpoint, based on various routing methods like priority, geographic, or performance?**

A) Azure Load Balancer

B) Azure Application Gateway

C) Azure Front Door

D) Azure Traffic Manager

**\*\*Question 17:\*\***

**You need to restrict access to an Azure Storage Account so that it can only be accessed by specific subnets within your Azure Virtual Networks. Which feature would you use?**

A) Service Endpoint

B) Private Endpoint

C) Network Security Group

D) Public IP Address

**\*\*Question 18:\*\***

**Which of the following is a benefit of using Azure Private Link?**

A) It allows public internet access to your Azure PaaS services.

B) It provides private connectivity from your VNet to Azure PaaS services using a private IP address.

C) It automatically encrypts all traffic between VNets.

D) It enables hybrid cloud connectivity over the public internet.

**\*\*Question 19:\*\***

**You are configuring Azure Firewall. Which rule collection type allows you to filter traffic based on fully qualified domain names (FQDNs)?**

**A)** Network rule collection

B) Application rule collection

C) DNAT rule collection

D) Threat intelligence rule collection

**\*\*Question 20:\*\***

**What is the purpose of an Azure Availability Zone when deploying a Virtual Network Gateway?**

A) To ensure higher availability for the VPN/ExpressRoute gateway.

B) To distribute traffic across multiple regions for disaster recovery.

C) To provide a dedicated public IP address for the gateway.

D) To encrypt all traffic passing through the gateway.

---

\*\*Answers:\*\*

1. \*\*C) Network Security Group (NSG)\*\*

2. \*\*B) VPN Gateway\*\* (VNet Peering is for VNets in the \*same\* region, or across regions with Global VNet Peering, but VPN Gateway is the most direct and common for different regions, especially if complex routing or firewalling is needed. For simple intra-Azure connectivity, Global VNet Peering is also an option, but VPN Gateway is explicitly cross-region and offers more features.)

3. \*\*C) Azure Firewall\*\*

4. \*\*B) Static IP address\*\*

5. \*\*C) Azure Application Gateway\*\*

6. \*\*C) ExpressRoute\*\*

7. \*\*C) Connection troubleshoot\*\*

8. \*\*B) Point-to-Site VPN\*\*

9. \*\*C) To allow resources to communicate with the internet or other public endpoints\*\*

10. \*\*C) It allows you to host your DNS zones in Azure and manage DNS records.\*\*

11. \*\*C) Azure Application Gateway\*\*

12. \*\*C) Virtual Network (VNet)\*\* (NSGs are applied at the subnet or NIC level, not the VNet level itself.)

13. \*\*B) Network Security Group (NSG) rules\*\*

14. \*\*C) It depends on the VM size\*\*

15. \*\*C) User Defined Route (UDR)\*\*

16. \*\*D) Azure Traffic Manager\*\* (Azure Front Door also does global routing but is Layer 7, Traffic Manager is DNS-based at Layer 3/4)

17. \*\*A) Service Endpoint\*\*

18. \*\*B) It provides private connectivity from your VNet to Azure PaaS services using a private IP address.\*\*

19. \*\*B) Application rule collection\*\*

20. \*\*A) To ensure higher availability for the VPN/ExpressRoute gateway.\*\*