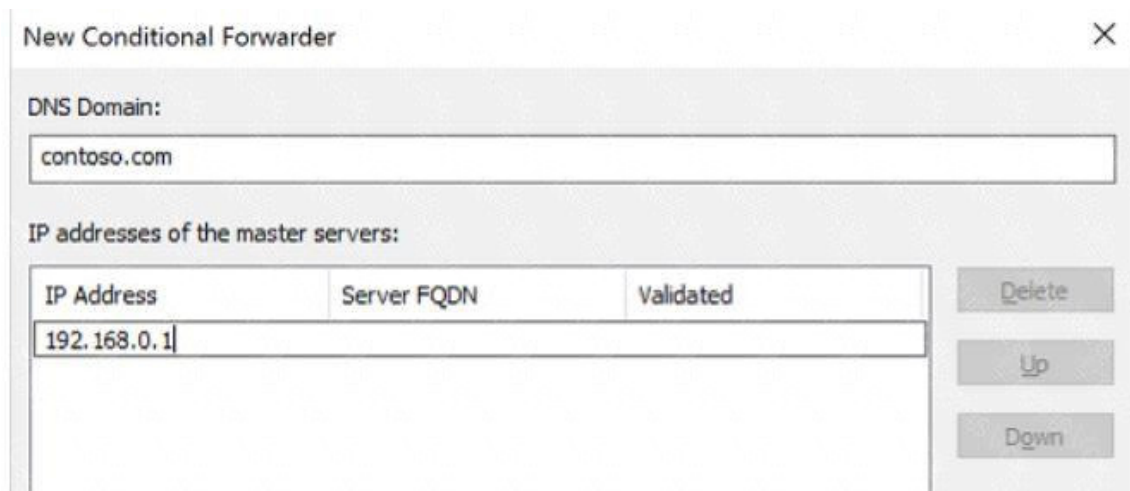**Explanation:**
An Azure AD DS DNS zone should only contain the zone and records for the managed domain itself.

A conditional forwarder is a configuration option in a DNS server that lets you define a DNS domain, such as contoso.com, to forward queries to. Instead of the local DNS server trying to resolve queries for records in that domain, DNS queries are forwarded to the configured DNS for that domain. This configuration makes sure that the correct DNS records are returned, as you don't create a local a DNS zone with duplicate records in the managed domain to reflect those resources.

To create a conditional forwarder in your managed domain, complete the following steps:

1. Select your DNS zone, such as aaddscontoso.com.
2. Select Conditional Forwarders, then right-select and choose New Conditional Forwarder...
3. Enter your other DNS Domain, such as contoso.com, then enter the IP addresses of the DNS servers for that namespace, as shown in the following example:

4. Check the box for Store this conditional forwarder in Active Directory, and replicate it as follows, then select the option for All DNS servers in this domain, as shown in the following example:

5. To create the conditional forwarder, select OK.

Name resolution of the resources in other namespaces from VMs connected to the managed domain should now resolve correctly. Queries for the DNS domain configured in the conditional forwarder are passed to the relevant DNS servers.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/manage-dns

QUESTION 63
You have an Azure subscription.

Users access the resources in the subscription from either home or from customer sites. From home, users must establish a point-to-site VPN to access the Azure resources. The users on the customer sites access the Azure resources by using site-to-site VPNs.

You have a line-of-business app named App1 that runs on several Azure virtual machine. The virtual machines run Windows Server 2016.

You need to ensure that the connections to App1 are spread across all the virtual machines.

What are two possible Azure services that you can use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A.   a public load balancer
B.   Traffic Manager
C.   an Azure Content Delivery Network (CDN)
D.   an internal load balancer
E.   an Azure Application Gateway

Correct Answer: DE
Explanation:
Line-of-business apps means custom apps. Generally these are used by internal staff members of the company.

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Internal Load Balancer provides a higher level of availability and scale by spreading incoming requests across virtual machines (VMs) within the virtual network.

Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview
https://docs.microsoft.com/en-us/azure/application-gateway/overview

QUESTION 64
DRAG DROP
You have an Azure subscription. The subscription includes a virtual network named VNet1. Currently, VNet1 does not contain any subnets.

You plan to create subnets on VNet1 and to use application security groups to restrict the traffic between the subnets. You need to create the application security groups and to assign them to the subnets.

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

Cmdlets	Answer Area
New-AzureRmVirtualNetwork	
New-AzureRmNetworkSecurityGroup	
New-AzureRmApplicationSecurityGroup	
New-AzureRmNetworkSecurityRuleConfig	
Add-AzureRmVirtualNetworkSubnetConfig	

Correct Answer:

Cmdlets

New-AzureRmVirtualNetwork
New-AzureRmNetworkSecurityGroup
New-AzureRmApplicationSecurityGroup
New-AzureRmNetworkSecurityRuleConfig
Add-AzureRmVirtualNetworkSubnetConfig

Answer Area

New-AzureRmNetworkSecurityRuleConfig
New-AzureRmNetworkSecurityGroup
Add-AzureRmVirtualNetworkSubnetConfig
New-AzureRmVirtualNetwork

QUESTION 65
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 that has a subnet named Subnet1
▪ Two network security groups (NSGs) named NSG-VM1 and NSG-Subnet1
▪ A virtual machine named VM1 that has the required Windows Server configurations to allow
    Remote Desktop connections

NSG-Subnet1 has the default inbound security rules only.

NSG-VM1 has the default inbound security rules and the following custom inbound security rule:

▪ Priority: 100
▪ Source: Any
▪ Source port range: *
▪ Destination: *
▪ Destination port range: 3389
▪ Protocol: UDP
▪ Action: Allow

VM1 connects to Subnet1. NSG1-VM1 is associated to the network interface of VM1. NSG-Subnet1 is associated to Subnet1.

You need to be able to establish Remote Desktop connections from the internet to VM1.

Solution: You add an inbound security rule to NSG-Subnet1 and NSG-VM1 that allows connections from the internet source to the VirtualNetwork destination for port range 3389 and uses the TCP protocol.

Does this meet the goal?

A.   Yes
B.   No

Correct Answer: A

Explanation:
The default port for RDP is TCP port 3389. A rule to permit RDP traffic must be created automatically when you create your VM.

Note on NSG-Subnet1: Azure routes network traffic between all subnets in a virtual network, by default.

References:
https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-connection

QUESTION 66
HOTSPOT
You have an Azure subscription named Sub1.

You plan to deploy a multi-tiered application that will contain the tiers shown in the following table.

Tier	Accessible from the Internet	Number of virtual machines
Front-end web server	Yes	10
Business logic	No	100
Microsoft SQL Server database	No	5

You need to recommend a networking solution to meet the following requirements:

▪ Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines.
▪ Protect the web servers from SQL injection attacks.

Which Azure resource should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Ensure that communication between the web servers and the business logic tier spreads equally across the virtual machines:

- an application gateway that uses the Standard tier
- an application gateway that uses the WAF tier
- an internal load balancer
- a network security group (NSG)
- a public load balancer

Protect the web servers from SQL injection attacks:

- an application gateway that uses the Standard tier
- an application gateway that uses the WAF tier
- an internal load balancer
- a network security group (NSG)
- a public load balancer