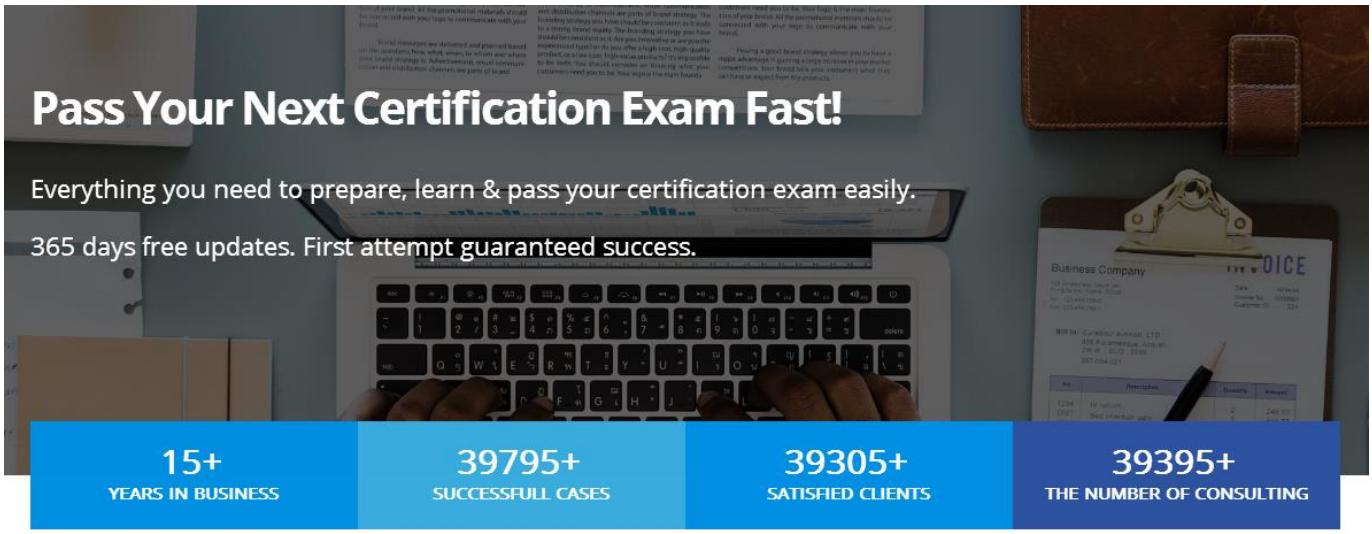
PracticeVCE



TRY BEFORE YOU BUY

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

http://www.practicevce.com

Professional Study Tool and Reliable Exam Practice Material

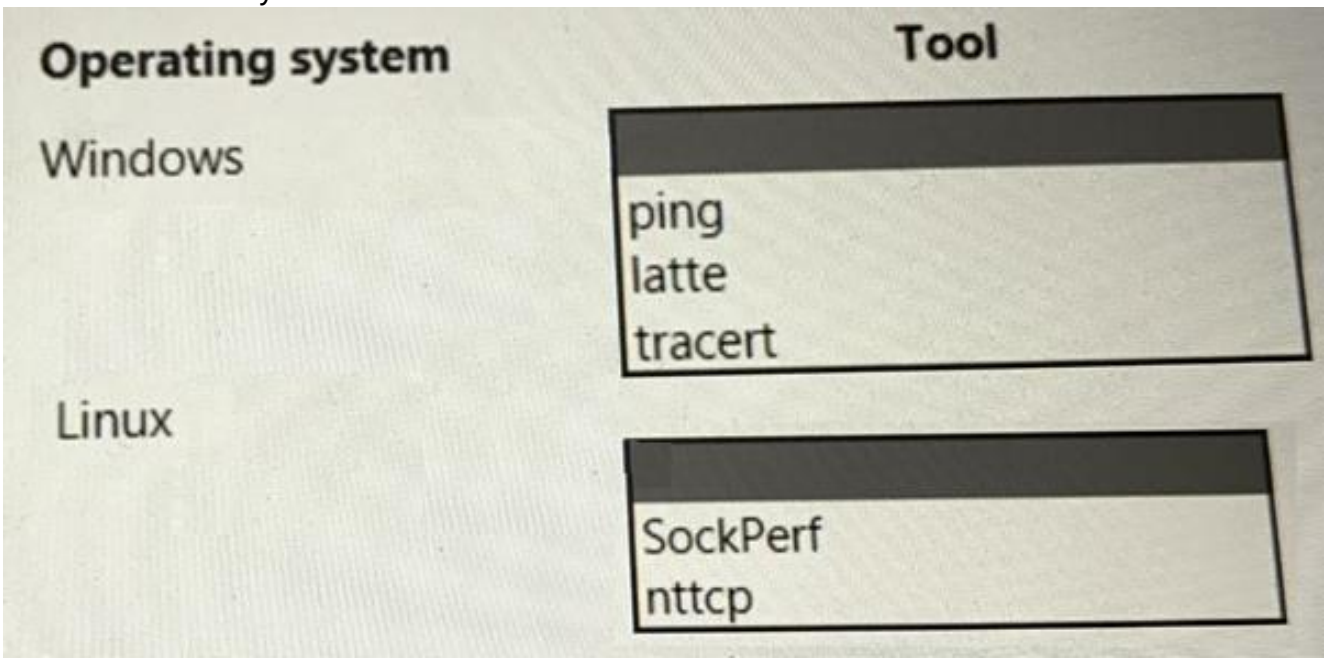
Exam : **AZ-720**

Title : Troubleshooting Microsoft Azure Connectivity

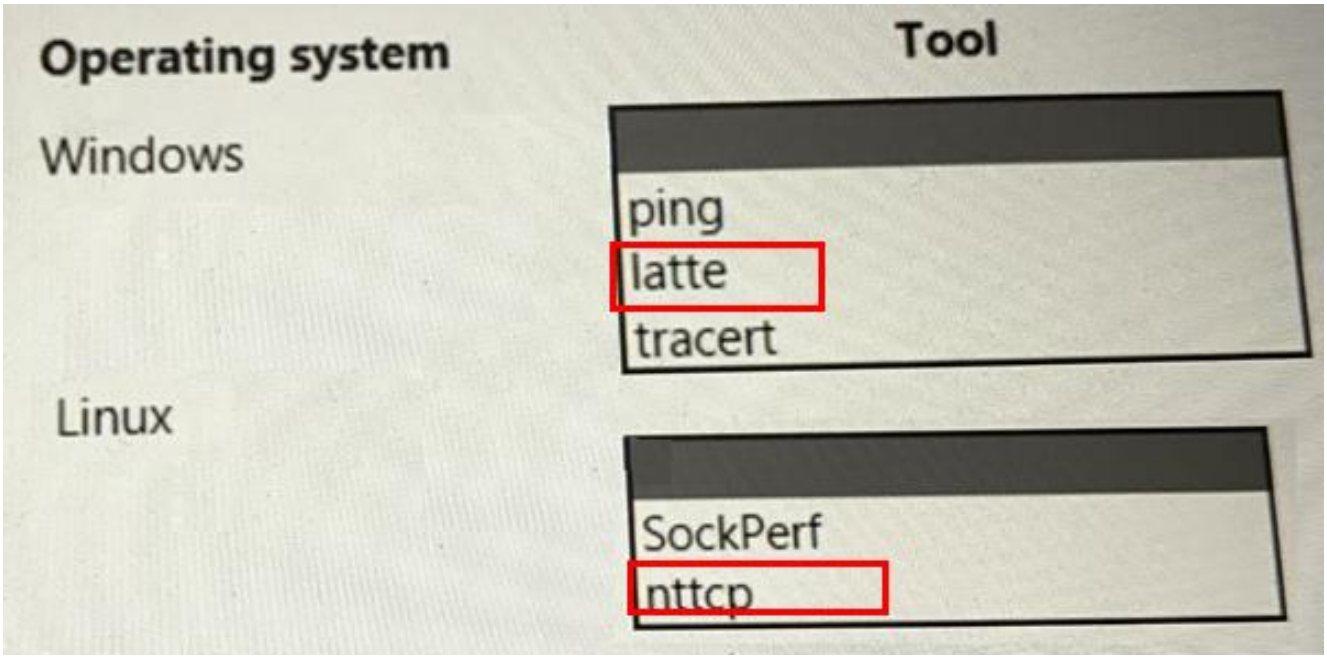
Vendor : Microsoft

Version : DEMO

NO.1 A company implements Windows and Linux VMs in an Azure Virtual Network. The company plans to apply routing changes to the virtual network.
You need to determine the impact of these changes on network latency affecting applications that use TCP and UDP traffic. The solution must provide the highest level of accuracy.
Which tools should you use?



Answer:



Topic 1, Fabrikam Inc.
VM3
Users report issues connecting from VM3 to resources at Margie's Travel. The administrator for Margie's Travel has verified that their VPN gateway is working correctly. You must verify whether the Fabrikam virtual network gateway is available.
VM10
All ping tests bust be performed by using the ICMP protocol. You are unable to ping VM10 from VM1
Alpine Ski House You discover during testing that scheduling agents are experiencing latency when

accessing resources at the Alpine Ski House. You suspect that the issue is related to ICMP latency.
Contoso Suites
You receive reports that VM1 is unable to access resources at Contoso Suites Blue Yonder Airlines
The administrator of a partner company named Blue Yonder Airlines reports VPN disconnections and IPsec failure to connect errors.
Other resource issues
* MFA requests on SRV2 are failing with a security token error.
* You are unable to ping VM10 from VM1.
Admin1
You receive the following error on SRV1 only when trying to synchronize an administrator named Admin1: 8344 insufficient access rights to perform the operation Admin2 An administrator named Admin2 reports they cannot connect to the web server public IP address on VM4 from VM2.
Agent 1
A scheduling agent named Agent1 reports issues authenticating to Azure AD.
Used 1
A scheduling agent named User1 reports that they can access the internet when connected to the point-to-site VPN.
User2
A user named User2 reports the following error when registering for SSPR: Your administrator has not enabled you to use this feature.
Sales team
Sales team employees report that they are unable to connect by using point-to-site VPN.

NO.2 A company has virtual machines (VMs) in the following Azure regions:
West Central US
Australia East
The company uses ExpressRoute private peering to provide connectivity to VMs hosted on each region and on-premises services.
The company implements global VNet peering between a VNet in each region. After configuring VNet peering, VM traffic attempts to use ExpressRoute private peering.
You need to ensure that traffic uses global VNet peering instead of ExpressRoute private peering. The solution must preserve existing on-premises connectivity to Azure VNets.
What should you do?

A. Add a user-defined route to the subnets route table.

B. Add a filter to the on-premises routers.

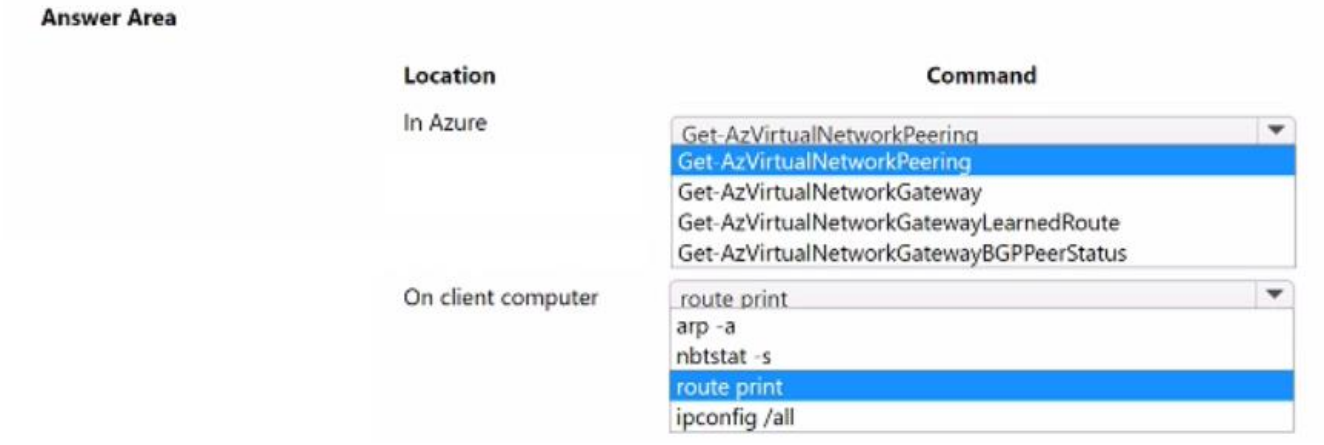
C. Add a second VNet to the virtual machines and configure VNet peering between the VNets.

D. Disable the ExpressRoute peering connections for one of the regions.

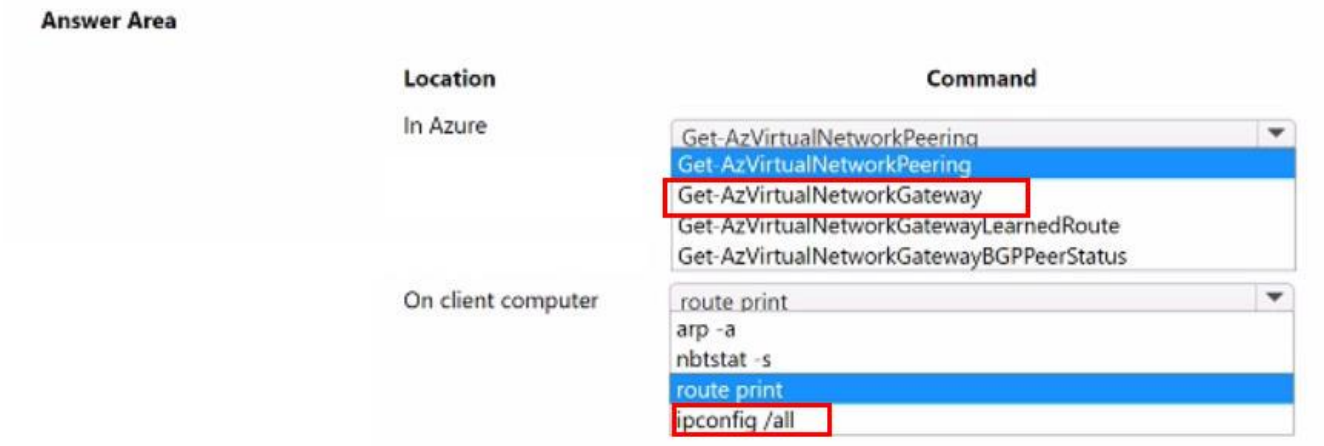
Answer: A
Explanation:
To ensure that traffic uses global VNet peering instead of ExpressRoute private peering, you should add a user-defined route to the subnets route table. According to 2, global VNet peering allows virtual networks across regions to communicate using private IP addresses as if they were in the same region. However, if there is an existing ExpressRoute private peering between two regions that also have global VNet peering enabled, traffic will prefer ExpressRoute over global VNet peering by default. To override this behavior and force traffic to use global VNet peering instead of ExpressRoute private peering for a specific subnet or virtual network gateway connection, you need to add a user-

defined route with a next hop type of Virtual Network Peering.

NO.3 You need to troubleshoot the issues reported by User1.
Which commands should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NO.4 A company enables just-in-time (JIT) virtual machine (VM) access in Azure.
An administrator observes a list of VMs on the Unsupported tab of the JIT VM access page in the Microsoft Defender for Cloud portal.
You need to determine why some VMs are not supported for JIT VM access.
What should you conclude?

A. The administrator is using the Microsoft Defender for Cloud free tier.

B. The VMs were provisioned by using a classic deployment.

C. The VMs were recently provisioned by using an Azure Resource Manager deployment.

D. The administrator does not have the SecurityReader role.

Answer: B

Explanation:
The Unsupported tab on the Just-in-Time VM access page in the Microsoft Defender for Cloud portal indicates that the VMs were provisioned by using a classic deployment Classic deployments were used in Azure before the deployment model was updated to Azure Resource Manager, which is now the preferred model for deploying and managing resources in Azure.

NO.5 A company connects their on-premises network by using Azure VPN Gateway. The on-premises

environment includes three VPN devices that separately tunnel to the gateway by using Border Gateway Protocol (BGP).
A new subnet should be unreachable from the on-premises network.
You need to implement a solution.
Solution: Disable peering on the virtual network.
Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:
Disabling peering on the virtual network will not prevent the on-premises network from reaching the new subnet. Virtual network peering is a way to connect virtual networks and allows resources in both virtual networks to communicate with each other securely. It does not affect connectivity between on-premises and virtual network resources.
A better solution would be to create a network security group (NSG) and associate it with the new subnet. The NSG can be configured to deny traffic from the on-premises network to the new subnet. This way, the new subnet will be isolated from the on-premises network.
Reference:
Azure Virtual Network peering: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview Azure Network Security Groups: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

NO.6 A company uses Active Directory Federation Services {AD FS) to authenticate users to Azure AD. Users report receiving a certificate warning after the company updates the AD FS certificate.
You need to ensure users can sign in to Azure AD. Which PowerShell cmdlet should you use?

A. Redo-MsolProvisionUser

B. Convert-MsolDomaInToFederated

C. Set-MsolOomaInFederatIonSettings

D. Confirm-MsolDomain

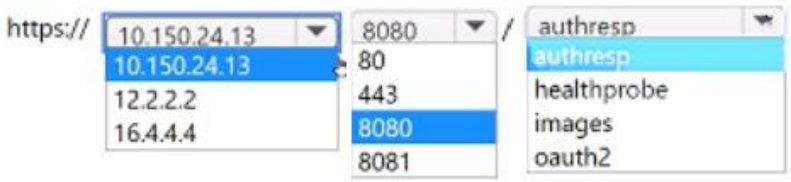
E. Update-MSOLFederatedDosain

Answer: E

Explanation:
Redo-MsolProvisionUser cmdlet retries the provisioning of a user object in Azure AD that previously failed or was canceled2.
Convert-MsolDomainToFederated cmdlet converts a standard domain to a federated domain3.
Set-MsolDomainFederationSettings cmdlet modifies the settings of an existing federated domain4.
Confirm-MsolDomain cmdlet confirms ownership of a domain after it has been added to Azure AD.
1: Update-MSOLFederatedDomain (MSOnline) 2: Redo-MsolProvisionUser (MSOnline) 3: Convert-MsolDomainToFederated (MSOnline) 4: Set-MsolDomainFederationSettings (MSOnline) : [Confirm-MsolDomain (MSOnline)]

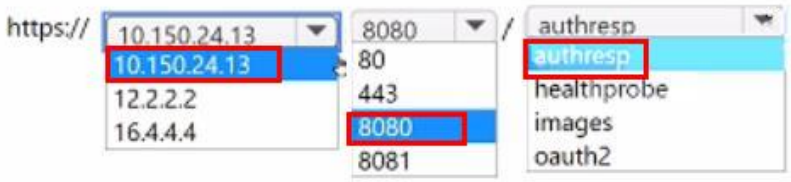
NO.7 You need to troubleshoot the issues related to VM3.
How should you complete the web link? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



NO.8 A company has an Azure tenant. The company deploys an Azure Firewall named FW1 using the Standard SKU. You configure FW1 using classic firewall rules.
The company creates an application rule collection with the following settings:
Priority: 100
Action: Deny
Rule type: FQDN
Source type: IP address
Source: *
Protocol: http:80,https:443
Target FQDN: *.cloud.contoso.com
An engineer observes that traffic to console.cloud.conotoso.com is still allowed by FW1.
You need to determine why the traffic is allowed.
What should you review?

A. Network rules

B. Web categories

C. Infrastructure rules

D. Application rules

Answer: A

Explanation:
To determine why the traffic is allowed, you should review network rules. According to 3, Azure Firewall uses network rules to allow or deny traffic based on source and destination IP address, port, and protocol. Network rules are applied before application rules and have higher priority than application rules. Therefore, if there is a network rule that allows traffic to

console.cloud.contoso.com on port 80 or 443, it will override the application rule that denies traffic based on FQDN.

NO.9 A company configures an Azure site-to-site VPN between an on-premises network and an Azure virtual network.
The company reports that after completing the configuration, the VPN connection cannot be established.
You need to troubleshoot the connection issue.
What should you do first?

A. Identify the shared key by running this PowerShell cmdlet: Get-AzVirtualNetworkGatewayConnectionSharedKey.

B. Identify the shared key by running this PowerShell cmdlet: Get-AzVirtualNetworkGatewayConnectionVpnDeviceConfigScript.

C. Verify the AzureRoot.cer file exists.

D. Verify the AzureClient.pfx file exists.

Answer: A

Explanation:
To troubleshoot the connection issue, you should do first identify the shared key by running this PowerShell cmdlet: Get-AzVirtualNetworkGatewayConnectionSharedKey. According to 1, this cmdlet returns the shared key that is used for authentication between an Azure virtual network gateway and a local network gateway. You can use this cmdlet to verify that the shared key matches on both sides of the VPN connection.
Therefore, you should choose A. Identify the shared key by running this PowerShell cmdlet: Get-AzVirtualNetworkGatewayConnectionSharedKey.

NO.10 A company deploys Azure Traffic Manager load balancing for an Azure App Service solution.
Load balancing performance is showing a degraded status after deployment, and new HTTPS probes are failing to reach the Traffic Manager endpoints.
You need to troubleshoot the probe failure.
How should you complete the PowerShell script?

Answer Area

```
add-type @"
using System.Net;
using System.Security.Cryptography.X509Certificates;
public class TrustAllCertsPolicy : [ICertificatePolicy / ICerfificateAuthority / ICertProperty] {
    public bool CheckValidationResult(
    ServicePoint srvPoint, X509Certificate certificate,
    WebRequest request, int certificateProblem) {
    return [true / false];
    }
}
"@
[System.Net.ServicePointManager]:: [ICertificatePolicy / CertificatePolicy / IEncryptionPolicy / EncryptionPolicy] New-Object TrustAllCertsPolicy
```

Answer:

Answer Area

```
add-type @"
using System.Net;
using System.Security.Cryptography.X509Certificates;
public class TrustAllCertsPolicy : [ICertificatePolicy / ICerfificateAuthority / ICertProperty] {
    public bool CheckValidationResult(
    ServicePoint srvPoint, X509Certificate certificate,
    WebRequest request, int certificateProblem) {
    return [true / false];
    }
}
"@
[System.Net.ServicePointManager]:: [ICertificatePolicy / CertificatePolicy / IEncryptionPolicy / EncryptionPolicy] New-Object TrustAllCertsPolicy
```

NO.11 A company migrates existing Ubuntu Linux servers from their on-premises vSphere infrastructure to Azure.
The virtual machines (VMs) are experiencing a low network throughput of 20 Mbps. The VMs are expected to sustain 300 Mbps.

You need to ensure that the VMs are compatible with Azure.
Which change should you make?

A. Install a kernel name that ends with -azure.

B. Configure the network interfaces to 1000 Mbps/full duplex.

C. Redeploy the VM with Accelerated Networking enabled.

D. Increase the TCP buffers and window size kernel parameters.

Answer: C

Explanation:
To ensure that Ubuntu Linux servers are compatible with Azure and to increase network throughput from 20 Mbps to 300 Mbps, you should redeploy the VM with Accelerated Networking enabled. Therefore, option C is correct. You should redeploy the VM with Accelerated Networking enabled.

NO.12 A company connects their on-premises network by using Azure VPN Gateway. The on-premises environment includes three VPN devices that separately tunnel to the gateway by using Border Gateway Protocol (BGP).
A new subnet should be unreachable from the on-premises network.
You need to implement a solution.
Solution: Configure subnet delegation.
Does the solution meet the goal?

A. Yes

B. No

Answer: B

Explanation:
The proposed solution, which is to configure subnet delegation, does not meet the goal of making the new subnet unreachable from the on-premises network. Subnet delegation is a mechanism to delegate management of a subnet to another resource such as a Network Virtual Appliance or a Service Endpoint. It does not provide any means to restrict or isolate a subnet from the rest of the network.
To meet the goal, you can use Network Security Groups (NSGs) to restrict traffic to and from the new subnet. NSGs allow you to define inbound and outbound security rules that specify the type of traffic that is allowed or denied based on different criteria such as source or destination IP address, protocol, port number, etc. By creating a custom NSG and defining rules that deny traffic to and from the new subnet, you can effectively make that subnet unreachable from the on-premises network.
Therefore, the correct answer is option B, "No".
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview