ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Topic 1, Litware. Inc Case Study 1

Overview

Litware. Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment:

Hybrid Environment

The on-prernises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by usinq Azure AD Connect.

All the offices connect to a virtual network named Vnetl by using a Site-to-Site VPN connection.

Azure Environment

Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant.

Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	**None**
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3.

Currently, Vnet2 and Vnet3 cannot communicate directly.

Requirements:

Business Requirements

Litware wants to minimize costs whenever possible, as long as all other requirements are met.

Virtual Networking Requirements

Litware identifies the following virtual networking requirements:

* Direct the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit.
* Ensure that the records in the cloud.litwareinc.com zone can be resolved from the on-premises locations.
* Automatically register the DNS names of Azure virtual machines to the cloud.litwareinc.com zone.
* Minimize the size of the subnets allocated to platform-managed services.
* Allow traffic from VMScaleSet1 to VMScaleSet2 on the TCP port 443 only.

Hybrid Networking Requirements

Litware identifies the following hybrid networking requirements:

* Users must be able to connect to Vnet1 by using a Point-to-Site (P2S) VPN when working remotely.
Connections must be authenticated by Azure AD.
* Latency of the traffic between the Boston datacenter and all the virtual networks must be minimized.

* The Boston datacenter must connect to the Azure virtual networks by using an ExpressRoute FastPath connection.
* Traffic between Vnet2 and Vnet3 must be routed through Vnet1.

PaaS Networking Requirements

Litware identifies the following networking requirements for platform as a service (PaaS):

* The storage1 account must be accessible from all on-premises locations without exposing the public endpoint of storage1.
* The storage2 account must be accessible from Vnet2 and Vnet3 without exposing the public endpoint of storage2.

Question: 1

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 peerings from Vnet2 and Vnet3, select Use remote gateways.
B. On the peering from Vnet1, select Allow forwarded traffic.
C. On the peering from Vnet1, select Use remote gateways.
D. On the peering from Vnet1, select Allow gateway transit.
E. On the peerings from Vnet2 and Vnet3, select Allow gateway transit.

Answer: BD

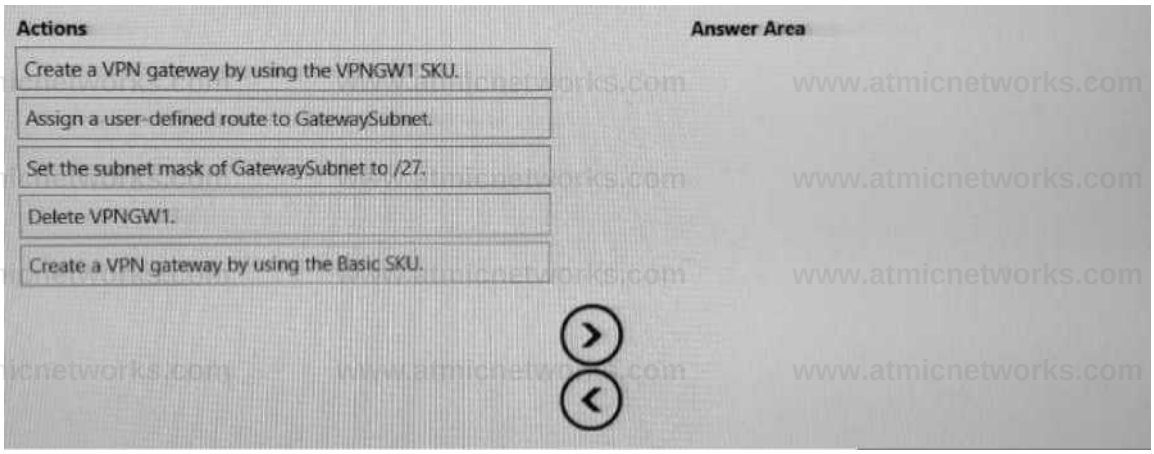
Explanation:

Question: 2

DRAG DROP

You need to prepare Vnet1 for the deployment of an ExpressRoute gateway. The solution must meet the hybrid connectivity requirements and the business requirements.

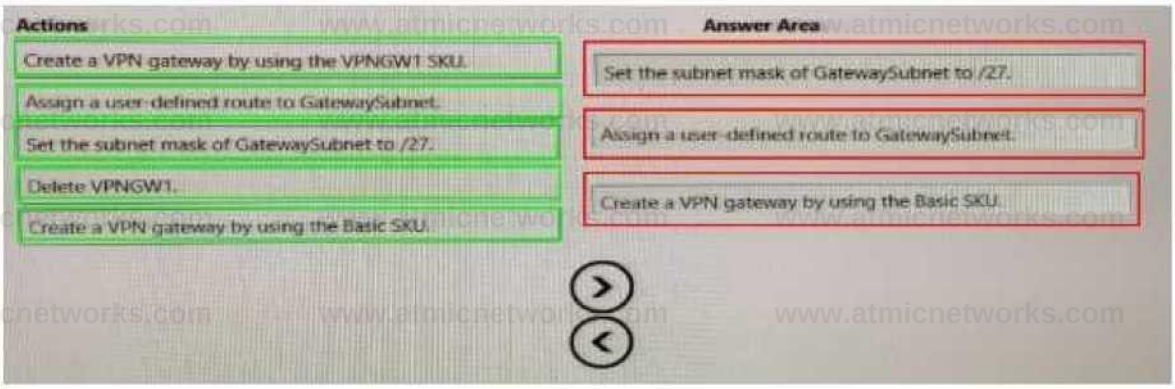
Which three actions should you perform in sequence for Vnet1? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct



Answer:

Explanation:

Answer:

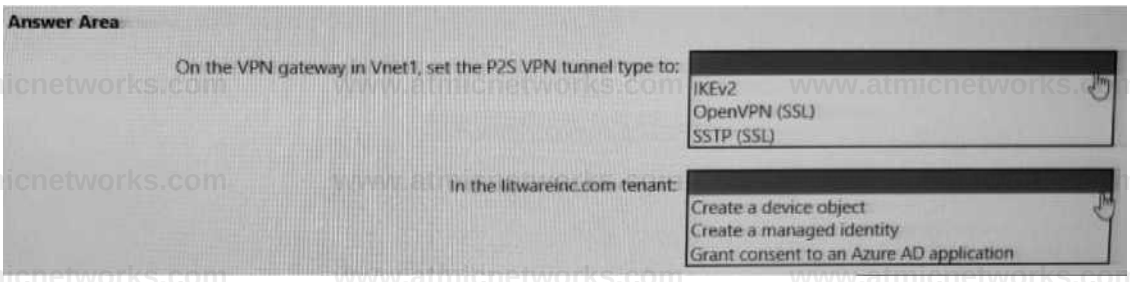


Question: 3

HOTSPOT

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one



Explanation:

You need to implement a P2S VPN for the users in the branch office. The solution must meet the hybrid networking requirements.

Answer:

On the VPN gateway in Vnetl, set the P2S VPN tunnel type to:

IKEv2
OpenVPN (SSL) SSTP (SSL)

In the litwareinc.com tenant:

Create a device object
Create a managed identity
Grant consent to an Azure AD application

Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant

Question: 4

You need to provide connectivity to storage1. The solution must meet the PaaS networking requirements and the business requirements.

What should you include in the solution?

A. a service endpoint
B. Azure Front Door
C. a private endpoint
D. Azure Traffic Manager

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints- overview

Question: 5

HOTSPOT

You need to recommend a configuration for the ExpressRoute connection from the Boston datacenter. The solution must meet the hybrid networking requirements and business requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Set the ExpressRoute gateway type to:

High Performance (ERGw2AZ)
Standard Performance (ERGwlAZ)
Ultra Performance (ERGw3AZ)

To minimize latency of traffic to Vnet2:

Create a dedicated ExpressRoute circuit for Vnet2
Connect Vnet2 directly to the ExpressRoute circuit
Configure gateway transit for the peering between Vnet! and Vnet2

Answer:

Explanation:

Set the ExpressRoute gateway type to: ▼

High Performance (ERGw2AZ)
Standard Performance (ERGwIAZ)
Ultra Performance (ERGwSAZ)

To minimize latency of traffic to Vnet2; 1

Create a dedicated ExpressRoute circuit for VnetZ Connect Vnet2 directly to the ExpressRoute circuit Configure gateway transit for the peering between Vnet! and Vnet2

For the first question, only ExpressRoute GW SKU Ultra Performance support FastPath feature.
For the second question, vnet1 will connect to ExpressRoute gw, once Vnet1 peers with Vnet2, the traffic from on-premise network will bypass GW and Vnet1, directly goes to Vnet2, while this feature is under public preview.

====Reference

ExpressRoute virtual network gateway is designed to exchange network routes and route network traffic. FastPath is designed to improve the data path performance between your on-premises network and your virtual network. When enabled, FastPath sends network traffic directly to virtual machines in the virtual network, bypassing the gateway.

To configure FastPath, the virtual network gateway must be either:
Ultra Performance
ErGw3AZ

VNet Peering - FastPath will send traffic directly to any VM deployed in a virtual network peered to the one connected to ExpressRoute, bypassing the ExpressRoute virtual network gateway.

https://docs.microsoft.com/en-us/azure/expressroute/about-fastpath

Gateway SKU
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways

Question: 6

DRAG DROP

You need to implement outbound connectivity for VMScaleSet1. The solution must meet the virtual networking requirements and the business requirements.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Create a health probe

Create a public load balancer in the Standard SKU

Create a public load balancer in the Basic SKU ^^

Create a backend pool that contains VMScaleSetl

Create a NAT rule

—

Create an outbound rule

Answer:

Explanation:

Create a public load balancer in the Standard SKU

Create a backend pool that contains VMScaleSetl

’ Create an outbound rule

Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/skus

https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections#outboundrules

Question: 7

You need to configure the default route in Vnet2 and Vnet3. The solution must meet the virtual networking requirements.

What should you use to configure the default route?

A. a user-defined route assigned to GatewaySubnet in Vnet2 and Vnet3

B. a user-defined route assigned to GatewaySubnet in Vnet1
C. BGP route exchange
D. route filters

Answer: C

Explanation:
VNet 1 will get the default from BGP and propagate it to VNET 2 and 3

Question: 8

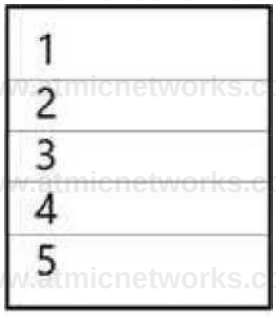
HOTSPOT

You need to restrict traffic from VMScaleSet1 to VMScaleSet2. The solution must meet the virtual networking requirements.

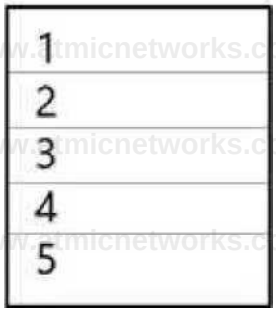
What is the minimum number of custom NSG rules and NSG assignments required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Minimum number of custom NSG rules:



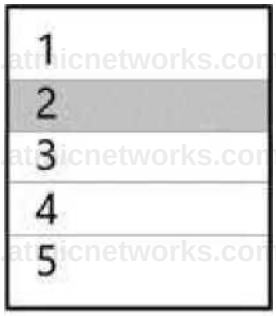
Minimum number of NSG assignments:



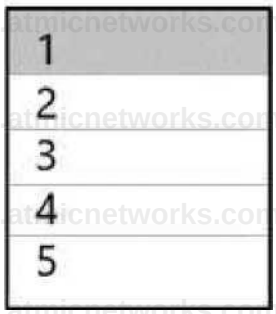
Answer:

Explanation:

Minimum number of custom NSG rules:



Minimum number of NSG assignments:



Box 2: One NSG

The minimum requirement is one NSG. You could attach the NSG to VMScaleSet1 and restrict outbound traffic, or you could attach the NSG to VMScaleSet2 and restrict inbound traffic. Either way you would need two custom NSG rules.

Box 1: Two custom rules

With the NSG attached to VMScaleSet2, you would need to create a custom rule blocking all traffic from VMScaleSet1. Then you would need to create another custom rule with a higher priority than the first rule that allows traffic on port 443.

The default rules in the NSG will allow all other traffic to VMScaleSet2.

Question: 9

HOTSPOT

You need to implement name resolution for the cloud.liwareinc.com. The solution must meet the networking requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To implement name resolution of the cloud.litwareinc.com DNS records from the on-premises locations:

Enable the Azure Firewall DNS proxy
Create SRV records in cloud.litwareinc.com
Deploy an Azure virtual machine configured as a DNS server to Vnet!

To implement automatic DNS name registration in cloud.litwareinc.com:

Create virtual network links
Configure conditional forwarding
Create an SOA record in cloud.litwareinc.com

Answer:

Explanation:

To implement automatic DNS name registration in cloud.litwareinc.com: y

Create virtual network links
Configure conditional forwarding
Create an SOA record in cloud.litwareinc.com

To implement name resolution of the cloud.litwareinc.com DNS records from the on-premises locations: ▼

Enable the Azure Firewall DNS proxy
Create SRV records in cloud.litwareinc.com
Deploy an Azure virtual machine configured as a DNS server to Vnetl

Reference:
https://docs.microsoft.com/en-us/azure/dns/private-dns-autoregistration

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms- and-role-instances

Question: 10

You need to configure the default route on Vnet2 and Vnet3. The solution must meet the virtual networking requirements.

What should you use to configure the default route?

A. route filters
B. BGP route exchange
C. a user-defined route assigned to GatewaySubnet in Vnet1
D. a user-defined route assigned to GatewaySubnet in Vnet2 and Vnet3

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Question: 11

You need to provide access to storage2. The solution must meet the PaaS networking requirements and the business requirements.
Which connectivity method should you use?

A. a service endpoint B. a private endpoint C. Azure Firewall
D. Azure Front Door

Answer: A

Explanation:

Topic 2, Contoso Case Study 2

Overview
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab. note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Existing Environment:

Azure Network Infrastructure

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com.

The Azure subscription contains the virtual networks shown in the following table.

Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	None

Vnet1 contains a virtual network gateway named GW1.

Azure Virtual Machines

The Azure subscription contains virtual machines that run Windows Server 2019 as shown in the following table.

Name	Connected to	Network security group (NSG)
VM1	Vnet1/Subnet1	NSG1
VM2	Vnet1/Subnet2	NSG2
VM3	Vnet2/Default	NSG3
VM4	Vnet3/Default	NSG4
VM5	Vnet4/SubnetA	NSG5

The NSGs are associated to the network interfaces on the virtual machines. Each NSG has one custom security rule that allows RDP connections from the internet. The firewall on each virtual machine allows ICMP traffic.

An application security group named ASG1 is associated to the network interface of VM1. Azure Private DNS Zones

The Azure subscription contains the Azure private DNS zones shown in the following table.

Zone1.contoso.com has the virtual network links shown in the following table.

Name	Virtual network	Auto registration
Link1	Vnet2	No
Link2	Vnet3	Yes

Other Azure Resources

The Azure subscription contains additional resources as shown in the following table.

Name	Type	Location
DB1	Azure SQL Database	West US
storage1	Azure Storage account	West US
Registry1	Azure Container Registry	Central US
KeyVault1	Azure Key Vault	Central US

Name	Location
zone1.contoso.com	Central US
zone2.contoso.com	West US

Requirements:

Virtual Network Requirements

Contoso has the following virtual networks requirements:

* Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:

Two container groups that connect to Vnet6

Three virtual machines that connect to Vnet6

Allow VPN connections to be established to Vnet6

Allow the resources in Vnet6 to access KeyVault1, DB1, and Vnet1 over the Microsoft backbone network

* The virtual machines in Vnet4 and Vnet5 must be able to communicate over the Microsoft backbone network.

* A virtual machine named VM-Analyze will be deployed to Subnet1. VM-Analyze must inspect the outbound network traffic from Subnet2 to the internet.

Network Security Requirements

Contoso has the following network security requirements:

* Configure Azure Active Directory (Azure AD) authentication for Point-to-Site (P2S) VPN users.

* Enable NSG flow logs for NSG3 and NSG4.

* Create an NSG named NSG10 that will be associated to Vnet1/Subnet1 and will have the custom inbound security rules shown in the following table.

* Create an NSG named NSG11 that will be associated to Vnet1/Subnet2 and will have the custom outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

Priority	Port	Protocol	Source	Destination	Action
500	3389	TCP	10.1.0.0/16	Any	Deny
1000	Any	ICMP	10.10.0.0/16	VirtualNetwork	Deny

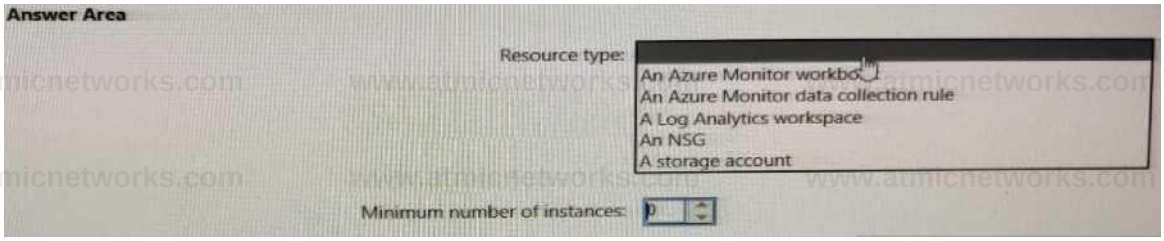
Question: 12

HOTSPOT

You need to meet the network security requirements for the NSG flow logs.

Which type of resource do you need, and how many instances should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

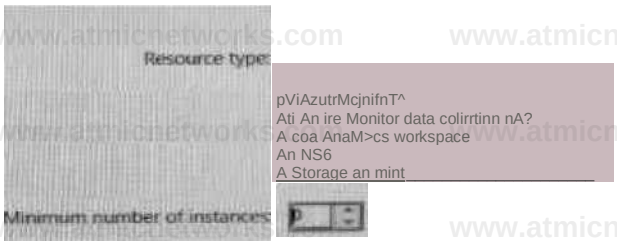


Answer:

Explanation:

Answer:

Answer Area



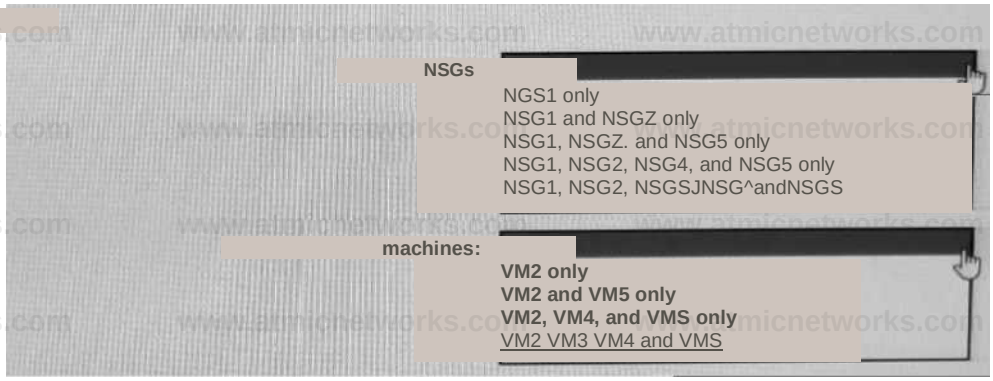
Question: 13

HOTSPOT

In which NSGs can you use ASG1 and to which virtual machine network interfaces can you associate ASG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

NGS1 only

VM2, VM3, VM4 and VM5

Question: 14

HOTSPOT

You are implementing the virtual network requirements for VM Analyze.

What should you include in a custom route that is linked to Subnet2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Address prefix:

- 0.0.0.0/0
- 0.0.0.0/32
- 10.1.0.0/16
- 255.255.255.255/0
- 255.255.255.255/32

Next hop type:

- None
- Internet
- Virtual appliance
- Virtual network
- Virtual network gateway

Explanation:

Answer:

Address prefix:

- 0.0.0.0/0
- 0.0.0.0/32
- 10.1.0.0/16
- 255.255.255.255/0
- 255.255.255.255/32

Next hop type:

- None
- Internet
- Virtual appliance
- Virtual network
- Virtual network gateway

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Question: 15

You are implementing the Virtual network requirements for Vnet6.

What is the minimum number of subnets and service endpoints you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer: 2, 4

Explanation:

Question: 16

What should you implement to meet the virtual network requirements for the virtual machines that connect to Vnet4 and Vnet5?

A. a private endpoint
B. a virtual network peering
C. a private link service
D. a routing table
E. a service endpoint

Answer: B

Explanation:

There is no virtual network peering between VM4's VNet (VNet3) and VM5's VNet (VNet4). To enable the VMs to communicate over the Microsoft backbone network a VNet peering is required between VNet3 and VNet4.

Question: 17

HOTSPOT

You create NSG10 and NSG11 to meet the network security requirements.

For each of the following statements, select Yes it the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

No

subnet1(WM1->NSG1 outbound->NSG10 outbound)->subnet2(NSG1 inbound->NSG11 inbound->VM2)

Yes

NSG10 blocks ICMP from VNet4 (source 10.10.0.0/16) but it is not blocked from VM2λ€™s subnet (VNet1/Subnet2).

No

NSG11 blocks RDP (port TCP 3389) destined for λ€˜VirtualNetworkλ€™. VirtualNetwork is a service tag and means the address space of the virtual network (VNet1) which in this case is 10.1.0.0/16.

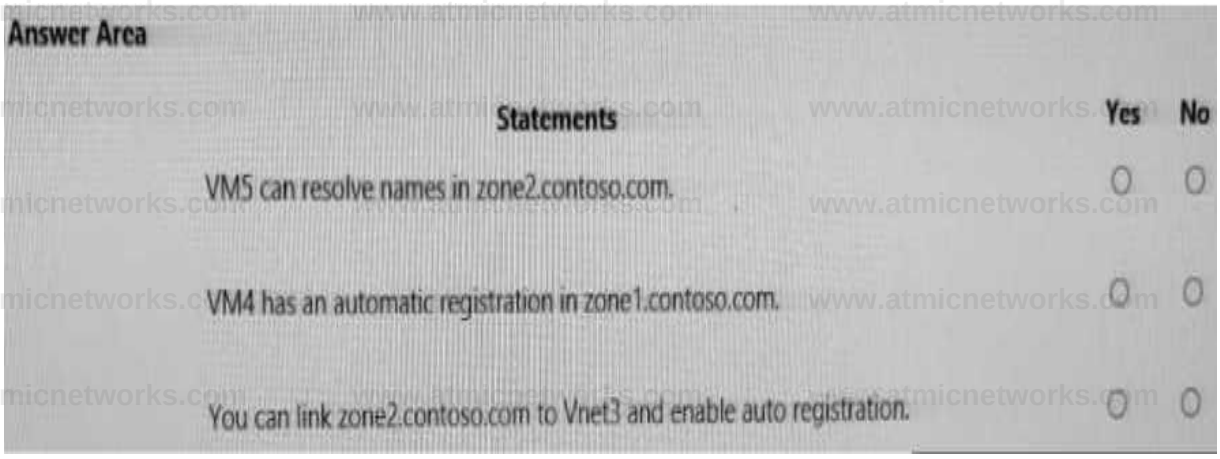
Therefore, RDP traffic from subnet2 to anywhere else in VNet1 is blocked.

Question: 18

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Answer:

Answer:

Answer Area

Statements	V« No
VMS can resolve names in roneZjcnntDso.com.	
VM4 has an autoirMtic registration in zone! cocitow com.	
You can link ZDneZcontoso.com to Vnet3 Mid enable auto registration	

Explanation:

Question: 19

You need to configure GW1 to meet the network security requirements for the P2S VPN users.
Which Tunnel type should you select in the Point-to-site configuration settings of GW1?

A. IKEv2 and OpenVPN (SSL)
B. IKEv2
C. IKEv2 and SSTP (SSL)
D. OpenVPN (SSL)
E. SSTP (SSL)

Answer: D

Explanation:

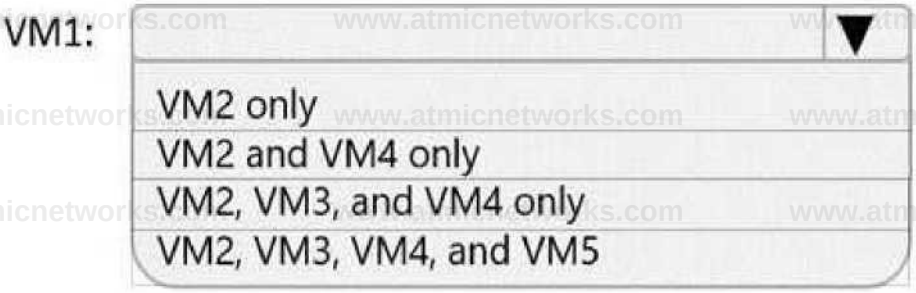
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/openvpn-azure-ad-tenant

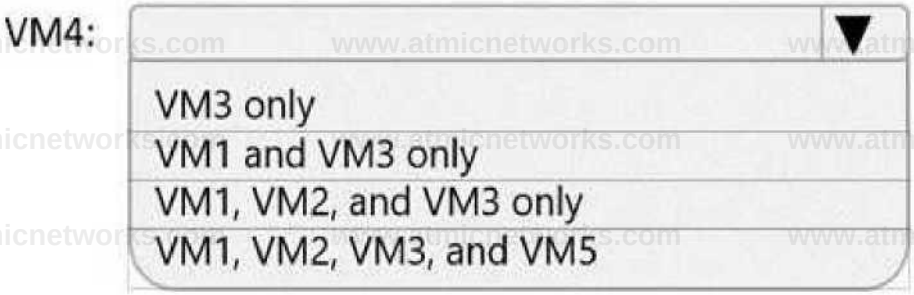
Question: 20

HOTSPOT

Which virtual machines can VM1 and VM4 ping successfully? To answer, select the appropriate options in the answer area.

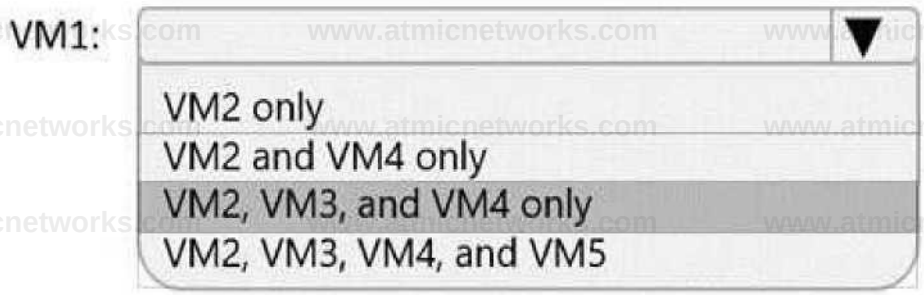
NOTE: Each correct selection is worth one point.

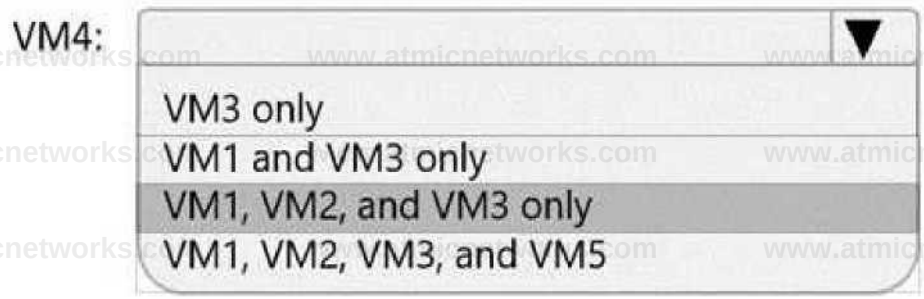




Answer:

Explanation:





Box 1: VM2, VM3 and VM4.

VM1 is in VNet1/Subnet1. VNet1 is peered with VNet2 and VNet3.

There are no NSGs blocking outbound ICMP from VNet1. There are no NSGs blocking inbound ICMP to VNet1/Subnet2, VNet2 or VNet3. Therefore, VM1 can ping VM2 in VNet1/Subnet2, VM3 in VNet2 and VM4 in VNet3.

Box 2:

VM4 is in VNet3. VNet3 is peered with VNet1 and VNet2. There are no NSGs blocking outbound ICMP from VNet3. There are no NSGs blocking inbound ICMP to VNet1/Subnet1, VNet1/Subnet2 or VNet2 from VNet3 (NSG10 blocks inbound ICMP from VNet4 but not from VNet3). Therefore, VM4 can ping VM1 in VNet1/Subnet1, VM2 in VNet1/Subnet2 and VM3 in VNet2.

Question: 21

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	No
Currently, VM5 can resolve names in zone2.contoso.com.	○
VM4 has an automatic registration in zonel.contoso.com.	○
You can link zone2.contoso.com to Vnet3 and enable auto registration.	○

Answer:

Explanation:

Statements	Yes	No
Currently, VM5 can resolve names in zone2.contoso.com.	○	●
VM4 has an automatic registration in zone1.contoso.com.	●	○
You can link zone2.contoso.com to Vnet3 and enable auto registration.	○	●

Box 1: No

Zone2.contoso.com is not linked to any virtual networks. Therefore, no VMs are able to resolve names in the zone.

Box 2: Yes

VM4 is in VNet3. Zone1.contoso.com has a link to VNet3 and auto-registration is enabled on the link.

Box3: No

VNet3 is linked to zone1.contoso.com and auto-registration is enabled on the link. A virtual network can only have one registration zone. You can link zone2.contoso.com to VNet3 but you won't be able to enable auto-registration on the link.

Topic 3, Proseware. Inc

Overview

Existing Environment

Proseware. Inc. is a financial services company that has a main office in New York City and a branch office in San Francisco.

Hybrid Environment

Proseware has an on-premises Active Directory Domain Services (AD DS) forest named corp.proseware.com that syncs with a Microsoft Entra tenant named proseware.com.

Proseware has an Azure subscription that is linked to proseware.com.

Proseware has an internal certification authority (CA).

Network infrashtructure

The offices contain the resources shown in the following table.

NYCNet connects to Azure by using an ExptessRoute circuit.

SFONet connects to Azure by using a Site to-Site (S2S) VPN.

The Azure subscriotion contains the virtual networks and subnets shown in the followina table.

Name	Type	Location	Description
HubVNet	Virtual network	East US Azure region	IP address space of 10 0 0.0/20 peered to SpokeVNet
SpokeVNet	Virtual network	East US Azure region	IP address space of 10.0.16.0/20 peered to HubVNet
VPNGW1	Virtual network gateway	HubVNet	Active-passive resiliency, in the Generation 2, VpnGw3 SKU that has the default ASN connected to SFONet
SUBNET PE	Subnet	HubVNet	Used for private endpoints
SUBNET JUMPHOSTS	Subnet	HubVNet	Used for jump hosts
SUBNET-APPGW1	Subnet	SpokeVNet	Contains an Azure application gateway named AP PG W1

The subscription contains four virtual machines named VM1, VM2, VM3, and VM4. VM1 and VM2 host an app named App1.

VM3 and VM4 host a web app named App2 that is accessed by using a FQDN of app2.proseware.com. Users access app2.proseware.com by using HTTP or HTTPS.

VM1, VM2, and VM4 are connected to SpokeVNet

The subscription contains Application Gateway resources shown in the following table.

Name	Type	Location	Description
APPGW1	Application Gateway	SpokeVNet	In the Azure Web Application Firewall (WAF) V2 SKU Terminates HTTPS connections to a backend pool that contains VMS and VM4
APPGW1-NSG1	Network security group (NSG)	East US region	Associated with SUBNET-APPGW1
APPGW1 WAFPolicy	Azure Web Application Firewall (WAF) policy	East US region	Applied to APPGW1

The subscription contains an Azure Front Door Standard profile named FD1. FD1 contains a single origin group that targets APPGW1 by using the default endpoint name.

HubVNet connects to NYCNet by using an ExpressRoute gateway named ERGW1.

The subscription contains an Azure Private DNS zone named DNSZonel in the East US region.

DNSZonel hosts a namespace of azure.piosewaie.com and is linked to HubVNet

The subscription contains a Standard Azure load balancer named LBS1 in the East US region. LBS1 contains a backend pool that hosts VM1 and VM2.

Planned Changes

Proseware plans to implement the following changes:

- Deploy an Azure Private DNS Resolver named PRDNSl to HubVNet and link PRDNS1 to SpokeVNet.
- Create a DNS forwarding ruleset named DNSRS1 and associate DNSRS1 with PRDNSl
- Deploy Azure Virtual Network Manager and implement the following rules:

o Allow inbound connections on TCP port 3389 from the on-premises networks to SU8NET-JUMPHOSTS. o Block inbound connections on TCP poit 80 from the internet to SpokeVNet.

- Ensure that Azure Virtual Network Manager rules take precedence over conflicting NSG rules.
- Deploy two network virtual appliances (NVAs) named NVA1 and NVA2 to HubVNet.
- Deploy a gateway load balancer named L8GW1 to HubVNet.
- Configure LBGW1 to inspect traffic on TCP ports 443, 1433, and 1434 from LBS1 by using NVA1 and NVA2.
- Ensure that all the traffic to App2 is processed by using FD1.

Connectivity Requirements

Proseware identifies the following connectivity requirements:

- Minimize the complexity of the Azure Virtual Network Manager deployment.
- Route traffic between NYCNet and SFONet via the ExpressRoute circuit and the S2S VPN
- Ensure that remote users on Windows 11 devices can connect to HubVNet by using a Point-to-Site (P2S) VP and their proseware.com credentials.

Security Requirements

Proseware identifies the following general requirements:

- Minimize the IP address space required to deploy platform-managed resources to the virtual networks.
- From SpokeVNet, resolve name resolution requests for the azure.proseware.com namespace and the corp.proseware.com namespace by using PRDNS1.
- Whenever possible, minimize administrative effort.

Question: 22

You need to configure a security rule for APPGW1-NSG1. The solution must support the planned changes.
Which service tag should you use?

A. AzureFrontDoor.FirstParty
B. AzureFrontDoor.Infra
C. AzureFrontDoor.Backend
D. AzureFrontDoor.Frontend

Answer: C

Explanation:

Question: 23

You need to manage connectivity from NYCNet to the Azure services that use private endpoints. The solution must meet the security requirements. What should you do first?

A. Add a route table to SUBNET-PL
B. Enable a network policy for SUBNET-PE.
C. From Azure Virtual Network Manager, create a security admin configuration.
D. From Azure Viitual Network Manager, create a network group that has Member type set to Subnet

Answer: B

Explanation:

Question: 24

HOTSPOT
You need to configure the P2S VPN to meet the connectivity requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

For VPNGW1, set Tunnel type to IKEv2

- **IKEv2**
- OpenVPN (SSL)
- SSTP (SSL)

For proseware.com Create an app registiatiOT,

Configure an enterprise application

- **Create an app registration.**
- Provision a user-assigned managed identity.

Answer:

Explanation:

Answer Area

For VPNGW1. set Tunnel type to: IKEvZ

For proseware coni Create an app registration.

Question: 25

HOTSPOT

You need to configure connectivity between NYCNet and SFONet. The solution must meet the connectivity requirements. What should you do? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Answer Area

For HubVNet: Configure a user-defined route (UDR).

ure a user defined route (UDR).

Deploy an Azure Route Server

Implement an Azure Virtual Network Manager connectivity configuration

ForVPNGWI: I Change the ASN numbet ^1

| Change the ASN number.

Configuie active-active mode.

Resize the SKU.

Answer:

Explanation:

Answer Area

For HubVNet: Configure a user-defined route (UDR)

For VPNGW1 Change the ASN number

Question: 26

You need to configure APPGW1 to support end-to-end encryption. The solution must meet the security requirements. What should you do?

A. From the SSL settings, upload a TLS client certificate that is issued by the internal root CA and includes the full certificate chain.

B. From the Backend settings, upload a wildcard TLS certificate that has a private key issued by the internal root CA

C. From the Backend settings, upload the internal root CA certificate.

D. From the SSL settings, upload a TLS client certificate that is issued by the internal root CA.

Answer: A

Explanation:

Question: 27

HOTSPOT

You need to identify which IP address space to allocate for the planned deployment of PRDNS1 to HubVNet and SpokeVNet. The solution must meet the general requirements

What should you identify for each virtual network? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

/24

Noaddressspacerequired

/24
/25
/28

SpokeVNet

/25

No address space required
/24
/25

/28

HubVNet

Answer:

Explanation:

Answer Area

HubVNet /24

SpokeVNet /25

Question: 28

You need to configure a custom rule for APPGWI-WAFPolicy to allow only connections that originate from FD1.

The solution must support the planned changes.

Which Match type and Match variable should you select?

A. String and RequestCookies
B. IP address and RemoteAddr
C. String and RequestHeaders
D. Geo location and RemoteAddr

Answer: B

Explanation:

Question: 29

HOTSPOT

You ate configuring the DNS forwarding luleset for DNSR1

You need to configure the destination IP address for azure.proseware.com and for corp.proseware.com. The solution must meet the general requirements.

Which IP addiesses should you configure for each namespace? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

azure proseware.com:
- 168 6312916
- 168.63.129.16
- 192.168.0 100
- The first IP address of the inbound endpoint subnet of PRDNS1
- The first IP address of the outbound endpoint subnet of PRDNS1

corp proseware com:
- 168.63 129 16
- 192 1680.100
- The first IP address of the inbound endpoint subnet of PRDNS1
- The first IP address of the outbound endpoint subnet of PRDNS1

Answer:

Explanation:

Answer Area

azureproseware.com: 1686312916

corp proseware.com 192 168.0.100

Question: 30

You need to configure FD1 to provide user access to app2.proseware.com. The solution must meet the security requirements and the general requirements.

What should you do first?

A. Add a custom domain to FD1.
B. Add a security policy to FD1.
C. Request a certificate from a trusted root CA.
D. Export the TLS certificate and the private key from App2.

Answer: C

Explanation:

Question: 31

HOTSPOT

You need to plan the deployment of LBGW1. The solution must support the planned changes.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Minimum required numbei of load balancing rules: 2'

2

Configure LBGW1 to reference LBS1 by modifying the Ffontend IP configuration

Backend pools

Frontend IP configuration

Load balancing rules

Answer:

Explanation:

Answer Area

Minimum tequired numbei of load balancing rules: 2

Configure LBGW1 to reference LBS1 by modifying the: Frontend IP configuration

Question: 32

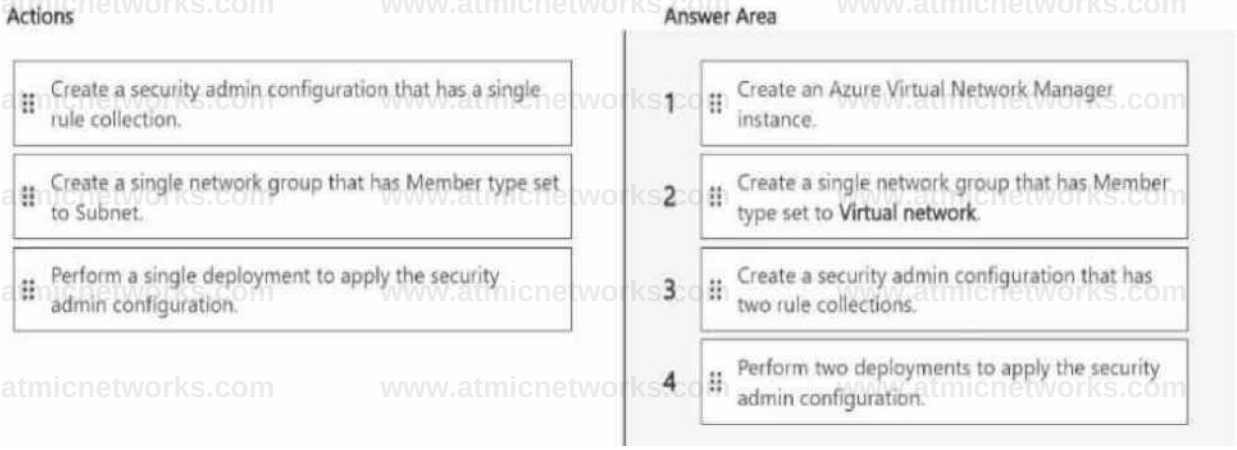
DRAG DROP

You need to deploy Azure Virtual Network Manager. The solution must support the planned changes and meet the connectivity requirements.

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

Answer:

Explanation:



Topic 4, Mix Questions

Question: 33

You have an Azure virtual network that contains two subnets named Subnet1 and Subnet2. Subnet1 contains a virtual machine named VM1. Subnet2 contains a virtual machine named VM2.

You have two network security groups (NSGs) named NSG1 and NSG2. NSG1 has 100 inbound security rules and is associated to VM1. NSG2 has 200 inbound security rules and is associated to Subnet1.

VM2 cannot connect to VM1.

You suspect that an NSG rule blocks connectivity.

You need to identify which rule blocks the connection. The issue must be resolved as quickly as possible.

Which Azure Network Watcher feature should you use?

A. Effective security rules
B. Connection troubleshoot
C. NSG diagnostic
D. NSG flow logs

Answer: C

Explanation:

Question: 34

You have an Azure Front Door instance that has a single frontend named Frontend1 and an Azure Web Application Firewall (WAF) policy named Policy1. Policy1 redirects requests that have a header containing "string1" to https://www.contoso.com/redirect1. Policy1 is associated to Frontend1.

You need to configure additional redirection settings. Requests to Frontend1 that have a header containing "string2" must be redirected to https://www.contoso.com/redirect2.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a custom rule.
B. Configure a managed rule.
C. Create a frontend host.
D. Create a policy.
E. Create an association.
F. Add a custom rule to Policy1.

Answer: C, E, F,

Explanation:

Question: 35

HOTSPOT

You have the network security groups (NSGs) shown in the following table.

Name	Resource	Prefix
NSG1	Subnet1	10.10.0.0/24
NSG2	Subnet2	10.10.1.0/24

In NSG1, you create inbound rules as shown in the following table.

Source	Priority	Port	Action
*	101	80	Allow
*	150	443	Allow
Virtual network	200	*	Deny

You have the Azure virtual machines shown in the following table.

Name	Subnet
VM1	Subnet1
VM2	Subnet1
VM3	Subnet2

NSG2 has only the default rules configured.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM3 can connect to port 8080 on VM1.	○	○
VM1 and VM2 can connect on port 9090.	○	○
VM1 can connect to VM3 on port 9090.	○	○

Answer:

Explanation:

NO, NO, YES

1. VM3 can connect to port 8080 on VM1 : false, UserRule_DenyVirtualNetworkInbound
2. VM1 and VM2 can connect on port 9090: false, UserRule_DenyVirtualNetworkInbound
3. VM1 can connect to VM3 on port 9090: true

Question: 36

You have an Azure virtual network that contains the subnets shown in the following table.

Name	IP address space
AzureFirewallSubnet	192.168.1.0/24
Subnet2	192.168.2.0/24

You deploy an Azure firewall to AzureFirewallSubnet. You route all traffic from Subnet2 through the firewall.
You need to ensure that all the hosts on Subnet2 can access an external site located at https://*.contoso.com.
What should you do?

A. Create a network security group (NSG) and associate the NSG to Subnet2.
B. In a firewall policy, create an application rule.
C. In a firewall policy, create a DNAT rule.
D. In a firewall policy, create a network rule.

Answer: B

Explanation:

Question: 37

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	In resource group	Location
Vnet1	RG1	West US
Vnet2	RG1	Central US
Vnet3	RG2	Central US
Vnet4	RG2	West US
Vnet5	RG3	East US

You plan to deploy an Azure firewall named AF1 to RG1 in the West US Azure region.
To which virtual networks can you deploy AF1?

A. Vnet1 only
B. Vnet1 and Vnet2 only
C. Vnet1, Vnet2, and Vnet4 only
D. Vnet1 and Vnet4 only
E. Vnet1, Vnet2. Vnet3, and Vnet4

Answer: A

Explanation:

Question: 38

HOTSPOT

You have an Azure application gateway named AppGW1 that provides access to the following hosts:

- www.adatum.com www.contoso.com www.fabrikam.com
- From 131.107.10.15, you can access www.contoso.com
-
-

AppGW1 has the listeners shown in the following table.

Name	Frontend IP address	Type	Host name
Listen1	Public	Multi site	www.contoso.com
Listen2	Public	Multi site	www.fabrikam.com
Listen3	Public	Multi site	www.adatum.com

You create Azure Web Application Firewall (WAF) policies for AppGW1 as shown in the following table.

Name	Policy mode	Custom rule		
		Priority	Condition	Association
Policy1	Prevention	50	If IP address does contain 131.107.10.15 then deny traffic.	Application gateway: AppGW1
Policy2	Detection	10	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen1
Policy3	Prevention	70	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From 131.107.10.15, you can access www.contoso.com.	○	○
From 131.107.10.15, you can access www.fabrikam.com.	○	○
From 131.107.10.15, you can access www.adatum.com.	○	○

Answer:

Explanation:

Statements	Yes	No
From 131.107.10.15, you can access www.fabrikam.com		
From 131.107.10.15, you can access www.adatum.com		

Reference:

https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/per-site-policies

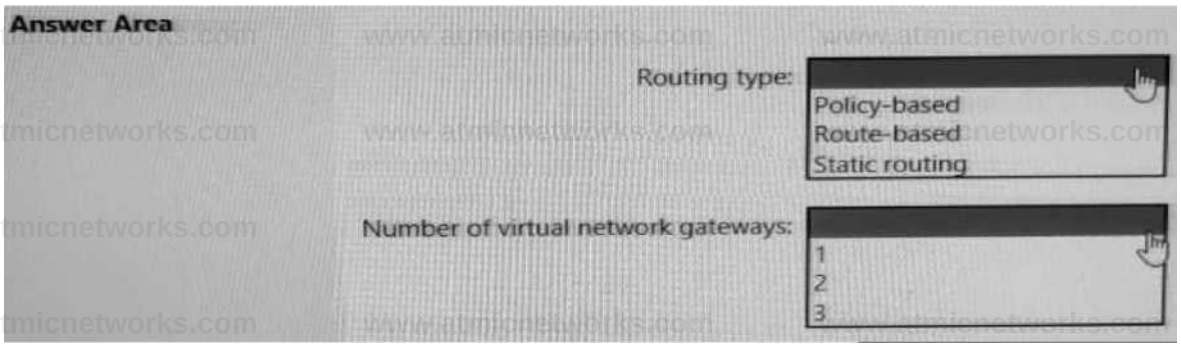
Question: 39

HOTSPOT

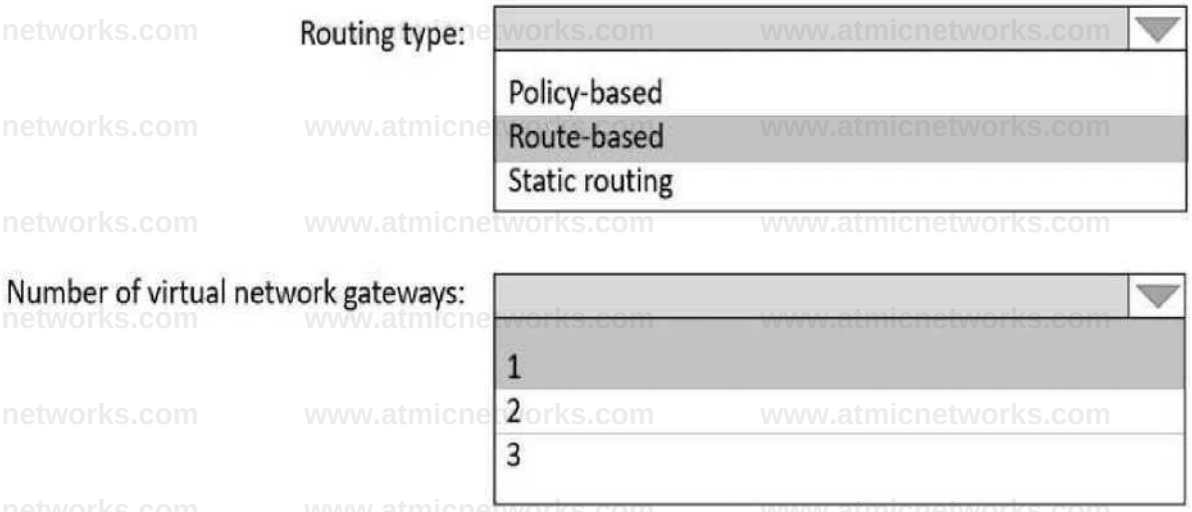
You need to connect an on-premises network and an Azure environment. The solution must use ExpressRoute and support failing over to a Site-to-Site VPN connection if there is an ExpressRoute failure.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one



Explanation:



Answer:

Reference:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource- manager

Question: 40

You are planning an Azure Point-to-Site (P2S) VPN that will use OpenVPN.
Users will authenticate by using an on premises Active Directory domain.
Which additional service should you deploy to support the VPN authentication?

A. a certification authority (CA) B. a RADIUS server

C. an Azure key vault

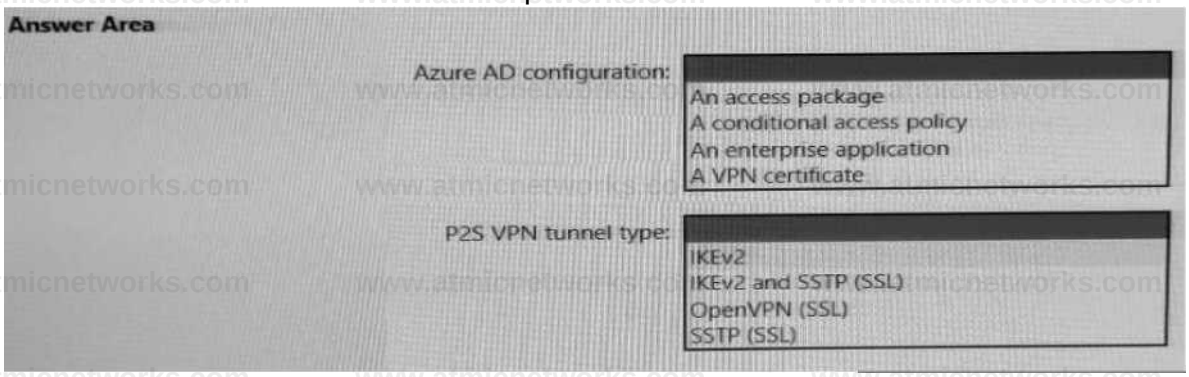
D. Azure Active Directory (Azure AD) Application Proxy

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

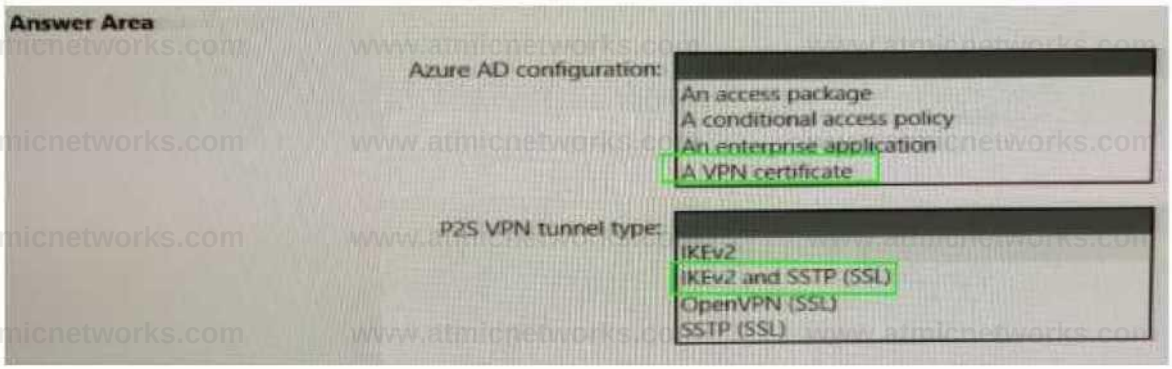
Question: 41

HOTSPOT
You have an Azure subscription that contains a single virtual network and a virtual network gateway.
You need to ensure that administrators can use Point-to-Site (P2S) VPN connections to access resources in the virtual network. The connections must be authenticated by Azure Active Directory (Azure AD).
What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer

Explanation:
Answer:



Question: 42

You fail to establish a Site-to-Site VPN connection between your company's main office and an Azure virtual network.
You need to troubleshoot what prevents you from establishing the IPsec tunnel.
Which diagnostic log should you review?

A. IKEDiagnosticLog
B. GatewayDiagnosticLog
C. TunnelDiagnosticLog
D. RouteDiagnosticLog

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics

IKEDiagnosticLog = The IKEDiagnosticLog table offers verbose debug logging for IKE/IPsec. This is very useful to review when troubleshooting disconnections, or failure to connect VPN scenarios.

GatewayDiagnosticLog = Configuration changes are audited in the GatewayDiagnosticLog table.

TunnelDiagnosticLog = The TunnelDiagnosticLog table is very useful to inspect the historical connectivity statuses of the tunnel.

RouteDiagnosticLog = The RouteDiagnosticLog table traces the activity for statically modified routes or routes received via BGP.

P2SDiagnosticLog = The last available table for VPN diagnostics is P2SDiagnosticLog. This table traces the activity for Point to Site.

https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics

Question: 43

Your company has an on-premises network and three Azure subscriptions named Subscription1, Subscription2, and Subscription3.
The departments at the company use the Azure subscriptions as shown in the following table.

Department	Subscription
IT	Subscription1
Research	Subscription1
Development	Subscription2
Testing	Subscription2
Distribution	Subscription3

All the resources in the subscriptions are in either the West US Azure region or the West US 2 Azure region.
You plan to connect all the subscriptions to the on-premises network by using ExpressRoute. What is the minimum number of ExpressRoute circuits required?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction

Question: 44

You have an Azure virtual network and an on-premises datacenter.
You need to implement a Site-to-Site VPN connection between the datacenter and the virtual network.
Which two resources should you create? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. a virtual network gateway
B. Azure Firewall
C. a local network gateway
D. Azure Web Application Firewall (WAF)
E. an on-premises data gateway
F. an Azure application gateway
G. a user-defined route

Answer: A, C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal

Question: 45

You have the Azure resources shown in the following table.

Name	Type	Location	Description
storage1	Storage account	East US	Read-access geo-redundant storage (RA-GRS)
Vnet1	Virtual network	East US	Contains one subnet

You configure storage1 to provide access to the subnet in Vnet1 by using a service endpoint.
You need to ensure that you can use the service endpoint to connect to the read-only endpoint of storage1 in the paired Azure region.
What should you do first?

A. Configure the firewall settings for storage1.
B. Fail over storage1 to the paired Azure region.
C. Create a virtual network in the paired Azure region.
D. Create another service endpoint.

Answer: A

Explanation:

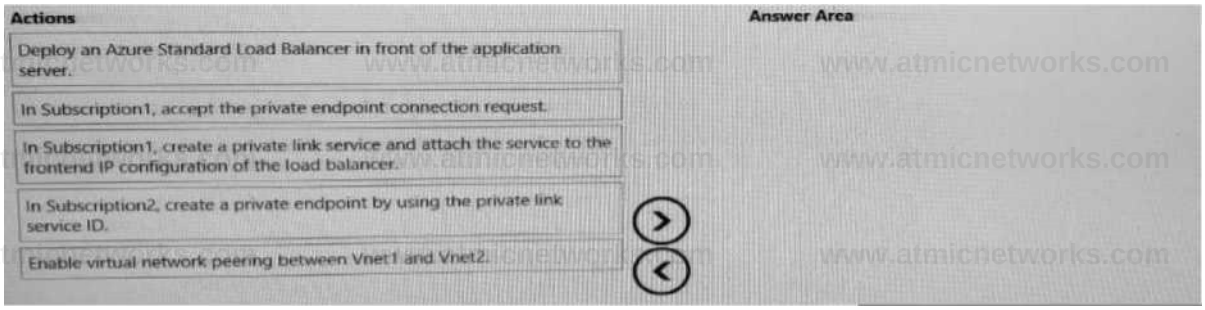
Question: 46

DRAG DROP

You have two Azure subscriptions named Subscnption1 and Subscription2. Subscription1 contains a virtual network named Vnet1. Vnet1 contains an application server. Subscription2 contains a virtual network named Vnet2.

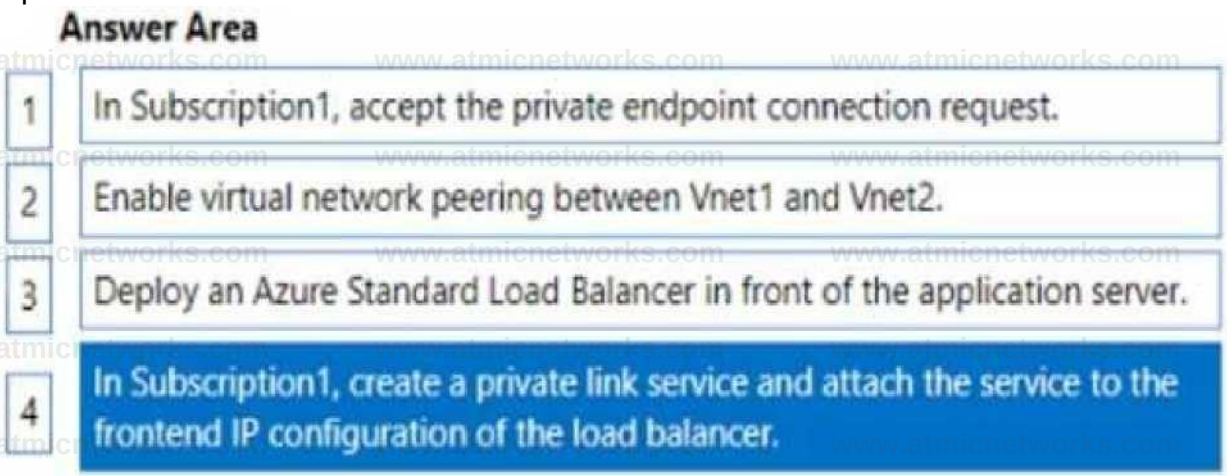
You need to provide the virtual machines in Vnet2 with access to the application server in Vnet1 by using a private endpoint.

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



Answer:

Explanation:



Question: 47

You have an Azure virtual network named Vnet1.

You need to ensure that the virtual machines in Vnet1 can access only the Azure SQL resources in the East US Azure region. The virtual machines must be prevented from accessing any Azure Storage resources.

Which two outbound network security group (NSG) rules should you create? Each correct answer

presents part of the solution.

NOTE: Each correct selection is worth one point.

A. an allow rule that has the IP address range of Vnet1 as the source and destination of Sq1.EastUS
B. a deny rule that has a source of VirtualNetwork and a destination of Sq1
C. a deny rule that has a source of VirtualNetwork and a destination of 168.63.129.0/24
D. a deny rule that has the IP address range of Vnet1 as the source and destination of Storage

Answer: C, D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview

Question: 48

DRAG DROP

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location
WebAppl	Web app	West US
VNetl	Virtual network	East US

The IP Addresses settings for Vnet1 are configured as shown in the exhibit.

You need to ensure that you can integrate WebApp1 and Vnet1.

Basic IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.3.0.0/16 10.3.0 0- 10.3.255.255 (65536 addresses)

J Add IPv6 address space O

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

Add subnet ® Remove subnet

Subnet name	Subnet address range	NAT gateway
Subnetl	10.3.0.0/16	

0 Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. Learn more

Which three actions should you perform in sequence before you can integrate WebApp1 and Vnet1? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions **Answer Area**

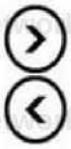
Create a service endpoint

Deploy a VPN gateway

Add a private endpoint

Modify the address space of Vnetl

Configure a Point-to-Site (P2S) VPN



Answer:

Explanation:

Modify the address space of Vnetl

Deploy a VPN gateway

Configure a Point-to-Site (P2S) VPN

Reference:
https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet#gateway- required-vnet-integration

Question: 49

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The subscription contains the following resources:

* An Azure App Service app named App1
* An Azure DNS zone named contoso.com
* An Azure private DNS zone named private.contoso.com
* A virtual network named Vnet1

You create a private endpoint for App1. The record for the endpoint is registered automatically in Azure DNS.

You need to provide a developer with the name that is registered in Azure DNS for the private endpoint.

What should you provide?

A. app1.privatelink.azurewebsites.net
B. app1.contoso.com
C. app1.contoso.onmicrosoft.com
D. app1.private.contoso.com

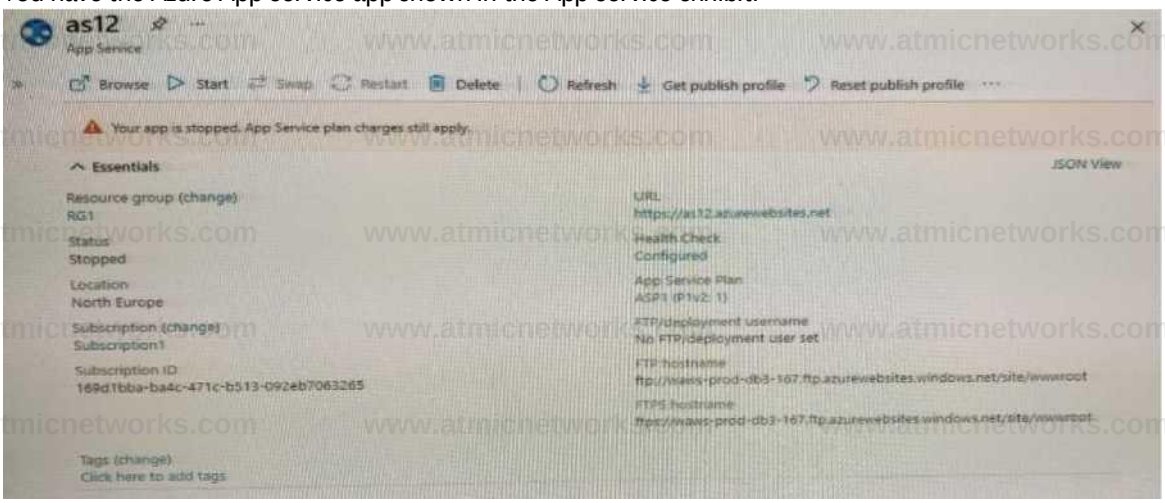
Answer: A

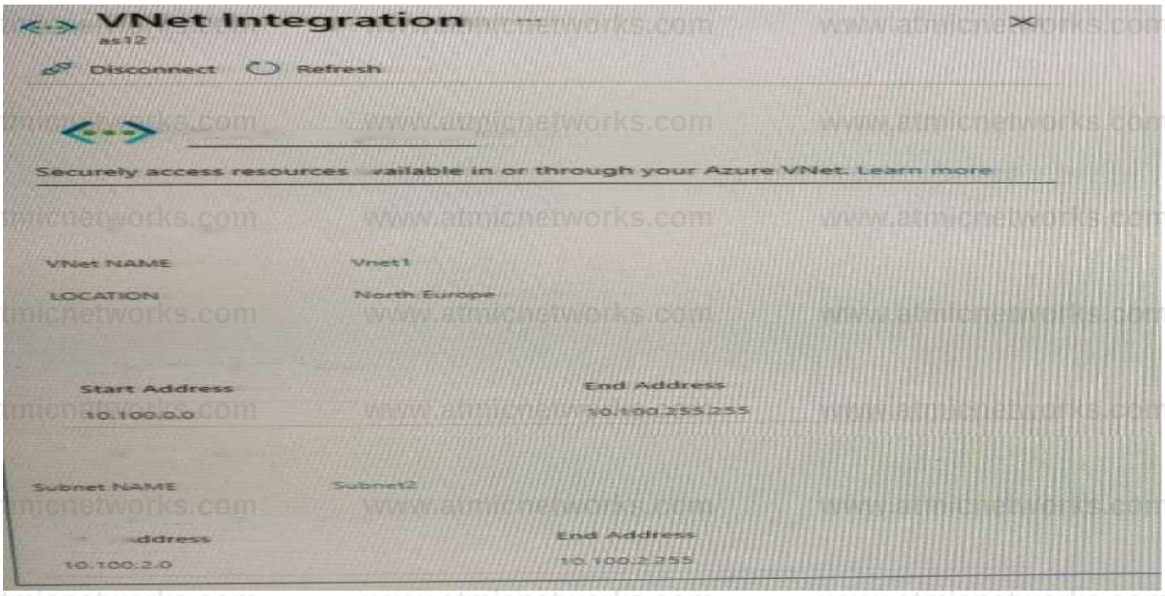
Explanation:

Question: 50

HOTSPOT

You have the Azure App Service app shown in the App Service exhibit.

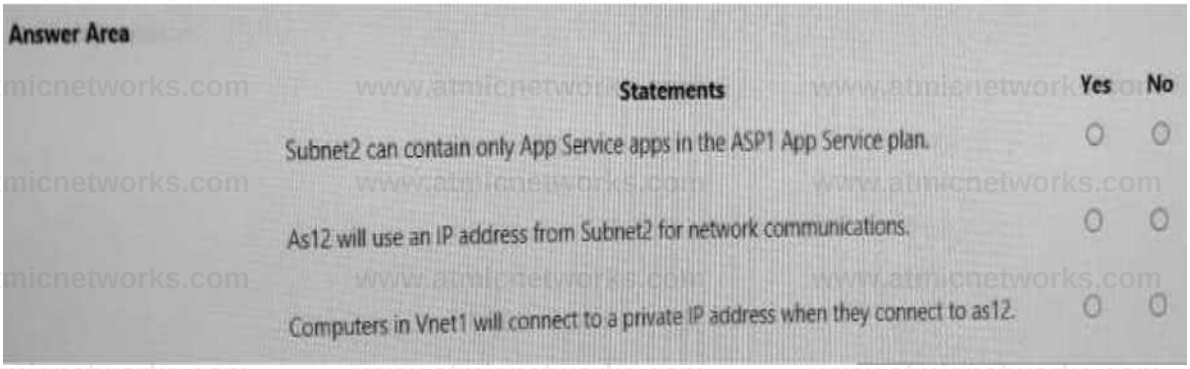




The VNet Integration settings for as12 are configured as shown in the Vnet Integration exhibit.

The Private Endpoint connections settings for as12 are configured as shown in the Private Endpoint connections exhibit.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Statements

	Yes	No
Subnet? can contain only App Service apps in the ASP1 App Service plan	○	○
Asl2 will use an IP address from Subnet2 for network communications	○	○
Computers in Vnetl will connect to a private IP address when they connect to asl2	○	○

Reference:
https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet

Question: 51

You have an Azure subscription that contains the public IP addresses shown in the following table.

Name	IP version	SKU	IP address assignment
IP1	IPv4	Basic	Static
IP2	IPv4	Basic	Dynamic
IP3	IPv4	Standard	Static
IP4	IPv6	Basic	Dynamic
IP5	IPv6	Standard	Static

You plan to deploy a NAT gateway named NAT1.
Which public IP addresses can be used as the public IP address for NAT1?

A. IP3 and IP5 only
B. IP5 only
C. IP1, IP3, and IP5 only
D. IP3 only
E. IP2 and IP4 only

Answer: D

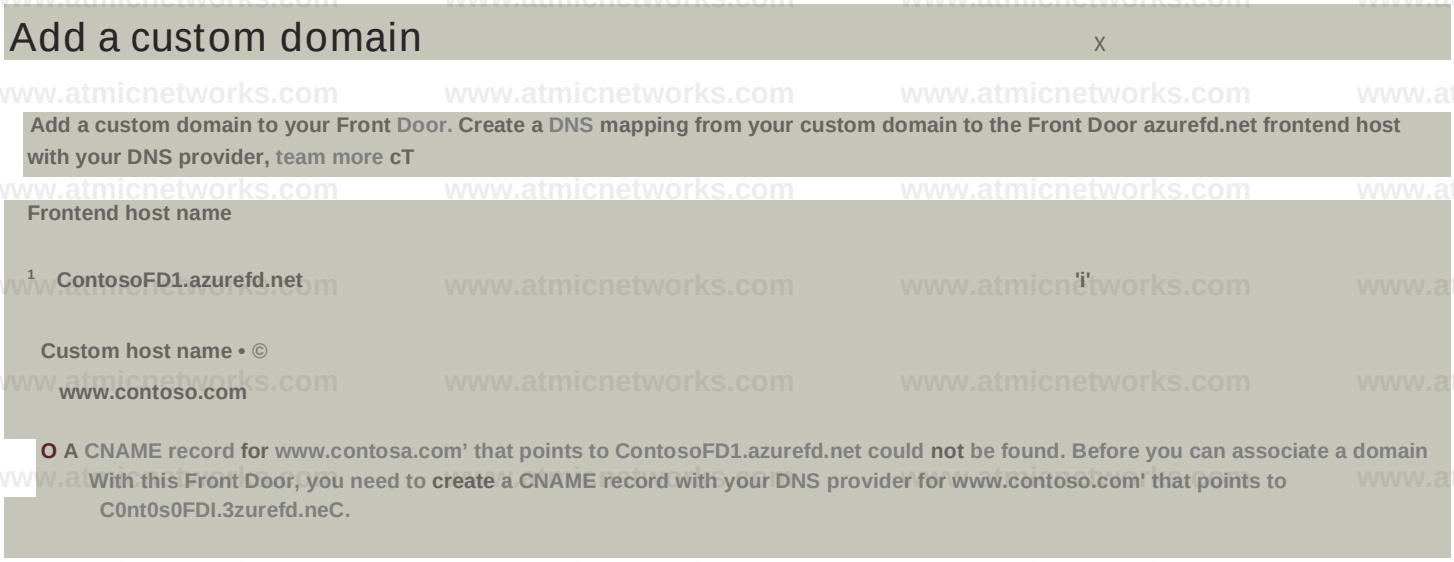
Explanation:

Only static IPv4 addresses in the Standard SKU are supported. IPv6 doesn't support NAT.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview

Question: 52

You have a website that uses an FQDN of www.contoso.com. The DNS record tor www.contoso.com resolves to an on-premises web server.
You plan to migrate the website to an Azure web app named Web1. The website on Web1 will be published by using an Azure Front Door instance named ContosoFD1.
You build the website on Web1.
You plan to configure ContosoFD1 to publish the website for testing.
When you attempt to configure a custom domain for www.contoso.com on ContosoFD1, you receive the error message shown in the exhibit.



You need to test the website and ContosoFD1 without affecting user access to the on-premises web server.
Which record should you create in the contoso.com DNS domain?

A. a CNAME record that maps www.contoso.com to ContosoFD1.azurefd.net

B. a CNAME record that maps www.contoso.com to Web1.contoso.com
C. a CNAME record that maps afdverify.www.contoso.com to ContosoFD1.azurefd.net
D. a CNAME record that maps afdverify.www.contoso.com to afdverify.ContosoFD1.azurefd.net

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain#map-the-temporary- afdverify-subdomain

Question: 53

You have an Azure Virtual Desktop deployment that has 500 session hosts.
All outbound traffic to the internet uses a NAT gateway.
During peak business hours, some users report that they cannot access internet resources. In Azure Monitor, you discover many failed SNAT connections.
You need to increase the available SNAT connections.
What should you do?

A. Add a public IP address.
B. Bind the NAT gateway to another subnet.
C. Deploy Azure Standard Load Balancer that has outbound rules.

Answer: A

Explanation: Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource

Question: 54

You have an Azure subscription that contains the public IPv4 addresses shown in the following table.

Name	SKU	IP address assignment	Location
IP1	Basic	Static	West US
IP2	Basic	Dynamic	West US
IP3	Standard	Static	West US
IP4	Basic	Static	West US 2
IP5	Standard	Static	West US 2

You plan to create a load balancer named LB1 that will have the following settings:

* Name: LB1
* Location: West US
* Type: Public
* SKU: Standard

Which public IPv4 addresses can be used by LB1?

A. IP1 and IP3 only
B. IP3 only
C. IP3 and IP5 only
D. IP2only
E. IP1, IP2. IP3. IP4. and IP5
F. IP1, IP3, IP4, and 1P5 only

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address

This is because "Load balancer and the public IP address SKU must match when you use them with public IP addresses"

https://docs.microsoft.com/en-us/azure/load-balancer/skus

Standard SKU Load Balancer routes traffic within and across regions, and to Availability Zones for high resiliency.

Question: 55

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 shtraffic ould you include in the solution?

A. Azure Standard Load Balancer
B. Azure Traffic Manager
C. Azure Application Gateway
D. Azure Front Door

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/dmz/nva-ha?tabs=cli

Question: 56

You have five virtual machines that run Windows Server. Each virtual machine hosts a different web app.
You plan to use an Azure application gateway to provide access to each web app by using a hostname of www.contoso.corn and a different URL path for each web app, for example: https://www.contoso.com/app1.
You need to control the flow of traffic based on the URL path.
What should you configure?

A. rules
B. rewrites
C. HTTP settings
D. listeners

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/url-route-overview

Question: 57

You have an Azure application gateway for a web app named App1. The application gateway allows end-to-end encryption.

You configure the listener for HTTPS by uploading an enterprise signed certificate.

You need to ensure that the application gateway can provide end-to-end encryption for App1. What should you do?

A. Set Listener type to Multi site.
B. Increase the Unhealthy threshold setting in the custom probe.
C. Upload the public key certificate to the HTTPS settings.
D. Enable the SSL profile for the listener.

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/end-to-end-ssl-portal
https://docs.microsoft.com/en-us/azure/application-gateway/create-ssl-portal#configuration-tab

Question: 58

HOTSPOT

Your company has 10 instances of a web service. Each instance is hosted in a different Azure region and is accessible through a public endpoint.

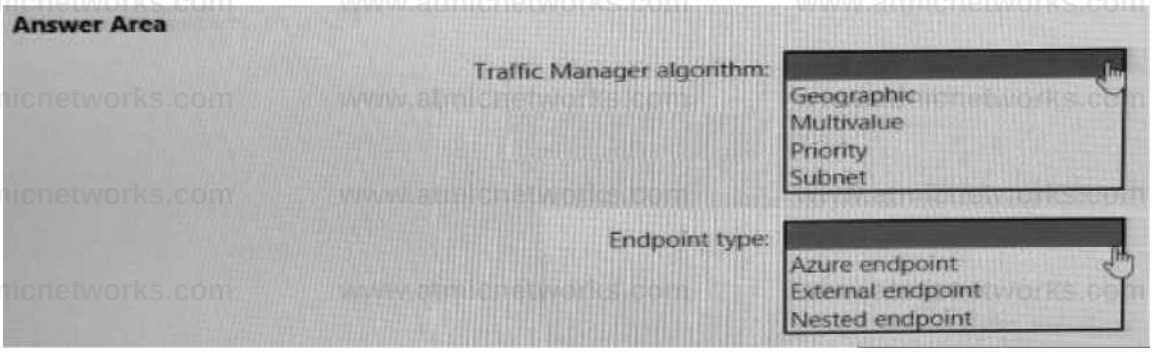
The development department at the company is creating an application named App1. Every 10 minutes. App1 will use a list of end points and connect to the first available endpoint.

You plan to use Azure Traffic Manager to maintain the list of endpoints.

You need to configure a Traffic Manager profile that will minimize the impact of DNS caching.

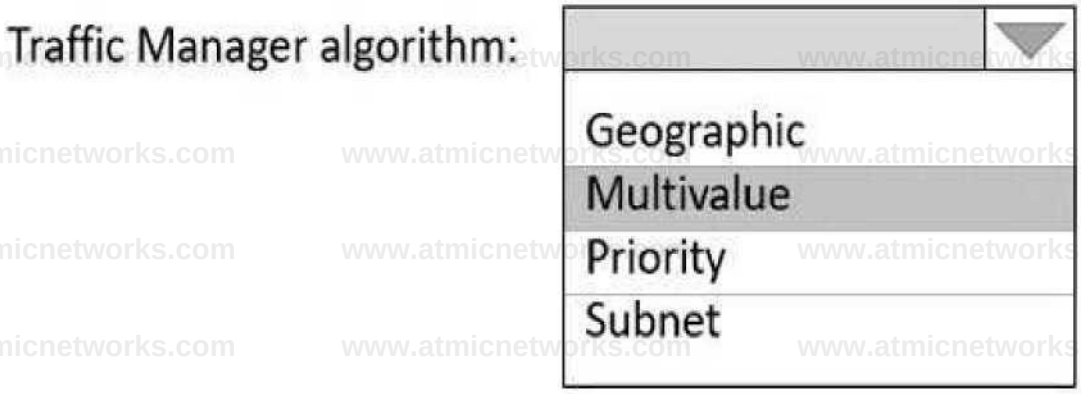
What should you configure? To answer, select the appropriate options in the answer area.

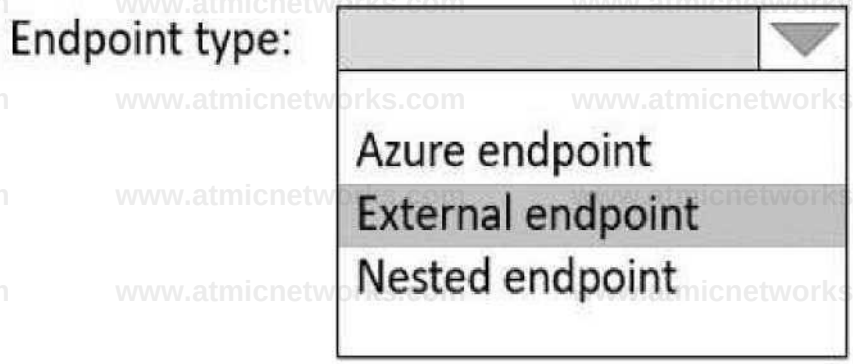
NOTE: Each correct selection is worth one point.



Answer:

Explanation:





Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types

Question: 59

You have an Azure application gateway named AppGW1 that balances requests to a web app named App1.
You need to modify the server variables in the response header of App1.

What should you configure on AppGW1?

A. HTTP settings
B. rewrites

C. rules
D. listeners

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-url

Question: 60

You have an Azure Front Door instance named FD1 that is protected by using Azure Web Application Firewall (WAF).
FD1 uses a frontend host named app1.contoso.com to provide access to Azure web apps hosted in the East US Azure region and the West US Azure region.
You need to configure FD1 to block requests to app1.contoso.com from all countries other than the United States.
What should you include in the WAF policy?

A. a frontend host association
B. a managed rule set
C. a custom rule that uses a rate limit rule
D. a custom rule that uses a match rule

Answer: D

Explanation:

Question: 61

You have an application named App1 that listens for incoming requests on a preconfigured group of 50 TCP ports and UDP ports.
You install App1 on 10 Azure virtual machines.
You need to implement load balancing for App1 across all the virtual machines. The solution must minimize the number of load balancing rules.
What should you include in the solution?

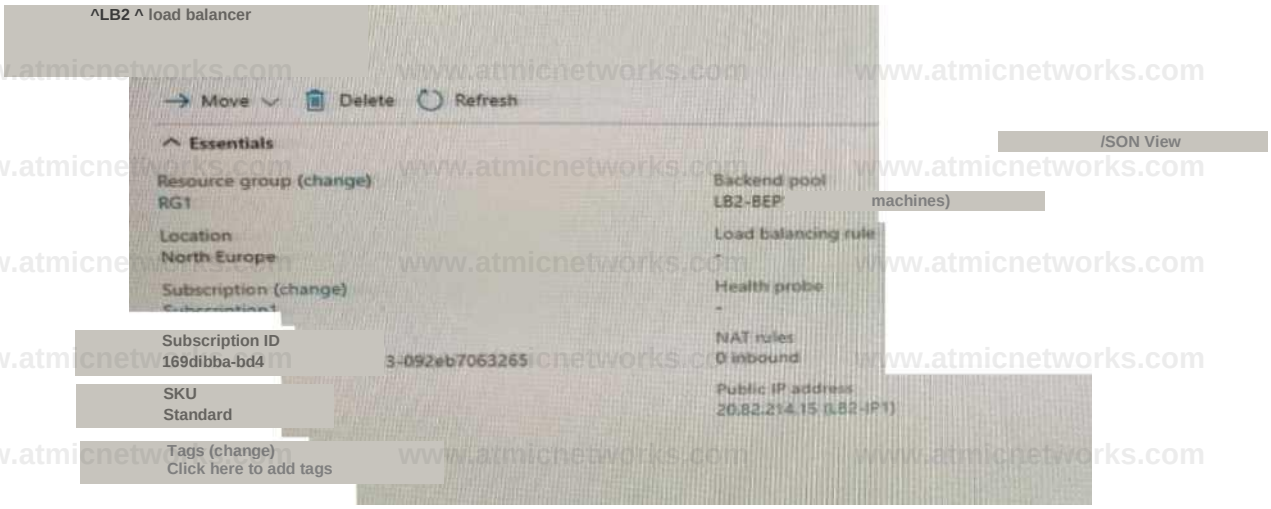
A. Azure Standard Load Balancer that has Floating IP enabled
B. Azure Application Gateway V2 that has multiple listeners
C. Azure Application Gateway v2 that has multiple site hosting enabled
D. Azure Standard Load Balancer that has high availability (HA) ports enabled

Answer: B

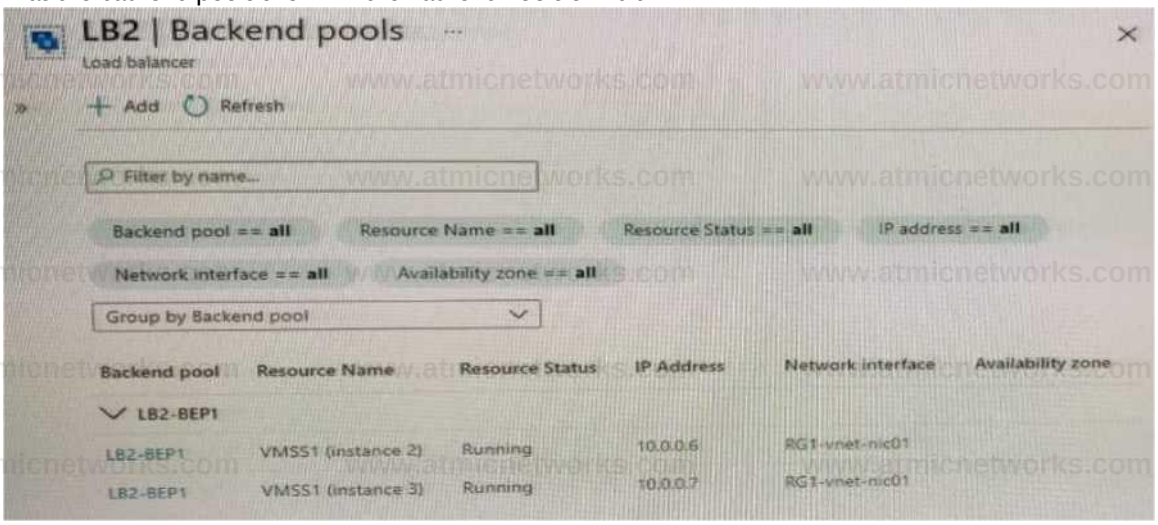
Explanation:

Question: 62

You have the Azure load balancer shown in the Load Balancer exhibit.



LB2 has the backend pools shown in the Backend Pools exhibit.



You need to ensure that LB2 distributes traffic to all the members of VMSS1.
Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add a network interface to VMSS1.
B. Configure a health probe.
C. Add a public IP address to each member of VMSS1.
D. Add a load balancing rule.

Answer: BD

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-portal?tabs=option-1-create-load-balancer-standard

Question: 63

You have the Azure Traffic Manager profiles shown in the following table.

Name	Routing method
Profile1	Performance
Profile2	Multivalue

You plan to add the endpoints shown in the following table.

Name	Type	Additional settings
Endpoint1	Azure endpoint	Target resource type: App Service
Endpoint2	External endpoint	FQDN or IP: www.contoso.com
Endpoint3	External endpoint	FQDN or IP: 131.107.10.15
Endpoint4	Nested endpoint	Target resource: Profile1

Which endpoints can you add to Profile2?

A. Endpoint1 and Endpoint4 only
B. Endpoint1, Endpoint2, Endpoint3, and Endpoint4
C. Endpoint1 only
D. Endpoint2 and Endpoint3 only
E. Endpoint3 only

Answer: A

Explanation:

Question: 64

You have two Azure App Service instances that host the web apps shown the following table.

Name	Web app URLs
As1.contoso.com	https://app1.contoso.com/ https://app2.contoso.com/
As2.contoso.com	https://app3.contoso.com/ https://app4.contoso.com/

You deploy an Azure application gateway that has one public frontend IP address and two backend pools.
You need to publish all the web apps to the application gateway. Requests must be routed based on the HTTP host headers.
What is the minimum number of listeners and routing rules you should configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer: 1, 2

Explanation:

Question: 65

You have 10 Azure App Service instances. Each instance hosts the same web app. Each instance is in a different Azure region.

You need to configure Azure Traffic Manager to direct users to the instance that has the lowest latency.

Which routing method should you use?

A. geographic
B. weighted
C. performance
D. priority

Answer: D

Explanation:

Question: 66

HOTSPOT

You configure a route table named RT1 that has the routes shown in the following table.

Name	Prefix	Next hop type	Next hop IP address
Route1	0.0.0.0/0	Network virtual appliance (NVA)	192.168.0.4
Route2	10.0.0.0/24	Network virtual appliance (NVA)	192.168.0.4

You have an Azure virtual network named Vnet1 that has the subnets shown in the following table.

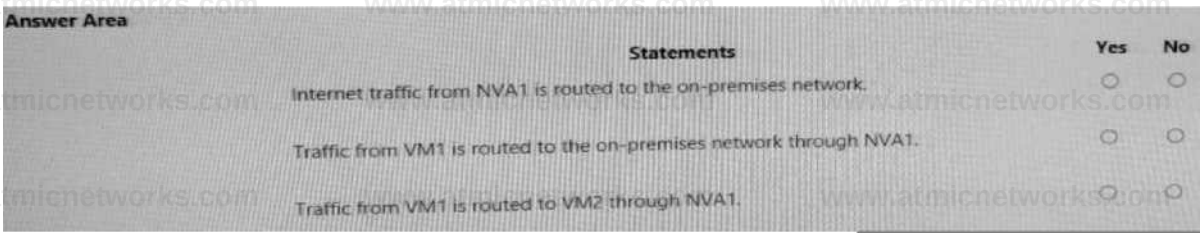
Name	Prefix	Route table
DMZ	192.168.0.0/24	None
FrontEnd	192.168.1.0/24	RT1
BackEnd	192.168.2.0/24	None

You have the resources shown in the following table.

Name	IP address	Type
NVA1	192.168.0.4	NVA
VM1	192.168.1.4	Virtual machine
VM2	192.168.2.4	Virtual machine

Vnet1 connects to an ExpressRoute circuit. The on-premises router advertises the following routes: * 0.0.0.0/0 * 10.0.0.0/16

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

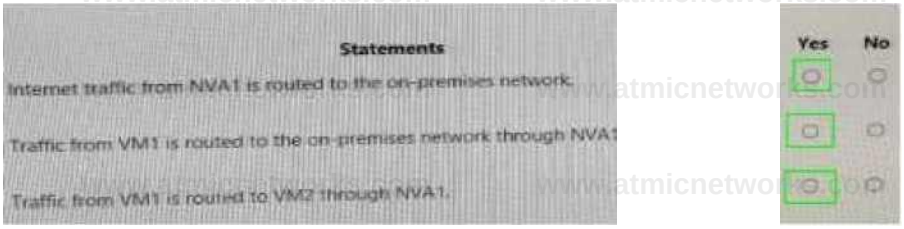


Answer:

Explanation:

Answer:

Answer Area



Question: 67

DRAG DROP

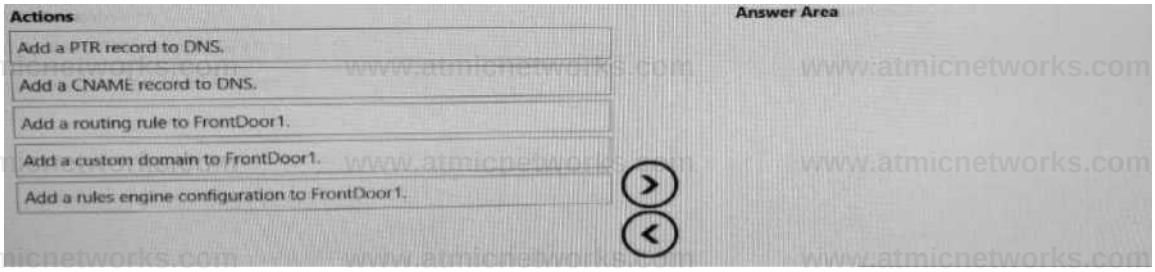
You have an Azure Front Door instance named FrontDoor1.

You deploy two instances of an Azure web app to different Azure regions.

You plan to provide access to the web app through FrontDoor1 by using the name app1.contoso.com.

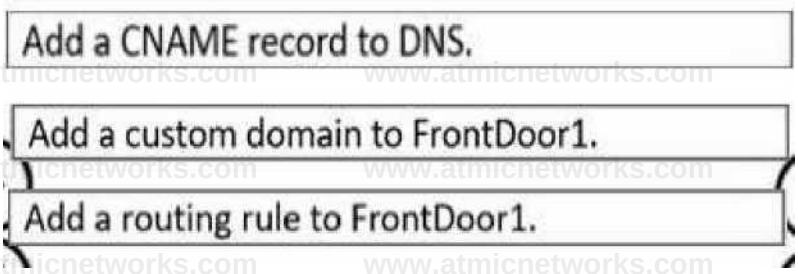
You need to ensure that FrontDoor1 is the entry point for requests that use app1.contoso.com.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Explanation:



Question: 69

Your company has offices in and Amsterdam. The company has an Azure subscription. Both offices connect

to Azure by using a Site-to-Site VPN connection.

The office in Amsterdam uses resources in the North Europe Azure region. The office in New York uses resources in the East US Azure region.

You need to implement ExpressRoute circuits to connect each office to the nearest Azure region. Once the ExpressRoute circuits are connected, the on-premises computers in the Amsterdam office must be able to connect to the on-premises servers in the New York office by using the ExpressRoute circuits.

Which ExpressRoute option should you use?

A. ExpressRoute Local
B. ExpressRoute FastPath
C. ExpressRoute Direct
D. ExpressRoute Global Reach

Answer: D

Explanation:

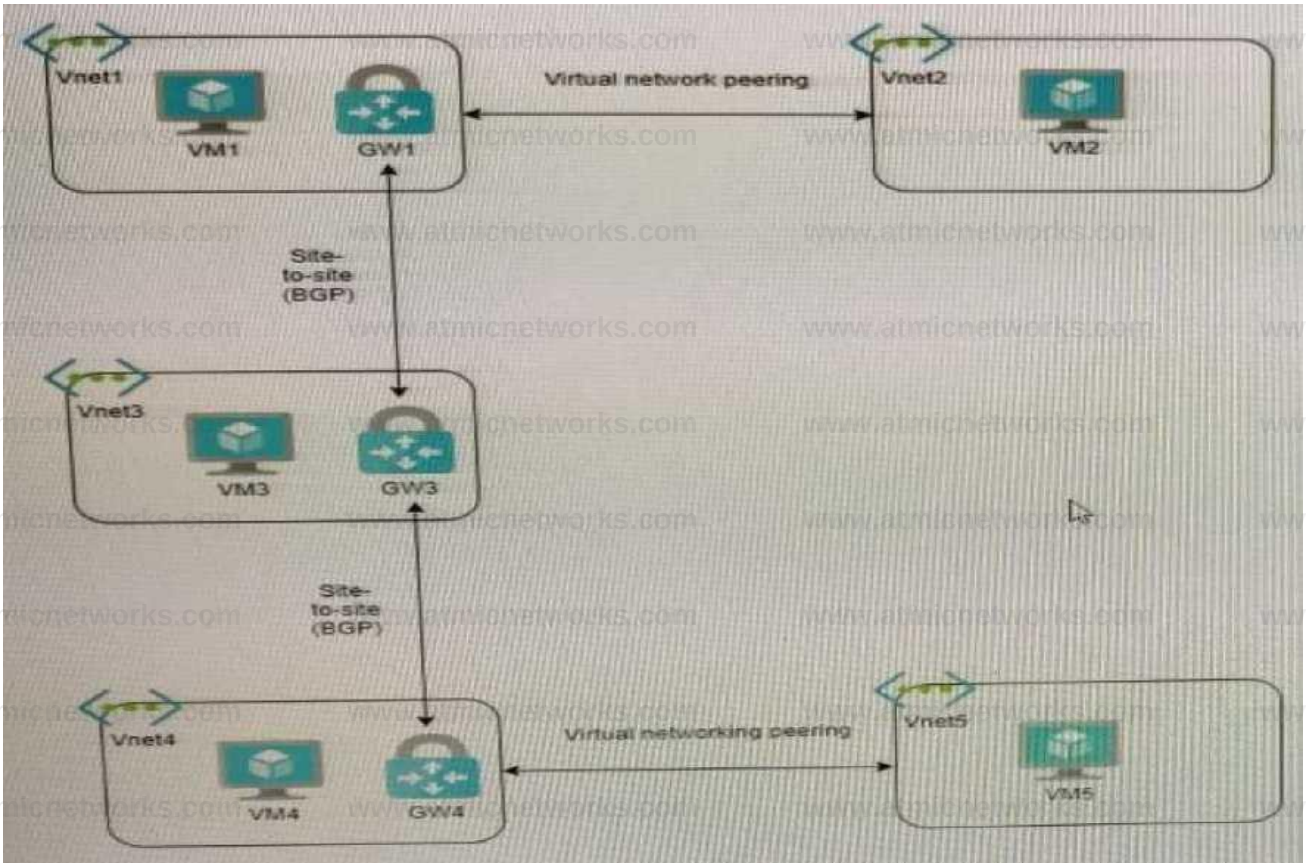
Reference:

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach

Question: 70

HOTSPOT

You have the Azure environment shown in the exhibit.

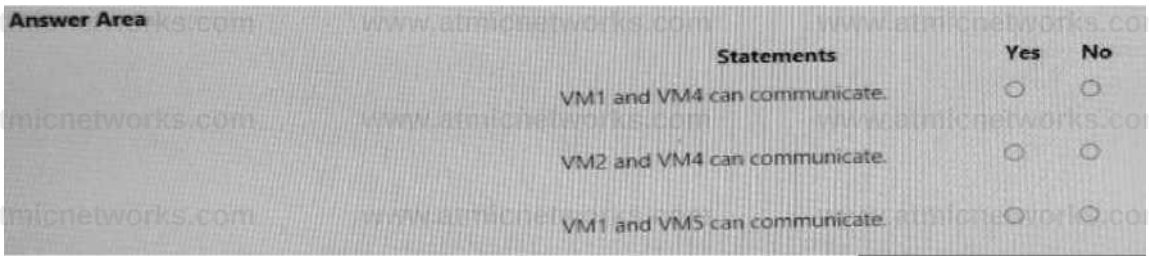


You have virtual network peering between Vnet1 and Vnet2. You have virtual network peering between Vnet4 and Vnet5. The virtual network peering is configured as shown in the following table.

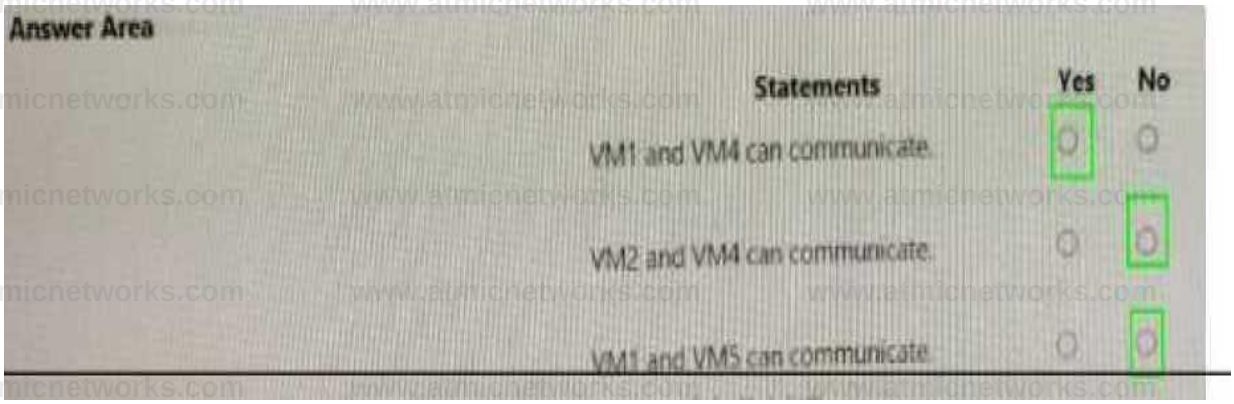
Virtual network	Traffic to remote virtual network	Use remote gateway	Allow gateway transit
Vnet1	Allow	**None**	Enabled
Vnet2	Allow	Enabled	**None**
Vnet4	Allow	**None**	Enabled
Vnet5	Block	Enabled	**None**

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Explanation: Answer:



Question: 71

HOTSPOT

You have an Azure subscription.

You have the on-premises sites shown the following table.

Name	Number of users	Connection type to Azure
Site1	500	ExpressRoute
Site2	100	Site-to-Site VPN
Site3	1	Point-to-Site (P2S) VPN

You plan to deploy Azure Virtual WAN.

You are evaluating Virtual WAN Basic and Virtual WAN Standard.

Which type of Virtual WAN can you use for each site? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Virtual WAN Basic:
- Site2 only
- Site3 only
- Site2 and Site3 only
- Site1, Site2, and Site3

Virtual WAN Standard:
- Site1 only
- Site1 and Site3 only
- Site2 and Site3 only
- Site1, Site2, and Site3

Virtual WAN Basic:

- Site2 only
- Site3 only
- Site2 and Site3 only
- Site1, Site2, and Site3

Virtual WAN Standard:

- Site1 only
- Site1 and Site3 only
- Site2 and Site3 only
- Site1, Site2, and Site3

Reference:
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Question: 72

Azure virtual networks in the East US Azure region as shown in the following table.

Name	IP address space
Vnet1	192.168.0.0/20
Vnet2	10.0.0.0/20

The virtual networks are peered to one another. Each virtual network contains four subnets.
You plan to deploy a virtual machine named VM1 that will inspect and route traffic between all the subnets on both the virtual networks.
What is the minimum number of IP addresses that you must assign to VM1?

A. 1
B. 2
C. 4
D. 8

Answer: B

Question: 74

You plan to deploy an Azure virtual network.
You need to design the subnets.
Which three types of resources require a dedicated subnet? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. VPN gateway
B. Azure Bastion
C. Azure Active Directory Domain Services (Azure AD DS)
D. Azure Application Gateway v2
E. Azure Private Link

Answer: ABD

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services

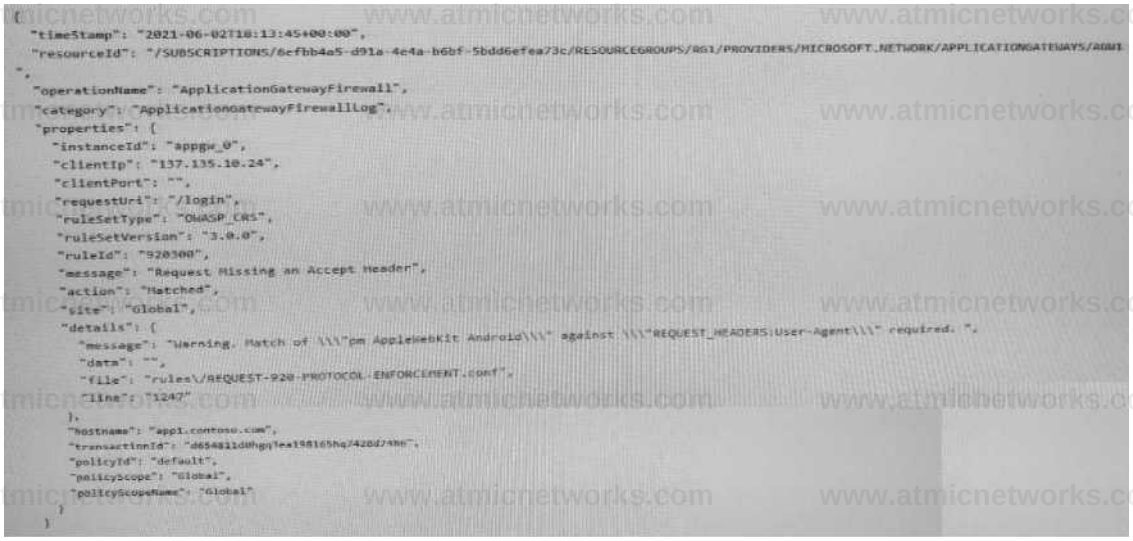
Question: 75

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/6cfbb4a5-d91a-4e4a-b6bf-5bdd6efea73c/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_HEADERS:User-Agent\\\" required. ",
      "data": "",
      "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
      "line": "1247"
    },
    "hostname": "app1.contoso.com",
    "transactionId": "d654811d0hgq1ea198165hq/420d74h6",
    "policyId": "default",
    "policyScope": "Global",
    "policyScopeName": "Global"
  }
}
```


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

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

Does this meet the goal?

A. Yes
B. No

Explanation:

Question: 76

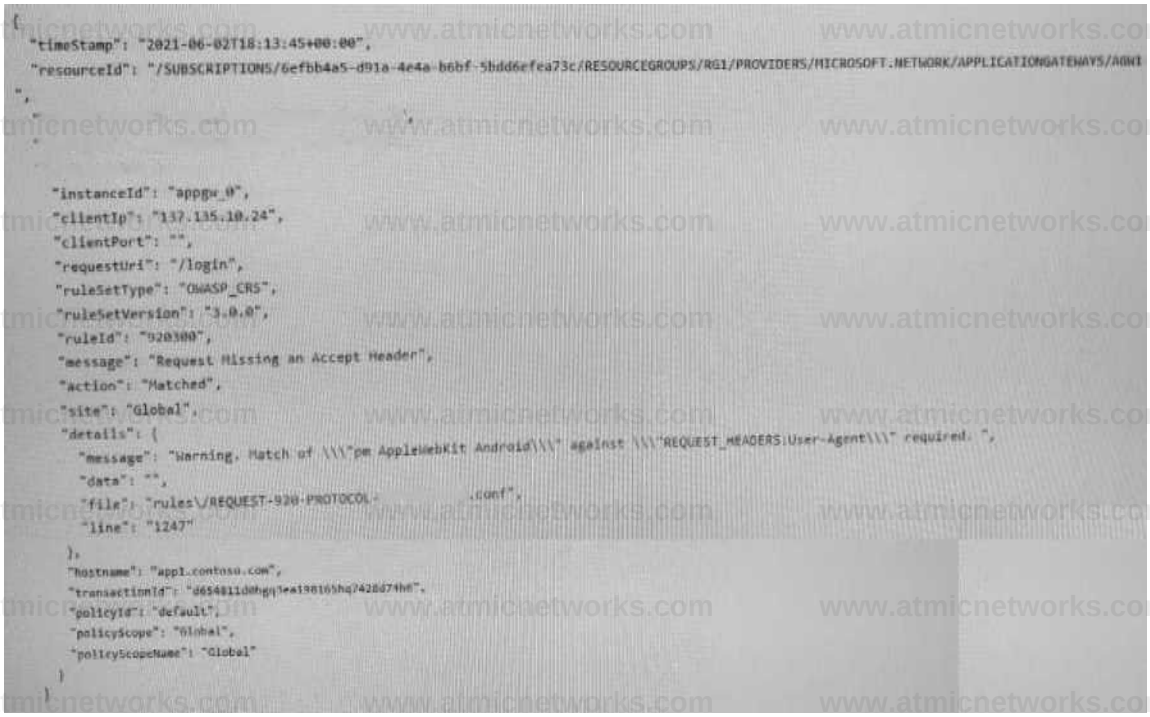
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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.

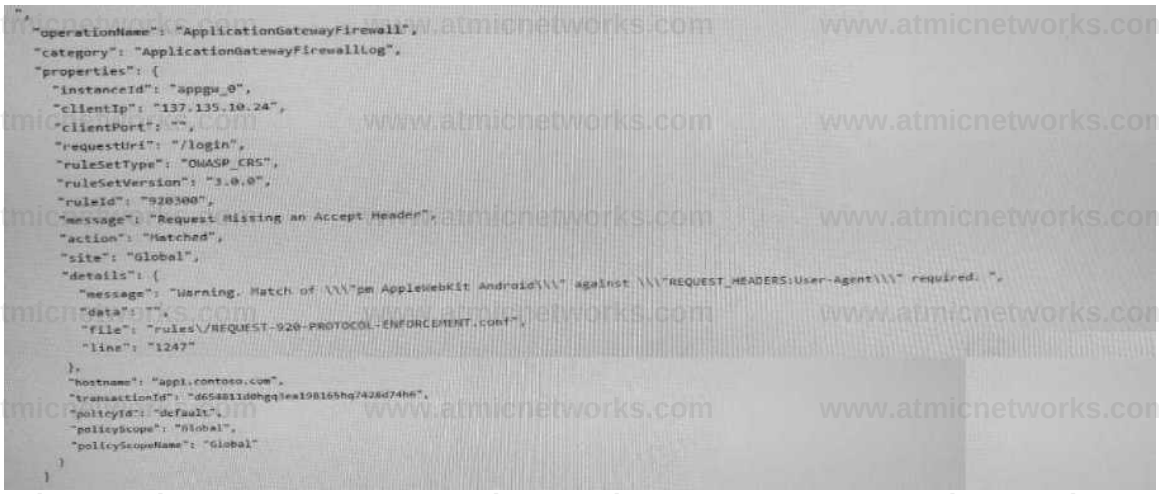


A. Yes
B. No

Answer: A

Question: 77

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.



You need to ensure that the URL is accessible through the application gateway.
Solution: You create a WAF policy exclusion request headers that contain 137.135.10.24.
Does this meet the goat?

A. Yes
B. No

Answer: B

Question: 78

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 named Vnet1
* A subnet named Subnet1 in Vnet1
* A virtual machine named VM1 that connects to Subnet1
* Three storage accounts named storage1, storage2, and storage3
You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.
Solution: You configure the firewall on storage1 to only accept connections from Vnet1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 79

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 named Vnet1
* A subnet named Subnet1 in Vnet1
* A virtual machine named VM1 that connects to Subnet1
* Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You create a network security group (NSG) and associate the NSG to Subnet1.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 80

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 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 named Vnet1
* A subnet named Subnet1 in Vnet1
* A virtual machine named VM1 that connects to Subnet1
* Three storage accounts named storage1, storage2. and storage3
You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.
Solution: You create a network security group (NSG). You configure a service tag for MicrosoftStorage and link the tag to Subnet1.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 81

Your company has a single on-premises datacenter in New York. The East US Azure region has a peering location in New York.

The company only has Azure resources in the East US region.

You need to implement ExpressRoute to support up to 1 Gbps. You must use only ExpressRoute Unlimited data plans. The solution must minimize costs.

Which type of ExpressRoute circuits should you create?

A. ExpressRoute Local
B. ExpressRoute Direct
C. ExpressRoute Premium
D. ExpressRoute Standard

Answer: A

Explanation:
Reference:
https://azure.microsoft.com/en-us/pricing/details/expressroute/

Question: 82

You plan to configure BGP for a Site-to-Site VPN connection between a datacenter and Azure.

Which two Azure resources should you configure? Each correct answer presents a part of the solution. (Choose two.)

NOTE: Each correct selection is worth one point.

A. a virtual network gateway
B. Azure Application Gateway
C. Azure Firewall
D. a local network gateway
E. Azure Front Door

Answer: AD

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/bgp-howto

Question: 83

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit. Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You reset the gateway of Vnet1.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

Question: 84

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit.
Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You enable BGP on the gateway of Vnet1.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

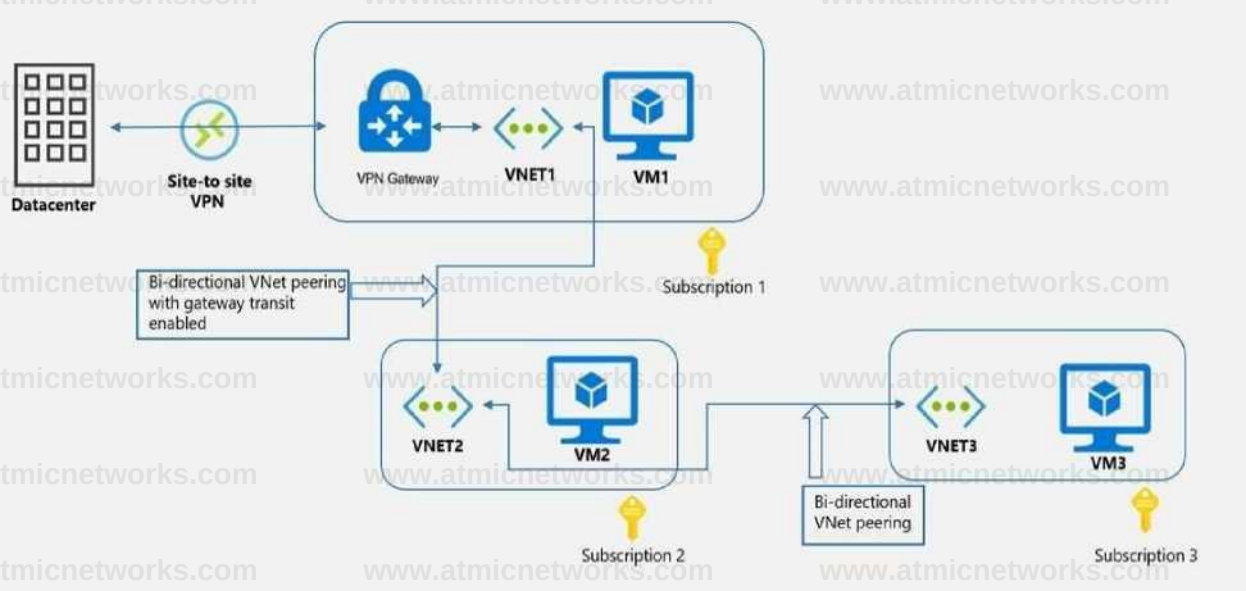
The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

Question: 85

HOTSPOT

You need to ensure that the URL is accessible through the application gateway.
Solution: You configure a custom cookie and an exclusion rule.
Does this meet the goal?



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

VM1 can communicate with (answer choice):

- VM2 only
- VM2 and VM3 only
- the on-premises datacenter and VM2 only
- the on-premises datacenter, VM2, and VM3 only

VM2 can communicate with (answer choice):	
	VM1 only
	VM1 and VM3 only
	the on-premises datacenter and VM3 only

Answer:

VM1 can communicate with **(answer choice):**

- VM2 only
- VM2 and VM3 only
- **the on-premises datacenter and VM2 only**
- the on-premises datacenter, VM2, and VM3 only

VM2 can communicate with **(answer choice):**

- VM1 only
- VM1 and VM3 only
- the on-premises datacenter and VM3 only
- **the on-premises datacenter, VM1, and VM3 only**

Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit?toc=/azure/virtual-network/toc.json

https://docs.microsoft.com/en-ca/azure/virtual-network/ip-services/ipv6-overview#capabilities

Question: 86

HOTSPOT

You have an Azure private DNS zone named contoso.com that is linked to the virtual networks shown in the following table.

Name	IP address
Vnet1	10.1.0.0/16
Vnet2	10.2.0.0/16

The links have auto registration enabled.

You create the virtual machines shown in the following table.

Name	IP address
VM1	10.1.10.10
VM2	10.2.10.10
VM3	10.2.10.11

You manually add the following entry to the contoso.com zone:

Name: VM1
IP address: 10.1.10.9

For each of the following statements, select Yes of the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM2 will resolve vm1xontoso.com to 10.1.111(1		
Deleting VM1 will delete all VM1 records automatically		
If VMS obtains a different IP address from Azure, VM3's DNS record is updated automatically.		

Answer:

Explanation:

Answer Area

Statements	Yes	No
VM2 will resolve vm 1 xontoso.com to 10.1.10.10,	O	S'
Deleting VMI will delete #0 VM1 records automatically,	O	&
If VMS obtains a different IP address from Azure. VMTs DNS record is updated automatically	O	®

Box 1: No
The manual DNS record will overwrite the auto-registered DNS record so VM1 will resolve to 10.1.10.9.

Box 2: No
The DNS record for VM1 is now a manually created record rather than an auto-registered record.
Only auto-registered DNS records are deleted when a VM is deleted.

Box 3: No
This answer depends on how the IP address is changed. To change the IP address of a VM manually, you would need to select

'Static' as the IP address assignment. In this case, the DNS record will not be updated because only DHCP assigned IP addresses are auto-registered.

Reference:
https://docs.microsoft.com/en-us/azure/dns/dns-faq-private

Question: 87

HOTSPOT

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.

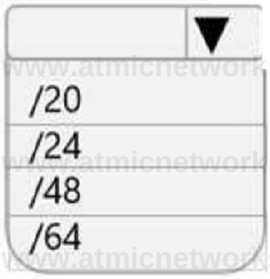
You create an IPv6 address range to Vnet1 by using a CIDR suffix of /48.

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? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Create an IPv6 subnet that uses a CIDR suffix of :



For each virtual machine, create an additional:

IP configuration
NIC
Public IPv6 address

Answer:

Explanation:

Create an IPv6 subnet that uses a CIDR suffix of:

/20
/24
/48
/64

For each virtual machine, create an additional:

IP configuration NIC
Public IPv6 address

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-overview

https://docs.microsoft.com/en-us/azure/virtual-network/ipv6-add-to-existing-vnet-powershell

Correct: /64

The subnets for IPv6 must be exactly /64 in size. This ensures future compatibility should you decide to enable routing of the subnet to an on-premises network since some routers can only accept /64 IPv6 routes.
Source: https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/ipv6-overview

1) Correct: Public IPv6 Address

Add IPv6 configuration to NIC. "Configure all of the VM NICs with an IPv6 address using Add- AzNetworkInterfaceIpConfig"
Source: https://docs.microsoft.com/en-us/azure/load-balancer/ipv6-add-to-existing-vnet-powershell

Question: 88

HOTSPOT

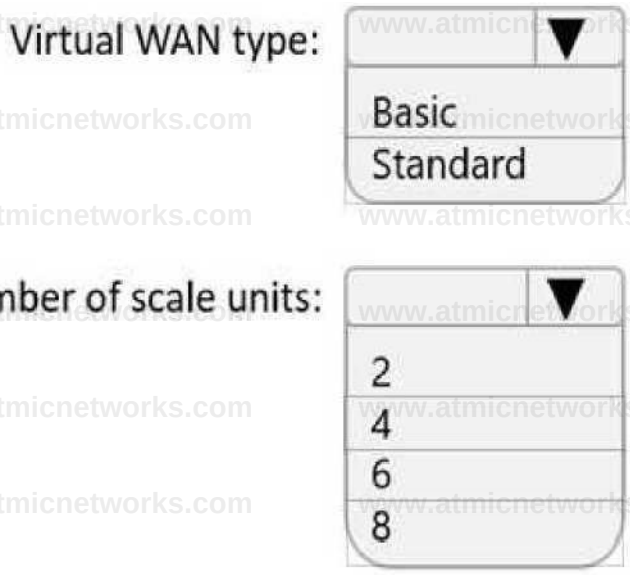
You plan to deploy Azure Virtual WAN.

You need to deploy a virtual WAN hub that meets the following requirements:

Supports 10 sites that will connect to the virtual WAN hub by using a Site-to-Site VPN connection
Supports 8 Gbps of ExpressRoute traffic
Minimizes costs

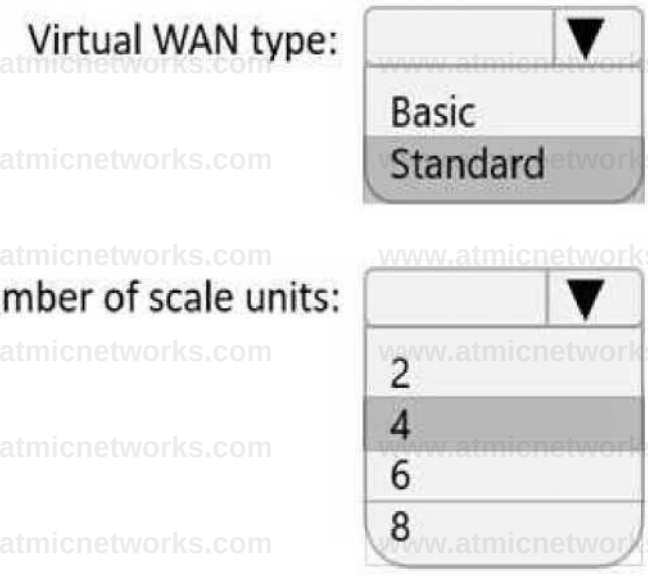
What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Question: 89

DRAG DROP

You have two Azure virtual networks named Hub1 and Spoke1. Hub1 connects to an on-premises network by using a Site-to-Site VPN connection.

You are implementing peering between Hub1 and Spoke1.

You need to ensure that a virtual machine connected to Spoke1 can connect to the on-premises network through Hub1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Explanation:

```
$hub Get-AZVirtualNetwork ResourceGroup "RG1" Mame "Hubl"
$spoke – Get-AZVirtualNetwork -ResourceGroup "RG2" Name "Spokel"
Add-AZVirtualNetworkPeering -Name "Hubl-Spokel" -VirtualNetwork Shub
                -RemoteVirtualNetworkld Sspoke.id -Al I wGatewayTransit
Add AZVirtualNetworkpeering -Name "Spoke 1-HubI" -VirtualNetwork $spoke
                ■RemoteVirtualNetworkld Shub.id UseRemoteGateways
```

Reference:
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid- networking/hub-spoke?tabs=cli#virtual-network-peering

Question: 90

DRAG DROP

You have three on-premises sites. Each site has a third-party VPN device.

You have an Azure virtual WAN named VWAN1 that has a hub named Hub1. Hub1 connects two of the three on-premises sites by using a Site-to-Site VPN connection.

You need to connect the third site to the other two sites by using Hub1.

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

Actions	Answer Area
Download the VPN configuration file from VWAN1	
In a Hub1. create a VPN gateway	
In a Hub1, create a VPN site	
In a Hub1, create a connection to the VPN site	
Configure the VPN device	

Answer:

Explanation:

In a Hub1, create a VPN site

In a Hub1, create a connection to the VPN site

Download the VPN configuration file from VWAN1

Configure the VPN device

Reference:
https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-site-to-site-portal

Question: 91

HOTSPOT

You are planning an Azure solution that will contain the following types of resources in a single Azure region:

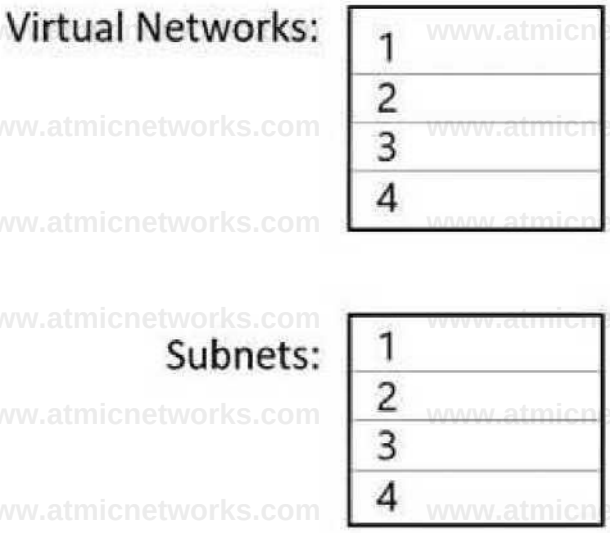
Virtual machine
Azure App Service
Virtual Network gateway
Azure SQL Managed Instance

App Service and SQL Managed Instance will be delegated to create resources in virtual networks.

You need to identify how many virtual networks and subnets are required for the solution. The solution must minimize costs to transfer data between virtual networks.

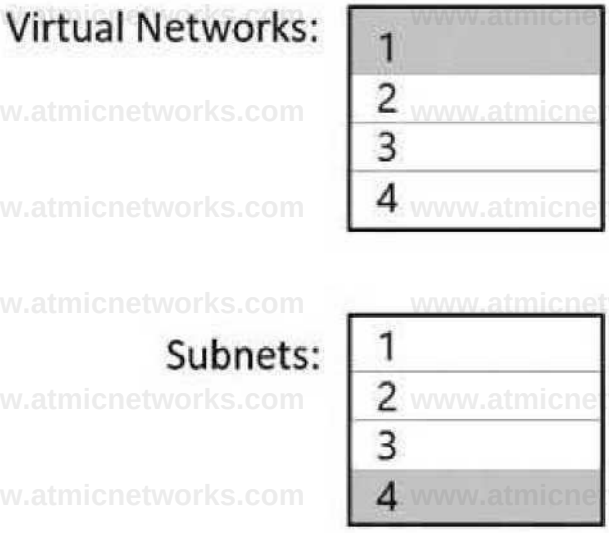
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:



https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure- services#services-that-can-be-deployed-into-a-virtual-network

Question: 92

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 two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit.

Vnet2 can use the remote gateway.

You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communicate with Vnet2.

Solution: You download and reinstall the VPN client configuration.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

The VPN client must be downloaded again if any changes are made to VNet peering or the network topology.

Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site-routing

Question: 93

HOTSPOT

You have an Azure subscription that contains the route tables and routes shown in the following table.

Route table name	Route name	Prefix	Destination
RT1	Default Route	0.0.0.0/0	VirtualNetworkGateway
RT2	Default Route	0.0.0.0/0	Internet

The subscription contains the subnets shown in the following table.

Name	Prefix	Route table	Virtual network
Subnetl	10.10.1.0/24	RT1	Vnetl
Subnet2	10.10.2.0/24	RT2	Vnetl
GatewaySubnet	10.10.3.0/24	None	Vnetl

The subscription contains the virtual machines shown in the following table.

Name	IP address
VM1	10.10.1.5
VM2	10.10.2.5

There is a Site-to-Site VPN connection to each local network gateway.

For each of the following statements, select Yes of the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN Q connection	○	
Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection Q		
Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN O connection	○	

Answer: ○

Explanation:

Statements	Yes	No
Traffic from VM2 to the internet is routed through the New-York Site-to-Site VPN connection	○	○

Traffic from VM1 to VM2 is routed through the New-York Site-to-Site VPN connection Q

Traffic from VM1 to the internet is routed through the New-York Site-to-Site VPN connection

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

Question: 94

You have an Azure application gateway named AGW1 that has a routing rule named Rule1. Rule 1 directs traffic for http://www.contoso.com to a backend pool named Pool1. Pool1 targets an Azure virtual machine scale set named VMSS1.

You deploy another virtual machine scale set named VMSS2.

You need to configure AGW1 to direct all traffic for http://www.adatum.com to VMSS2.

The solution must ensure that requests to http://www.contoso.com continue to be directed to Pool1.

Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add a backend pool.
B. Modify an HTTP setting.
C. Add an HTTP setting.
D. Add a listener.
E. Add a rule.

Answer: ADE

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/configuration-overview

Question: 95

HOTSPOT

You have an Azure Traffic Manager parent profile named TM1. TM1 has two child profiles named TM2 and TM3.

TM1 uses the performance traffic-routing method and has the endpoints shown in the following table.

Name	Location
App1	North Europe
App2	East US
App3	Central US
TM2	West Europe
TM3	West US

TM2 uses the weighted traffic-routing method with MinChildEndpoint = 2 and has the endpoints shown in the following table.

Name	Location	Weight
App4	West Europe	99
App5	West Europe	1

TM3 uses priority traffic-routing method and has the endpoints shown in the following table.

Name	Location
App6	West US
App2	East US

The App2, App4, and App6 endpoints have a degraded monitoring status.

To which endpoint is traffic directed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Traffic from West Europe:

Traffic from West US:

Answer:

Explanation:

Traffic from West Europe:

Traffic from West US:

Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-nested-profiles

Traffic from West Europe:

Basedd on TM1 table, West Europe will trigger TM2. However, as the MinChildEndpoint is set to 2, and App4 is degraded (down), the entire TM2 will not be considered available.

This goes back to the origin TM1 that uses performance traffic-routing method, which means the closest location is App1 and naturally be the next best performance instance.

Hence, Answer = App1

Traffic from West US:

Based on TM1 table, West US will trigger TM3. However, both App2 and App6 were degraded (down), so none of them can be considered.

This goes back to the original TM1 that uses performance traffic-routing method, from TM1, the other 2 US locations would be App2 and App3. But App2 we know it's already degraded (unavailable), hence the only option would be App3.

Answer = App3

Question: 96

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.

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

Solution: You add a rewrite rule for the host header.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/application-gateway/rewrite-http-headers-url#limitations

Question: 97

HOTSPOT

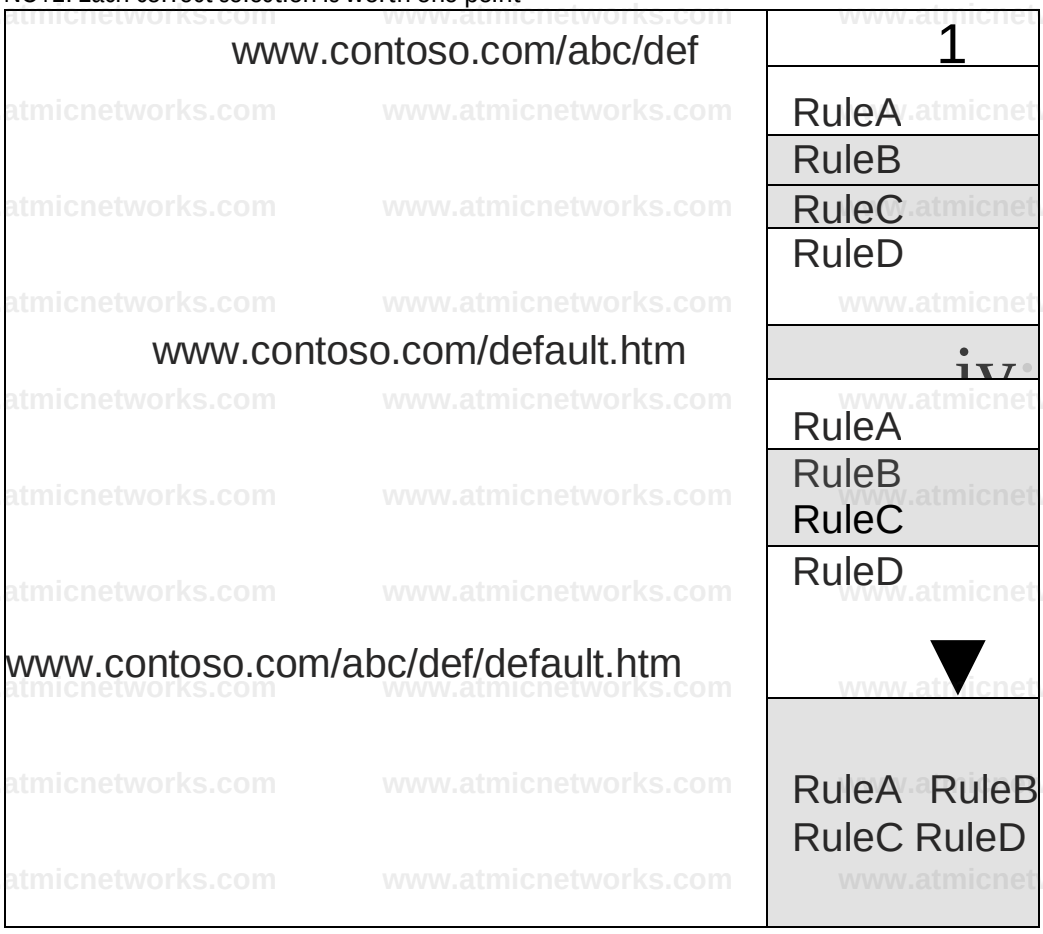
You have an Azure Front Door instance that provides access to a web app. The web app uses a hostname of www.contoso.com.

You have the routing rules shown in the following table.

Name	Path
RuleA	/abc/def
RuleB	/ab
RuleC	/*
RuleD	/abc/'

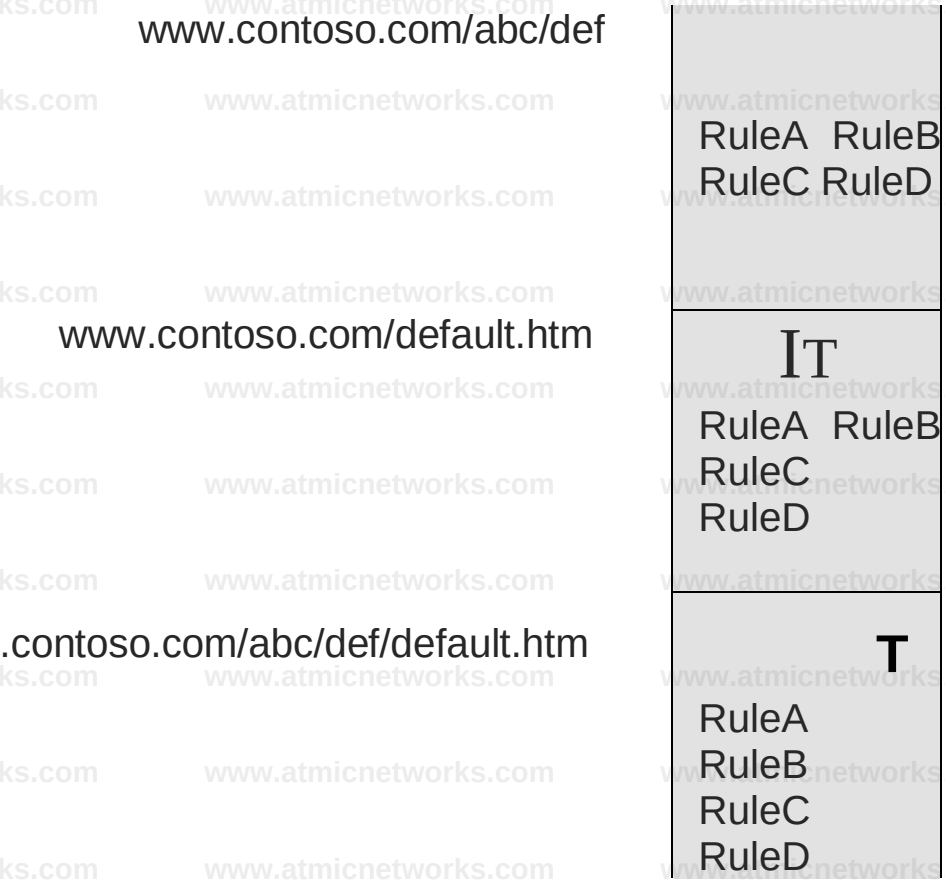
Which rule will apply to each incoming request? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point



Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-route-matching

Question: 98

You have an Azure subscription that contains an Azure App Service app. The app uses a URL of https://www.contoso.com.

You need to use a custom domain on Azure Front Door for www.contoso.com. The custom domain must use a certificate from an allowed certification authority (CA).

What should you include in the solution?

A. an enterprise application in Azure Active Directory (Azure AD)
B. Active Directory Certificate Services (AD CS)
C. Azure Key Vault
D. Azure Application Gateway

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-custom-domain-https

Question: 99

HOTSPOT

You have an Azure virtual network named Vnet1 that contains two subnets named Subnet1 and Subnet2.

You have the NAT gateway shown in the NATgateway1 exhibit.

You have the virtual machine shown in the VM1 exhibit.

VM1 ^

Virtual macnme

O Connect ► Start Q¹ Restart ■ Stop & Capture 0 Delete 0 Refresh

^ Essentials

Resource group (change)
RG1

Status
Running

Location
North Europe (Zone 2)

Subscription (change)
Subscription!

Subscription ID
489f2hht-se7y-987v-g571-463hw3679512

Availability zone
2

Tags (change)
Click here to add tags

Operating system
Windows

Size
Standard B1s (1 vcpus, 1 GiB memory)

Public IP address

Virtual network/subnet
Vnet1/Subnet1

DNS name

Subnet1 is configured as shown in the Subnet1 exhibit.

Subnetl

Vnetl

Name

Subnetl

Subnet address range ‘

10.100.1.0/24

10.100.1.0 - 10.100.1.255 (251 + 5 Azure reserved addresses

] Add IPv6 address space 0

NAT gateway

NATgatewayl xz

Network security group

None xz

Route table

RouteTablel xz

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services Q

Microsoft.Storage xz

Service	Status
Microsoft.Storage	Succeeded

Service endpoint policies

0 selected \z

SUBNET DELEGATION

Delegate subnets to a service Q

None

For each of the following statements, select Yes of the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can communicate outbound by using NATgatewayl	○	○
The virtual machines in Subnet? communicate outbound by using NATgatewayl	○	○
All the virtual machines that use NATgatewayl to connect to the internet use the same public IP address	○	○

Answer:

Explanation:

Statements	Yes	No
The virtual machines in Subnet? communicate outbound by using NATgatewayl	○	○
VM1 can communicate outbound by using NATgatewayl	○	○
All the virtual machines that use NATgatewayl to connect to the internet use the same public IP address	○	○

Box 1: No

VM1 is in Zone2 whereas the NAT Gateway is in Zone1. The VM would need to be in the same zone as the NAT Gateway to be able to use it. Therefore, VM1 cannot use the NAT gateway.

Box 2: Yes

NATgateway1 is configured in the settings for Subnet2.

Box 3: No

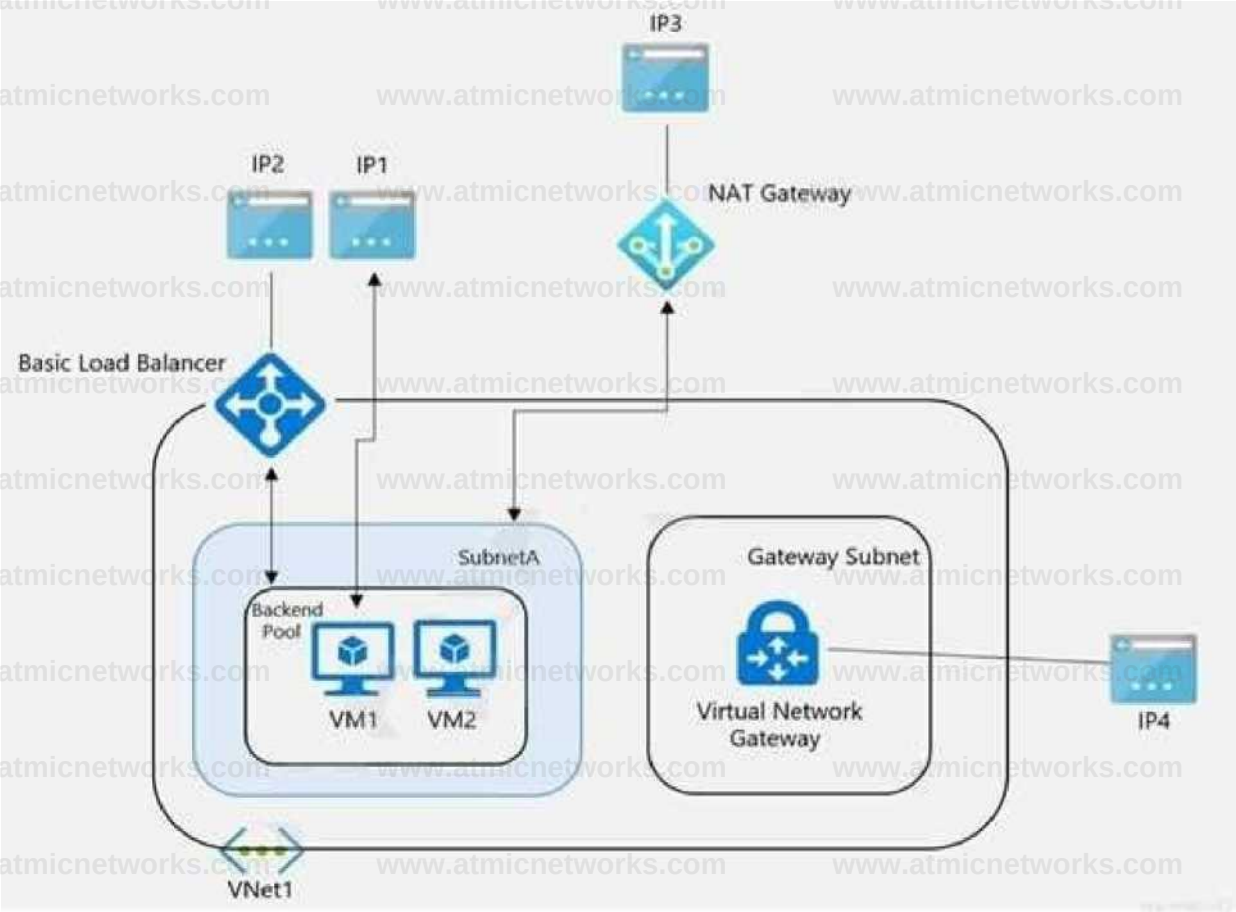
The NAT gateway does not have a single public IP address, it has an IP prefix which means more than one IP address. The VMs the use the NAT Gateway can use different public IP addresses contained within the IP prefix.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource

Question: 100

You have the Azure environment shown in the exhibit.



VM1 is a virtual machine that has an instance-level public IP address (ILPIP).

Basic Load Balancer uses a public IP address. VM1 and VM2 are in the backend pool.

NAT Gateway uses a public IP address named IP3 that is associated to SubnetA.

VNet1 has a virtual network gateway that has a public IP address named IP4.

When initiating outbound traffic to the internet from VM1, which public address is used?

A. IP1
B. IP2
C. IP3
D. IP4

Answer: A

Explanation:

Question: 101

You plan to publish a website that will use an FQDN of www.contoso.com. The website will be hosted by using the Azure App Service apps shown in the following table.

Name	FQDN	Location	Public IP address
AS1	Asl.contoso com	East US	131 107 100 1
AS2	As2 contoso com	West US	131 107 200 1

You plan to use Azure Traffic Manager to manage the routing of traffic for www.contoso.com between AS1 and AS2.

You need to ensure that Traffic Manager routes traffic for www.contoso.com.

Which DNS record should you create?

A. two A records that map wmv.contoso.com to 131 107 100 1 and 131 107 200 1
B. a CNAME record that maps www.contoso.com to TMprofile1.azurefd.net
C. a CNAME record that mapswww.contoso.comtoTMprofile1.trafficmanager.net
D. a TXT record that contains a string ofas1.contoso.com and as2.contoso.com in the details

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/quickstart-create-traffic-manager-profile
https://docs.microsoft.com/en-us/azure/app-service/configure-domain-traffic-manager

Question: 102

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.

'twltufi'I ■2B?j-«-02T!ilJJin»KiCO*i
•ruaoutolQ-j •/KfMCITP?ia»tt/l0M?hlit-a«7y-MTv-i>5?I-4*l!«147»517<m3OWCr<»»M/MI/P»C*/3BEM/incftMOrr.«HWW[/APM.ICAno<IG*mr*Yfl/*£»I *Op»rttl<MI#«W*:
"ftppllaHlM6ftC«W4yfll9iMH*t
•<M •qnry*; • App |H«t I <xn><«C way Y1 raw* 11 Uq*.
•ptcpertiaCs I
"laitance! J" J 'iivr# 0*, MUMl^: •l#M>MMe.
*/#itm#m*i
■raquwtUrl-r •/loqln'i
"rwl»8ctTyp*-t "OWAJFJW, "tult >* r.v«r r lna'i *'J.C.0*4
"ruUIP-i ••7&JM-,

"w^saqe-i -Request Musing an Accept Hr«d»f*(
"actLofTr "NBtCbMl*"
•ftHft*! ■QJdM>*t
MKftiU"! I
•w«i»5e*l "Wainimj. KatCb •£ WVfa ftppMMMtlt. MxkeidWV wiiMlt *BXqUESTJKAC£fl;D*«r~Ai)«nt\W MaUtd. *(MaU'i "p
•HUa: *euU«VMXW7•W-R0WOL'tMK^MtMT.wnt\
•Hw*' •twit
•ho»t naw': #appl«po<itWP*MB-4
•triM<cU«l<ri •t7M41B9yUi)k?V4U4B€aitSi3ltWiP~,
"policy 14'J "deIndf, *policy$ccp*®r %l-4>al*» "peyjLirYSwpalUar: *Gl4bai*•

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

Solution: You create a WAF policy exclusion for request headers that contain 137.135.10.24.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The parameter here should be RemoteAddr not Request header. https://docs.microsoft.com/en- us/azure/web-application-firewall/ag/custom-waf-rules-overview#match-variable-required

Question: 103

You have an Azure Web Application Firewall (WAF) policy in prevention mode that is associated to an Azure Front Door instance.

You need to configure the policy to meet the following requirements:

Log all connections from Australia.
Deny all connections from New Zealand.
Deny all further connections from a network of 131.107.100.0/24 if there are more than 100 connections during one minute.

What is the minimum number of objects you should create?

A. three custom rules that each has one condition
B. one custom rule that has three conditions
C. one custom rule that has one condition
D. one rule that has two conditions and another rule that has one condition

Answer: A

Explanation:
Reference:

https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

Question: 104

You have an Azure subscription that contains multiple virtual machines in the West US Azure region.

You need to use Traffic Analytics.

Which two resources should you create? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct answer selection is worth one point.

A. an Azure Monitor workbook
B. a Log Analytics workspace
C a storage account
D. an Azure Sentinel workspace
E. an Azure Monitor data collection rule

Answer: BC

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

A storage acccount is used to store network security group flow logs.

A Log Analytics workspace is used by Traffic Analytics to store the aggregated and indexed data that is then used to generate the analytics.

https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics#enable-flow-log-settings

Question: 105

HOTSPOT

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Connected to
VM1	Vnet1/Subnet1
VM2	Vnet1/Subnet2

Subnet1 and Subnet2 are associated to a network security group (NSG) named NSG1 that has the following outbound rule:

Priority: 100
Port: Any
Protocol: Any
Source: Any
Destination: Storage
Action: Deny

You create a private endpoint that has the following settings:

Name: Private1
Resource type: Microsoft.Storage/storageAccounts
Resource: storage1
Target sub-resource: blob
Virtual network: Vnet1
Subnet: Subnet1

For each of the following statements, select Yes of the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
From VM2, you can create a container in storagel	○	○
From VM1, you can upload data to a blob storage container in storagel	○	○
From VM2, you can upload data to a blob storage container in storagel	○	○

Answer:

Explanation:

Yes, Yes, Yes

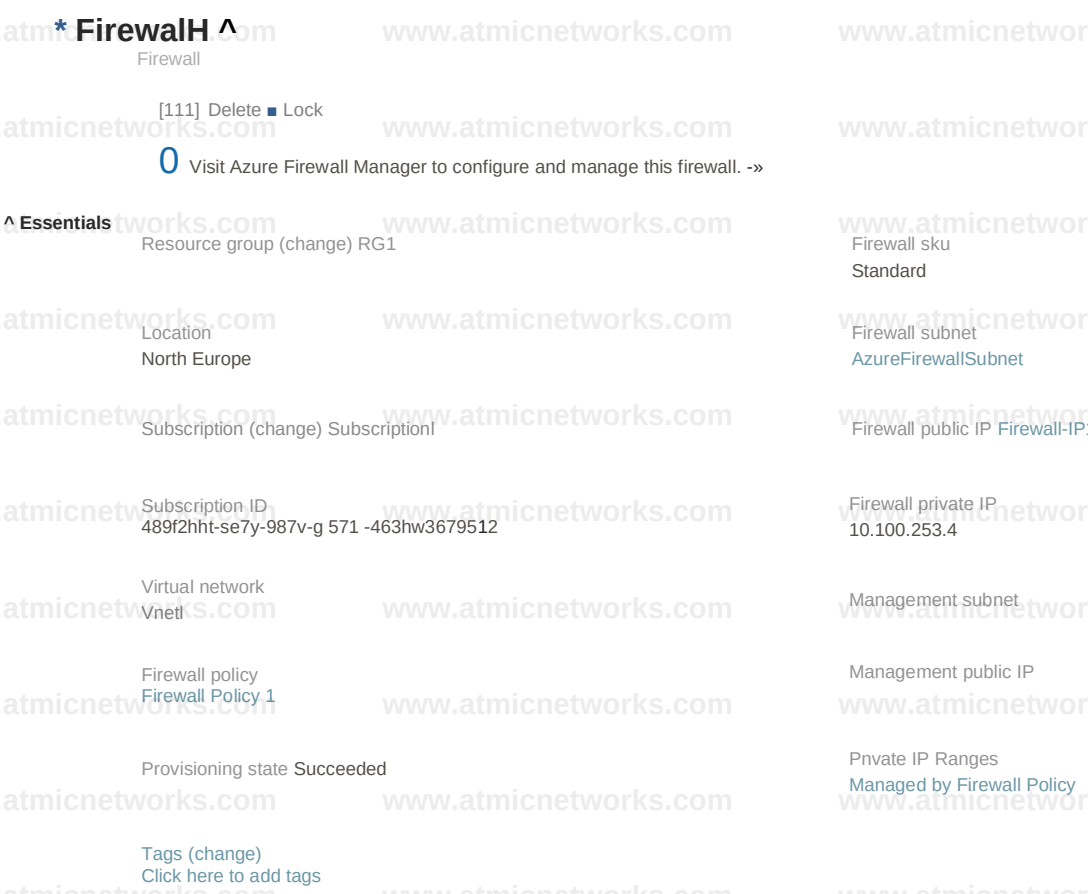
NSG rules applied to the subnet hosting the private endpoint are not applied to the private endpoint.So the NSG1 doesn't limit storage access from either VM1 or VM2.

https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints#network- security-group-rules-for-subnets-with-private-endpoints

Question: 106

HOTSPOT

You have an Azure firewall shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

On FirewalH, forced tunneling [answer choice]

is enabled already
cannot be enabled
is disabled but can be enabled

On Firewall!, management by Azure Firewall Manager [answer choice]

is enabled already cannot be enabled
is disabled but can be enabled

Answer:

Explanation:

On Firewalll, forced tunneling [answer choice]

is enabled already
cannot be enabled
is disabled but can be enabled

On Firewalll, management by Azure Firewall Manager [answer choice]

is enabled already
cannot be enabled
is disabled but can be enabled

Box 1:
If forced tunneling was enabled, the Firewall Subnet would be named AzureFirewallManagementSubnet. Forced tunneling can only be enabled during the creation of the firewall. It cannot be enabled after the firewall has been deployed.

Box 2:
The "Visit Azure Firewall Manager to configure and manage this firewall" link in the exhibit shows that the firewall is managed by Azure Firewall Manager.

Question: 107

You have a hybrid environment that uses ExpressRoute to connect an on-premises network and Azure.

You need to log the uptime and the latency of the connection periodically by using an Azure virtual machine and an on-premises virtual machine.

What should you use?

A. Azure Monitor
B. IP flow verify
C. Connection Monitor
D. Azure Internet Analyzer

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor

Question: 108

You have an Azure subscription that contains the following resources:

A virtual network named Vnet1
Two subnets named subnet1 and AzureFirewallSubnet
A public Azure Firewall named FW1
A route table named RT1 that is associated to Subnet1
A rule routing of 0.0.0.0/0 to FW1 in RT1

After deploying 10 servers that run Windows Server to Subnet1, you discover that none of the virtual machines were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

A. Deploy an application security croup mat allows outbound traffic to 1688.
B. Deploy an Azure Standard Load Balancer that has an outbound NAT rule
C. On fW1.configure a DNAT rule for port 1688.
D. Add an internet route to RI1 for the Azure Key Management Service (KMS).

Answer: D

Explanation:
Reference:
https://ryanmangansitblog.com/2020/05/11/firewall-considerations-windows-virtual-desktop-wvd/

Question: 109

You have an Azure virtual network that contains a subnet named Subnet1. Subnet1 is associated to a network security group (NSG) named NSG1. NSG1 blocks all outbound traffic that is not allowed explicitly.

Subnet1 contains virtual machines that must communicate with the Azure Cosmos DB service.

You need to create an outbound security rule in NSG1 to enable the virtual machines to connect to Azure Cosmos DB.

What should you include in the solution?

A. a service tag
B. a private endpoint
C. a subnet delegation
D. an application security group

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview

Question: 110

DRAG DROP

You have an Azure virtual network named Vnet1 that connects to an on-premises network.
You have an Azure Storage account named storageaccount1 that contains blob storage.

You need to configure a private endpoint for the blob storage. The solution must meet the following requirements:

Ensure that all on-premises users can access storageaccount1 through the private endpoint.
Prevent access to storageaccount1 from being interrupted.

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

Actions	Answer Area
Install the DNS server role and configure the forwarding ot blob.core.windows.net to 168.63.129.16	
Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine	
Configure a private endpoint on storageaccountl and disable public access to the account	
Configure on-premises DNS server to forward blob.core.windows.net to 168.63.129.16	
Deploy a virtual machine to a subnet in Vnetl	

Answer:

Explanation:

Configure a private endpoint on storageaccount1 and disable public access to the account
Deploy a virtual machine to a subnet in Vnet1
Install the DNS server role and configure the forwarding of blob.core.windows.net to 168.63.129.16
Configure on-premises DNS servers to forward blob.core.windows.net to the virtual machine

168.63.129.16 is the IP address of Azure DNS which hosts Azure Private DNS zones. It is only accessible from within a VNet which is why we need to forward on-prem DNS requests to the VM running DNS in the VNet. The VM will then forward the request to Azure DNS for the IP of the storage account private endpoint.

Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints

Question: 111

You have an Azure virtual network named Vnet1 that has one subnet. Vnet1 is in the West Europe Azure region.

You deploy an Azure App Service app named App1 to the West Europe region.

You need to provide App1 with access to the resources in Vnet1. The solution must minimize costs.

What should you do first?

A. Create a private link.
B. Create a new subnet.
C. Create a NAT gateway.
D. Create a gateway subnet and deploy a virtual network gateway.

Answer: D

Explanation:
Virtual network integration depends on a dedicated subnet.

https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration#regional-virtual- network-integration

For outgoing traffic from Web App to vnet, it will go through Internet, so the cost not the minimum.

The connection between the Private Endpoint and the Web App uses a secure Private Link. Private Endpoint is only used for incoming flows to your Web App. Outgoing flows will not use this Private Endpoint, but you can inject outgoing flows to your network in a different subnet through the VNet integration feature.

https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint#conceptual- overview

Question: 112

You are planning the IP addressing for the subnets in Azure virtual networks. Which type of resource requires IP addresses in the subnets?

A. Azure Virtual Network NAT
B. virtual network peering
C. service endpoints
D. private endpoints

Answer: D

Explanation:

Question: 113

You have Azure App Service apps in the West US Azure region as shown in the following table.

Name	App Service plan	Number of instances
Appl	ASP1	3
App2	ASP1	3
App3	ASP2	2
App4	ASP3	1

You need to ensure that all the apps can access the resources in a virtual network named Vnet1 without forwarding traffic through the internet-How many integration subnets should you create?

A. 0
B. 1
C. 3
D. 4
E. 6

Answer: C

Explanation:

One integration subnet is required per App Service Plan regardless of how many apps are running in the App Service Plan.

Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration

Question: 114

HOTSPOT

You have the Azure environment shown In the Azure Environment exhibit. (Click the Azure Environment tab.) The settings for each subnet are shown in the following table.

Subnet	Service endpoint
Vnetl/Subnet 1	Storage
.:i-	Storage
Vnet2/Subnet1	None

The Firewalls and virtual networks settings for storage1 are configured as shown in the Storage1 exhibit. (Click the Storage1 tab.) For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM1 can access storage!.	O	O
VM2 can access storage! by using aservice endpoint.	O	O
VM3 can access storage! by using thepublic IP address.	O	O

Answer:

Explanation:

Statements	Yes	No
VM1 can access storagel.		
VM2 can access storagel by using a service endpoint.	O	O
VMS can access storagel by using the public IP address.	O	O

Question: 115

HOTSPOT

You have the network topology shown in the Topology exhibit. (Click the Topology tab.)

You have the Azure firewall shown in the Firewall 1 exhibit. (Click the Firewall tab.)

All services Firewalls

FirewalH

Firewall

» a Delete S Lock

o V«*4 Azure Firewall Manager to configura and manage fhrt Firewall —^

zx Essentials

JSON View

Resource group (change) RG2
Location
North Europe
Subscription (change)
Visual Studio Premium with MSDN
Subscription ID
837?f433-2dcd 4361 bSef 5bl88fed87d0
Virtual network
Vnetl
Firewall policy
FirewallPolicy
Provisioning state
Succeeded
Tags (change)
Click here to add tags

Firewall sku
Standard
Firewall subnet
AzureFirewallSubnet
Firewall public IP
FirewalH IP1
Firewall private IP
10.100.253.4
Management subnet
Management public IP
Private IP Ranges
Managed by Firewall Policy

You have the route table shown in the RouteTable1 exhibit. (Click the RouteTable1 tab.)

All services > Route tables >

J* RouteTablel ^ — X

Route table

» —> Move xz ® Delete O Refresh Pr Give feedback

" Essentials

JSON View

Resource group (change)
RG1
Location
North Europe
Subscription (change) Visual Studio Premium with MSDN
Subscription ID
8372f433-2dCd-4361 -b5ef- 5b 188fed87dO
Tags (change) Click here to add tags

Associations
1 subnet associations

Routes

r^^^earcbTroutes Name	T4, Address prefix	T4. Next hop type	T4. Next hop IP address T^	
Route 1	10.1.0.0/16	Virtual network gateway	•	•••
Route2	0.0.0.0/0	Virtual appliance	10.100.253.4	•••

Subnets | Search subnets

Name	T^, Address range	T^ Virtual network	*4. Security group	tj.
Subnet!	10.100.1.0/24	Vnetl	•	•••

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements			Yes	No
The resources in Subnetl can	connect to the	internet through Firewall 1.	O	O
The resources tn Subnetl can	connect to the	resources in VnetZ		
The resources in Subnets can	connect to the	internet through Firewall!.	O	O

Answer:

Explanation:

Answer Area

Statements		Yes	No
The resources in Subnetl can connect to the internet through	Firewall!	•	O
The resources in Subnet! can connect to the resources in Vnet2.		®	
The resources in Subnet2 can connect to the internet through	Firewall!.	a	o

Question: 116

HOTSPOT

You have two Azure virtual networks named Vnet1 and Vnet2 in an Azure region that has three availability zones.

You deploy 12 virtual machines to each virtual network, deploying four virtual machines per zone.

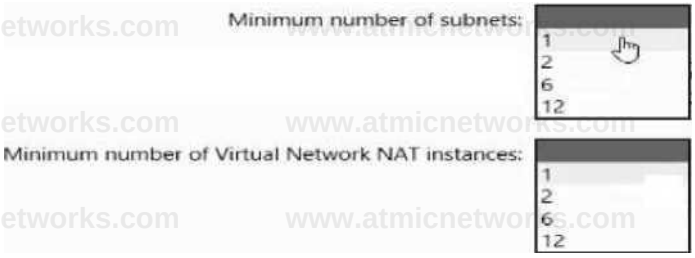
The virtual machines in Vnet1 host an app named App1. The virtual machines in Vnet2 host an app named App2.

You plan to use Azure Virtual Network NAT to implement outbound connectivity for App1 and App2. You need to identify the minimum number of subnets and Virtual Network NAT instances required to meet the following requirements:

- A failure of two zones must NOT affect the availability of either App1 or App2.
- A failure of two zones must NOT affect the outbound connectivity of either App1 or App2.

What should you identify? To answer, select the appropriate options in the answer are a.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Minimum number of subnets:

1
2
6
12

Minimum number of Virtual Network NAT instances:

1
2
6
12

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview

Question: 117

You have an Azure virtual network named Vnet1 and an on-premises network.

The on-premises network has policy-based VPN devices. In Vnet1, you deploy a virtual network gateway named GW1 that uses a SKU of VpnGw1 and is route-based.

You have a Site-to-Site VPN connection for GW1 as shown in the following exhibit.

You need to ensure that the on-premises network can connect to the route-based GW1. What should you do before you create the connection?

A. Set Use Azure Private IP Address to Enabled
B. Set IPsec / IKE policy to Custom.
C. Set Connection Mode to ResponderOnly
D. Set BGP to Enabled

Answer: D

Explanation:

Question: 118

Your company has offices in Montreal. Seattle, and Paris. The outbound traffic from each office originates from a specific public IP address.

You create an Azure Front Door instance named FD1 that has Azure Web Application Firewall (WAF) enabled.

You configure a WAF policy named Policy! that has a rule named Rule1. Rule1 applies a rate limit of 100 requests for traffic that originates from the office in Montreal.

You need to apply a rate limit of 100 requests for traffic that originates from each office.

What should you do?

A. Modify the conditions of Rule1.
B. Create two additional associations.
C. Modify the rule type of Rule1.
D. Modify the rate limit threshold of Rule1.

Answer: A

Explanation:

https://techcommunity.microsoft.com/t5/azure-network-security-blog/rate-limiting-feature-for- azure-waf-on-application-gateway-now/ba-p/3934957#:~:text=Rate%20limiting%20is%20configured%20using,and%20a%20group%20by%20var iable.

Question: 119

You have an Azure virtual network named Vnet1 that hosts an Azure firewall named FW1 and 150 virtual machines. Vnet1 is linked to a private DNS zone named contoso.com. All the virtual machines have their name registered in the contoso.com zone.

Vnet1 connects to an on-premises datacenter by using ExpressRoute.

You need to ensure that on-premises DNS servers can resolve the names in the contoso.com zone.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. On the on-premises DNS servers, configure forwarders that point to the frontend IP address of FW1.
B. On the on-premises DNS servers, configure forwarders that point to the Azure provided DNS service at 168.63.129.16.
C. Modify the DNS server settings of Vnet1.
D. For FW1, enable DNS proxy.
E. For FW1, configure a custom DNS server.

Answer: AD

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns#on-premises-workloads- using-a-dns-forwarder

https://azure.microsoft.com/en-gb/blog/new-enhanced-dns-features-in-azure-firewall-now- generally-available/

Question: 120

You are planning the IP addressing for the subnets in Azure virtual networks.

Which type of resource requires IP addresses in the subnets?

A. internal load balancers
B. storage account
C. serviice endpoints
D. service endpoint policies

Answer: A

Explanation:

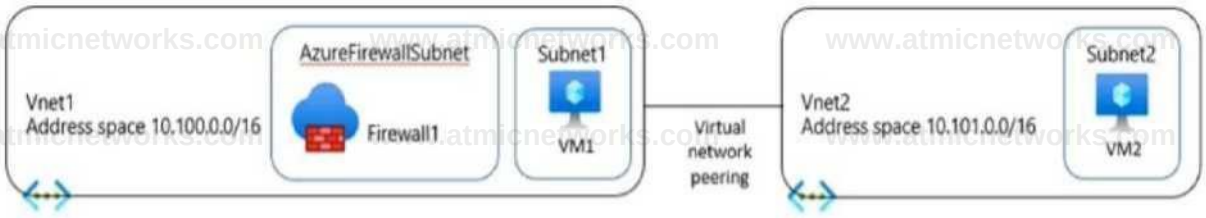
Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

Question: 121

HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.

Name	Type
VnetI	Virtual network
Vnet2	Virtual network
FirewallI	Azure Firewall
Subnet 1	Virtual subnet
Subnet?	Virtual subnet
VM1	Virtual machine
VM2	Virtual machine

The virtual network topology is shown in the following exhibit.



Firewall1 is configured as shown in following exhibit.

Firewalll ^ -

Furnull

» 1 Delete □ lock

0 WM Aaaef mwa ■ Manager to c&n'gure and manage th# f»e*»[1] -*

^ Essentials

Resource group (change)
RG1

Location
North Europe

Subscription (change)
Subscription1

Virtual network
Vnet1

Firewall policy
FirewallPolicy1

Provisioning state
Succeeded

Tags (change)
Click here to add tags

Firewall sku
Standard

Firewall subnet
AzureFirewallSubnet

Firewall public IP
Firewall1-IP1

Management subnet
-

Management public IP
-

Private IP Ranges
Managed by Firewall Policy

FirewallPolicy1 contains the following rules:

- Allow outbound traffic from Vnet1 and Vnet2 to the internet.
- Allow any traffic between Vnet1 and Vnet2.

No custom private endpoints. service endpoints. routing tables, or network security groups (NSGs) were created. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No

A routing table must be associated with Subnetl and Subnets to ensure that all internet traffic for VM1 and VM2 is sent via Firewall!.

The enable remote gateway setting must be enabled on the virtual net peering to provide VM2 Internet access by using Firewall!.

Firewalll can be configured to limit access to websites by categories.

Answer:

Explanation:

Answer:

Answer ATM

Statement!	I--------1	Yes	No
A touting table mull be associated with Subnet! and Subnet? to onsumihit all internet traffic for VM1 and VM2 » sent w* f irewall!.			
The enable remote gateway setting must be enabled on the virtual net peering to provide I VM2 I met net access by uung Frewolll Firewall 1			
can be configured to limit access to websites by categories		Ci	

Question: 122

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.
RG1 contains an Azure Network Watcher instance named NW1.

You need to ensure that Admin1 can place a lock on NW1. The solution must use the principle of least privilege.
Which role should you assign to Admin1?

A. User Access Administrator
B. Network Contributor
C. Resource Policy Contributor
D. Monitoring Contributor

Answer: A

Explanation:

Question: 123

You need to use Traffic Analytics to monitor the usage of applications deployed to Azure virtual machines.
Which Azure Network Watcher feature should you implement first?

A. Connection monitor

B. Packet capture

C. NSG flow logs

D. IP flow verify

Answer: C

Explanation:

Question: 124

HOTSPOT

You have two Azure subscriptions named Subscription1 and Subscription2.

There are no connections between the virtual networks in two subscriptions.

You configure a private link service as shown in the privatelinkservice1 exhibit. (Click the privatelinkservice1 tab.)

You create a load balancer name in Subscription1 and configure the backend pool shown in the lb1 exhibit. (Click tie 1b1 tab.)

You create a private endpoint in Subscription2 as shown in the privateendpoint4 exhibit. (Click the privateendpoint4)

For each of the following statements, select YES if the statement is true. Otherwise. select No.

Statements	Ye*	No
The resources that mil be accessed by using prtvatelinkservicei must be added to backendpool 1 on LB1		
Users in Subscription^ can connect to the resource* published by pnvatelinkserwcel by using IP address 103 0.7.		
The private endpoint must be approved by an administrator in Subscription 1		

Answer:

Explanation:

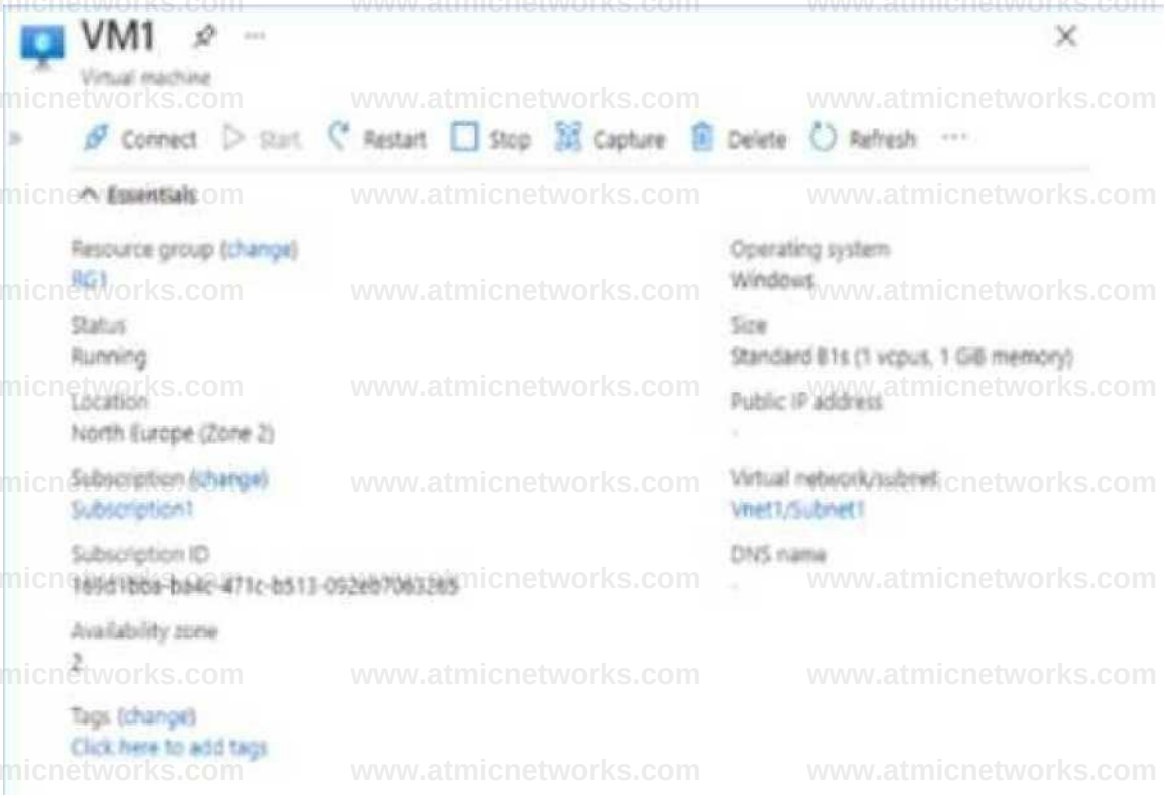
Yes, Yes, No

Question: 125

HOTSPOT

You have an Azure virtual network named Vnet1 that contains two subnets named Subnet1 and Subnet2. You have the NAT gateway shown in the NATgateway1 exhibit, (Click the NATgateway1 tab)

You have the virtual machine shown in the VM1 exhibit, (Click the VM1 tab)



Subnet1 is configured as shown in the Subnet1 exhibit, (Click the Subnet1 tab)

Subnetl

For each of the following statements, select Yes if the statement is true. Otherwise, select No

Statement*	Vet No
VMl car cor^ur ate o^w^a Oy usrg NATggtewsyl-	(C
f« . n_j Tae r« r Secret* cc^* »r cate ouBOOuro oy .c *g NAtgatewr/T	

A ire * 4u* macr r« tut use SA'cetew*/ to correct to ire -ferret -te tie jene Puo < ' aoereis.

Answer:

Explanation:

Yes, Yes, No

Question: 126

You have an Azure subscription that is linked to an Azure AD tenant named contoso.onmicrosoft.com. The subscription contains the following resources:

- A virtual network named Vnet1
- An App Service plan named ASPI
- An Azure App Service named webapp1
- An Azure private DNS zone named private.contoso.com
- Virtual machines on Vnet1 that cannot communicate outside the virtual network

You need to ensure that the virtual machines on Vnet1 can access webapp1 by using a URL of https:/Avwwprivate.contosocom.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a private endpoint for webapp1.

B. Create a service endpoint for webapp1.

C. Create a CNAME record that maps www.pnvate.contoso.com to webapp1.privatelink.azurewebsites.net.

D. Create a CNAME record that maps wwwprivatemntoso.com to webapp1.contoso.onmicrosoft.com.

E. Register an enterprise application in Azure AD for webapp1.

F. Create a CNAME record that maps wow.private.contoso.com to webapp 1 private@ntoso.com.

Answer: AD

Explanation:

Question: 127

You have an Azure subscription that contains the resources is shown in the following table.

Name	Type	BIIIIHS^^^
VNetl	Virtual network	Contains two subnets named Subnetl and Subnet2
VM1	Virtual machine	Connected to Subnetl
azsql!	Azure SQL Database logical server	Has a private endpoint on Subnet? 1

You need to ensure that the apps hosted on VM1 can resolve the IP address of the What should you create first?

A. a public DNS zone named database.windows.net
B. a private DNS zone named database.windows.net
C. a public DNS zone named private ink.database.windows.net
D. a private DNS zone named privatelink.database.windows.net

Answer: D

Explanation:

Question: 128

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure App Service	A web app
Gatewayl	Azure Application Gateway	includes an SSL certificate that has a subject name of k.contoso.com

Gateway1 provides access to App1 by using a URL of http://app1.contoso.com.
You create a new web app named App2.
You need to configure Gateway1 to enable minimize administrative effort.
What should you configure on Gateway1?

A. a backend pool and a routing
B. a listener and a routing rule
C. a listener, a backend pool, and a rule
D. a listener and a backend pool

Answer: B

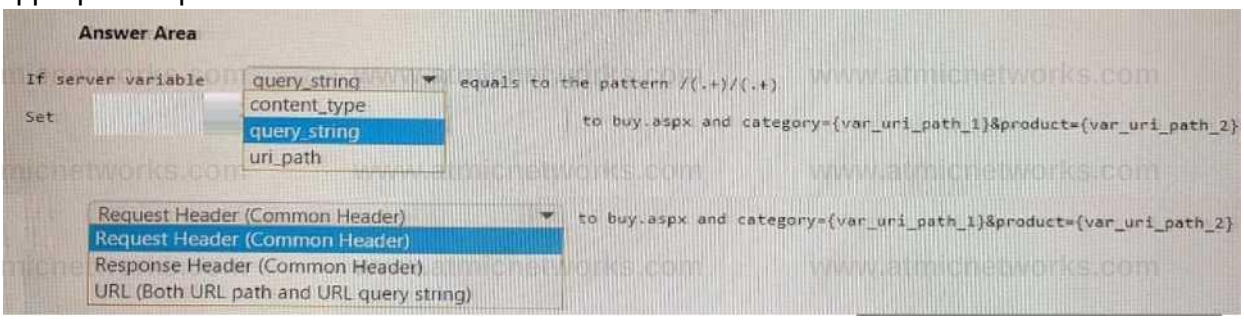
Explanation:

Question: 129

HOTSPOT
You have an Azure application gateway named AppGw1.
You need to create a rewrite rule for AppGw1. The solution must rewrite the URL of requests from https://www.contoso.com/fashion/shirts to ttps://www.contoso.com/buy.aspx?category-

fashion&product=shirts.

How should you complete the rule? To answer NOTE: Each correct selection is worth one point appropriate options in the answer area.



Answer:

Explanation:

Query _string
Request Header (Common Header)

Question: 130

HOTSPOT

You have an Azure subscription that contains the virtual networks.shown in the following table.

Name	Location	IP address space
Vnet1	East US 2	10.5.0.0/16
Vnet2	East US 2	10.3.0.0/16
Vnet3	East US 2	10.4.0.0/16

You have a virtual machine named VM5 that has the following IP address configurations:

- IP address: 10.4.0.5
- Subnet mask:255.255.255.0
- Default gateway:10.4.0.1
- DNSserver:168.63.129.16

You have an Azure Private DNS zone named, fabrikam.com that contains the records shown in, the following table.

Name	Type	Value
app1	CNAME	lb1.fabrikam.com
lb1	A	10.3.0.7
vm1	A	10.3.0.4

The virtual network links in the fabrikam.com DNS /one are configured as shown in the exhibit. (Click the Exhibit tab.)

VMS fails to resolve the IP address for.appKfabrik3in.com.

For each of the following statements, select Yes if, the statement is true. Otherwise, select No.

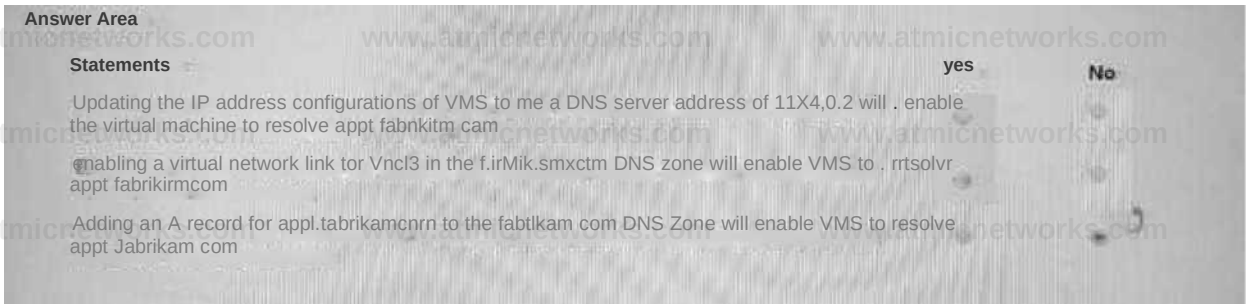
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Updating the IP address configuratio VMS to use DNS server address 10.4.0.2 will enable the virtual machine to resolve app1.fabrikam.com.		
Enabling a virtual network link for VpetS in the 1abnkam.c INS zone will enable VMS to resolve app1 .fabrikam.com.		
Adding an A record for app1.fabrikain.com to the fabnkam.com DNS zone will enable VMS to resolve app1.fabnkam.com.		

Answer:

Explanation:



Question: 131

You have two Azure virtual networks named Vnet1 and Vnet2.

You have a Windows 10 device named Client1 that connects to Vnet1 by using a Point-to-Site (P2S) IKEv2 VPN.

You implement virtual network peering between Vnet1 and Vnet2. Vnet1 allows gateway transit Vnet2 can use the. You discover that Client1 cannot communicate with Vnet2.

You need to ensure that Client1 can communication with Vnet2.

Solution: You resize the gateway of Vnet1 to a larger SKU.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 132

HOTSPOT

You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Virtual network	Subnet	Workload
SQL1	VNetl	Subnetl	Microsoft SQL Server 2019
Webl	VNetl	Subnetl	IIS
Web2	VNetl	Subnet2	IIS
SQL2	VNet2	Subnetl	Microsoft SQL Server 2019
Web3	VNet2	Subnetl	IIS
SQL3	VNet2	Subnet2	Microsoft SQL Server 2019

VNet1 and VNet2 are NOT connected to each other.

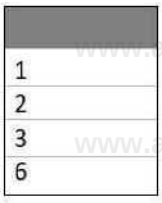
You need to block traffic from SQL Server 2019 to IIS by using application security groups. The solution must minimize administrative effort.

How should you configure the application security groups? To answer, select the appropriate options in the answer area.

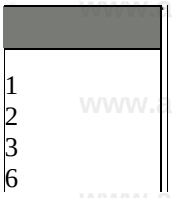
NOTE: Each correct selection is worth one point.

Answer Area:

Minimum number of application security groups:



Minimum number of application security group assignments:



Answer:

Explanation:

2 ASGs e 3 assignments,

"All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in." https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

Question: 133

HOTSPOT

You have an Azure subscription that contains a virtual network gateway named VNetGwy1.

VNetGwy1 has a public IP address of 20.25.32.214.

You need to query the health probe of VNetGwy1,

How should you complete the URI? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer

Explanation:

Answer Area

Question: 134

HOTSPOT

You have an Azure subscription that contains an app named Appl. App1 is hosted on the Azure App Service instances shown in the following table.

You need to implement Azure Traffic Manager to meet the following requirements:

- App1 traffic must be assigned equally to each App Service instance in each Azure region.
- App1 traffic from North Europe must be routed to the Appl instances in the North Europe region.
- App1 traffic from North America must be routed to the Appl instances in the East US Azure region.

Answer Area

Name	Location
AppSrv1	East US
AppSrv2	East US
AppSrv3	North Europe
AppSrv4	North Europe

Answer:

Explanation:

Answer Area

Minimum number of Traffic Manager profiles required: 2

Routing method for the traffic in each region: Performance

Question: 135

HOTSPOT

You are planning an Azure Front Door deployment that will contain the resources shown in the following table.

Name	Type
ASP93	App Service plan
Webapp93.azur ewebsite4.net	App Service
FD93.azurefd.net	Front Door

Users will connect to the App Service through Front Door by using a URL of https://www.fabrikarn.com. You obtain a certificate for the host name of www.fabfikam.com.

You need to configure a DNS record for www.fabrikam.com and upload the certificate to Azure. What should you do? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Upload the certificate to: A secret in Azure Key Vault

Set the DNS record target to: FD91azurefd.net

Question: 136

HOTSPOT

You have an Azure virtual network named Vnet1 that contains two subnets named Subnet1 and Subnet2. Both subnets contain virtual machines. You create a NAT gateway named NATgateway1 as shown in the following exhibit.

Home NAT gateways >

Create network address translation (NAT) gateway

O Validation passed

Basics Outbound IP Subnet Tags Review * create

Basics

Subscription	Subscription!
Resource group	RG1
Name	NATgateway 1
Region	North Europe
Availability zone idle timeout (minute	

Outbound IP

Public IP addres	None
Public IP prefit	(New) NATgateway! prefix (28)

Subnets

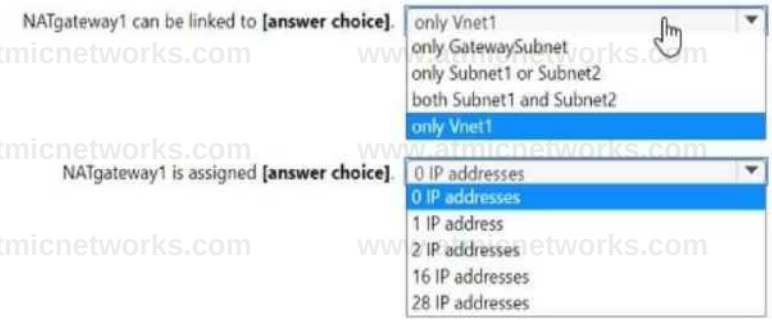
Virtual network	well
Subnets	None

Tags

None

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

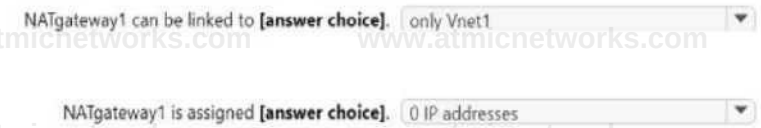
Answer Area



Answer

Explanation:

Answer Area



Question: 137

HOTSPOT

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the resources shown in the following table.

Name	Type	Description
AG1	Azure Application Gateway	Will automatially scale up to three instances
VMSS1	Virtual machine scale set	Consists of four virtual machines that run an app named App1

You need to publish App1 by using AG1 and a URL of https://app1.contoso.com. The solution must meet the following requirements:

- TLS connections must terminate on AG1.
- Minimize the number of targets in the backend pool of AG1.
- Minimize the number of deployed copies of the SSL certificate of App1.

How many locations should you import to the certificate, and how many targets should you add to the backend pool of AG1? To answer, select the appropriate options in the answer area.

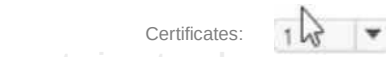
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area



Question: 138

HOTSPOT

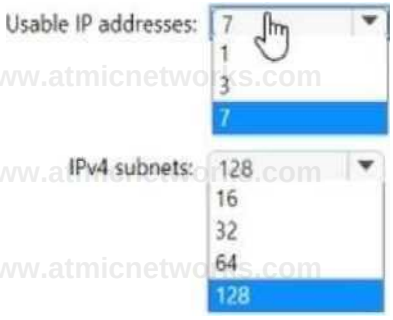
You have an Azure subscription that contains a virtual network named Vnetl. Vnetl has a /24 IPv4 address space.

You need to subdivide Vnet1. The solution must maximize the number of usable subnets.

What is the maximum number of IPv4 subnets you can create, and how many usable IP addresses will be available per subnet? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Usable IP addresses: 7

IPv4 subnets: 128

Question: 139

You have a network security group named NSG1.

You need to enable network security group (NSG) flow logs for NSG1. The solution must support retention policies.

What should you create first?

A. A standard general-purpose v2 Azure Storage account
B. An Azure Log Analytics workspace
C. A premium Block blobs Azure Storage account
D. A standard general-purpose v1 Azure Storage account

Answer: A

Explanation:

Question: 140

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNetl	Virtual network	Contains a subnet named Subnetl
storagel	Storage account	*None*
VM1	Virtual machine	Linked to Subnetl
VM2	Virtual machine	linked to Subnetl

You need to ensure that VM1 and VM2 can connect only to storage1. The solution must meet the following requirements:

- Prevent VM1 and VM2 from accessing any other storage accounts.
- Ensure that storage1 is accessible from the internet.

What should you use?

A. a network security group (NSG)
B. a private endpoint
C. a private link
D. a service endpoint policy

Answer: D

Explanation:

Question: 141

Your company has five offices. Each office has a firewall device and a local internet connection. The offices connect to a third-party SD-WAN.

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains a virtual network gateway named Gateway1. Each office connects to Gateway1 by using a Site-to-Site VPN connection.

You need to replace the third-party SD-WAN with an Azure Virtual WAN. What should you include in the solution?

A. Delete Gateway1.
B. Create new Point-to-Site (P2S) VPN connections on the firewall devices.
C. Create an Azure Traffic Manager profile.
D. Enable active-active mode on Gateway1.

Answer: B

Explanation:

Question: 142

You have an Azure subscription that contains a virtual network named Vnet1. Vnet1 contains 20 subnets and 500 virtual machines. Each subnet contains a virtual machine that runs network monitoring software.

You have a network security group (NSG) named NSG1 associated to each subnet.

When a new subnet is created in Vnet1, an automated process creates an additional network monitoring virtual machine in the subnet and links the subnet to NSG1.

You need to create an inbound security rule in NS61 that will allow connections to the network monitoring virtual machines from an IP address of 131.107.1.15. The solution must meet the following requirements:

- Ensure that only the monitoring virtual machines receive a connection from 131.107.1.15.
- Minimize changes to NSG1 when a new subnet is created.

What should you use as the destination in the inbound security rule?

A. a virtual network
B. an IP address
C. an application security group
D. a service tag

Answer: C

Explanation:

Question: 143

HOTSPOT

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Subnet	Peered with
VNetl	Subnetl 1. Subnetl?	VNetZ
VNet2	Subnet21	VNetl

The subscription contains the virtual machines shown in the following table.

Name	Connected to	Availability set
VM1	Subnetl 1	AS1
VM2	Subnetl 1	AS1
VM3	Subnet 12	*None*
[VM4	Subnet2l	*None*

You create a load balancer named LB1 that has the following configurations:

- SKU: Basic
- Type: Internal
- Subnet: Subnetl2
- Virtual network VNet1

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
LB1 can balance requests between VM1 and VW.		
LB1 can balance requests between VM2 and VMS.	Q	O
LB1 can balance requests between VMS and VM4	O	O

Answer:

Explanation:

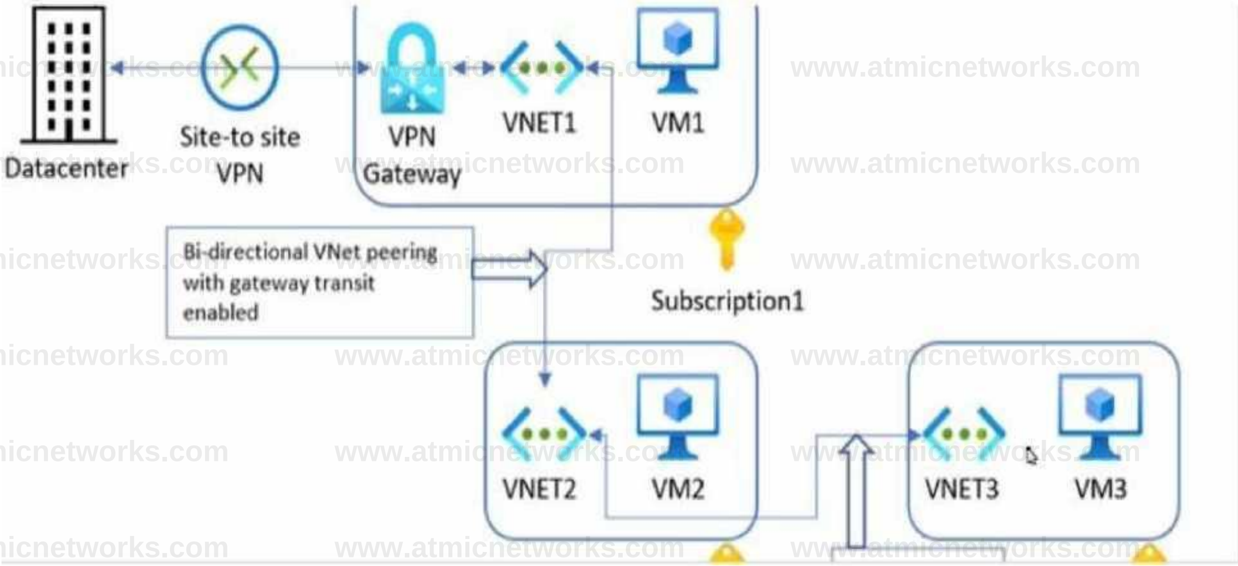
Answer Area

Statements	Yes	No
LB1 can balance requests between VM1 and VM2	#	O
LB1 can balance requests between VM2 and VW.	0	●
LB1 can balance requests between VM3 and VM4	o	

Question: 144

HOTSPOT

You have the Azure environment shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

VM1 can communicate with (answer choice)

| the on-piemises datacenter and VM2 only
VM2 only
VM2 and VM3 only
the on premises datacenter and VM2 only

(the on-premises datacenter VM1 and VMS
VM1 only
VM1 and VM 3 only
the on-premises datacenter and VM3 only
[the on-premises datacenter, VM1, and VM3

3

Answer:

Explanation:

Answer Area

VM1 can communicate with [answer choice] the on-premises datacenter and VM2 only

VM2 can communicate with [answer choice] the on-premises datacenter VM1. and VM3

Question: 145

HOTSPOT

You have the Azure resources shown in the following table.

Name	Type	Location	Description
Subi	Azure subscription	West Europe	None
Sub2	Azure subscription	West Europe	*None*
VNet!	Virtual network	West Europe	Created in Subi

VNet2	Virtual network	West Europe	Created in Sub2
Circuit 1	ExpressRoute circuit	West Europe	Linked to VNetl
Gateway 1	ExpressRoute gateway	West Europe	Created in VNetl
Gateway2	ExpressRoute gateway	West Europe	Created in VNet2

You need to link VNei2 to Circuit1

What should you create in each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Subi: [A new ExpressRoute circuit

new ExpressRoute circuit

An ExpressRoute circuit connection

An ExpressRoute circuit connection authorization

Sub2: [A new ExpressRoute circuit

i new ExpressRoute orcuit

An ExpressRoute circuit connection

An ExpressRoute circuit connection authonzation

Answer:

Explanation:

Answer Area

Subi A new ExpressRoute circuit

Subi A new ExpressRoute circuit

Question: 146

HOTSPOT

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Location
RG1	East US
RG2	UK West

You have the virtual networks shown in the following table.

Vne1l contains two virtual machines named VM1 and VM2. Vnet2 contains two virtual machines named VM3 and VM4. You have the network security groups (NSGs) shown in the following table that include only default rules.

Name	Associated to
N$q1	Sb1
Nsg2	Network interface of VM2
N$g3	Network interface of VM3
Nsg4	Sb4

You have the Azure load balancers shown in the following table.

Name	Resource group	Location	Type	Backend pool	Virtual machine	Rule
Lb1	RG1	East US	Public	Vnetl	VM1	Protocol; TCP Port 80 Backend port: 80
Lb2	RG2	West US	Internal	Vnet2	VM3	Protocol: TCP Port 1433 Backend port: 1433

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM2 can be added to the backend pool of Lb2		
VM4 can access VMS via port 1433 by using the frontend address of Lb2.		
VM1 can be accessed via port 80 from the internet by using the frontend address of Lbl		

Answer:

Explanation:

J

Answer Area

Statements	Yes	No
VM2 can be added to the backend pool of Lb2.	O	•
VM4 can access VM3 via port 1433 by using the frontend address of Lb2.		
VM1 can be accessed via port 80 from the internet by using the frontend address of Lb1.		

Question: 147

DRAG DROP

Your company, named Contoso, Ltd, has an Azure subscription that contains the resources show in the following table.

Name	Type	Location	Description
Apptus	Azure App Service	East US	A website for the United States office of Contoso
Appiuk	Azure App Service	UK West	A website for the United Kingdom office of Contoso
Stlus	Storage account	East US	Contains images for the United States website
St 1uk	Storage account	UK West	Contains images for the United Kingdom website

You plan to deploy Azure Front Door. The solution must meet the following requirement:

- Requeststo a URL of https://contoso.azurefd.net/uk must be routed to App1uk.
- Requeststo a URL of https://contoso.azurefd.net/us must be routed to App1us.
- Requeststo a URL of https://contoso.azurefd.net/images must be routed to the storage account closest to the user.

What is the minimum number of backend pools and routing rules you should create? To answer, the appropriate number to the correct component. Each number may be used once, more than once, or not at all. You may need to drag the spilt bar between panes scroll to view content: Note: Each correct selection is worth one point.

Number

2 1

I 7 I 4 I •

I 11 I *

Answer Area

Bartend pods

Routing ruin:

4

Answer:

Explanation:

Question: 148

DRAG DROP

You have an Azure subscription that contain a viral network named Vnet1 and an Azure SQL database named SQL1 has a private endpoint on Vnet1.

You have a partner company named fabrikam, has an Azure subscription that contains a virtual network named Vnet1 and a virtual machine named VM1, VM1 is connected to Vnet2

You need to provide VM1 with accesss to SQL 1 by using an Azure private Link service.

What should you implement on each virtual network? To answer, drag the appropriate resources to the correct virtual networks. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content Note: Each correct selection is worth one point.

Resources

A NAT gateway

A peering link

A private endpoint

| A service endpoint

An Azine application gateway

An Azure load balancer

Answer Area

Vnetl: f

Vnet2:

Answer:

Explanation:

Question: 149

HOTSPOT

Your on-premises network contains a VPN device.

You have an Azure subscription that contains a virtual network and a virtual network gateway.

You need to create a Site-to-Site VPN connection that has a custom cryptographic policy.

How should you complete the PowerShell script? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Question: 150

HOTSPOT

You have an on-premises datacenter.

You have an Azure subscription that contains 10 virtual machines and a virtual network named VNe1l in the East US Azure region. The virtual machines are connected to VNet1 and replicate across three availability zones. You need to connect the datacenter to VNetI1by using ExpressRoute. The solution must meet the following requirements:

- Maintain connectivity to the virtual machines if two availability zones fail.
- Support 1000-Mbps connections-

What should you include in the solution? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

One ExpressRoute Standard circuit
One ExpressRoute Premium circuit
Two ExpressRoute Standard circuits
Two ExpressRoute Premium circuits
Three ExpressRoute Standaid circuits
Three ExpressRoute Premium circuits

Minimum numbet of ExpressRoute circuits: Three ExpressRoute Standaid circuits

Minimum number of ExpressRoute gateways:

One ExpressRoute gateway of the High performance SKU Two ExpressRoute gateways of the ErGwl AZ SKU Two ExpressRoute gateways of the High performance SKU Three ExpressRoute gateways of the ErGwl AZ SKU Three ExpressRoute gateways of

One ExpressRoute gateway of the ErGwl AZ SKU

Answer:

Explanation:

Answer Area

Minimum numbet of ExpressRoute circuits: Three ExpressRoute Standard circuits

Minimum number of ExpressRoute gateways: One ExpressRoute gateway of the ErGwtAZ SKU

Question: 151

You have an Azure subscription that contains the Azure app service web apps show in the following table:

Name	Location	Description
App'eu	West Europe	Production app service for a URL o' https://Mw.fabnkcm,com
Apptus	East US	Standby app service for a URL of https://wwvj.fabrikam.com

You need to deploy Azure Traffic Manager. The solution must meet the following requirements:

- Traffic to https//www.fabrikam.com must be directed to App1eu.
- If App1eu becomes unresponsive, all the traffic to https://www.fabrikam.com must be directed to App1us. You need to implement Traffic Manager to meet the requirements.

Which two resources should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a Traffic Manager profile that uses the priority routing method
B. a Traffic Manager profile that uses the geographic routing method
C a CNAME record in a DNS domain named fabrikam.com
D. a TXT record in a DNS domain named tabrikam.com
E. a real user measurements key in Traffic Manager

Answer: A, C

Explanation:

Question: 152

HOTSPOT

You have an Azure load balancer that has the following configurations:

- Name:LB1
- Location: East US 2
- SKU: Standard
- Private IP address: 10.3.0.7
- Load balancing rule: rule! (Tcp/80)
- Health probe: probe1 (Http:80)
- NAT rules; 0 inbound

The backend pool of LB1 has the following configurations:

- Name: backend I
- Virtual network: Vnet1
- Backend pool configuration: NIC
- IP version: IPv4
- Virtual machines: VM1.VM2. VM3:

You have an Azure virtual machine named VM4 that has the following network configurations:

- Network interface: vm49Sl
- Virtual network/subnet: Vnet3/Subnet3
- NIC private IP address: 10.4.0.4
- Accelerated networking: Enabled

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Arn

Statements	fa	No
To add VM4 to LSI. you must Crete a new backend pool		
VMI n connected to VnetZ		
ionnecbons to https.710.307 w*D be toad balanced between VW. VMI and VW3		

Answer

Explanation:

Answer Area

Statements	Yes	No
To add VM4 to 181. you must create a new backend pool		
VMI is connected to VnetZ		
Connections to https: .710.3.07 will be load balanced between VMi. VMi and VM3.		

Question: 153

DRAG DROP

Your on-premises network contains an Active Directory Domain Services {AD DS) domain named contoso.com that has an internal certification authority (CA).

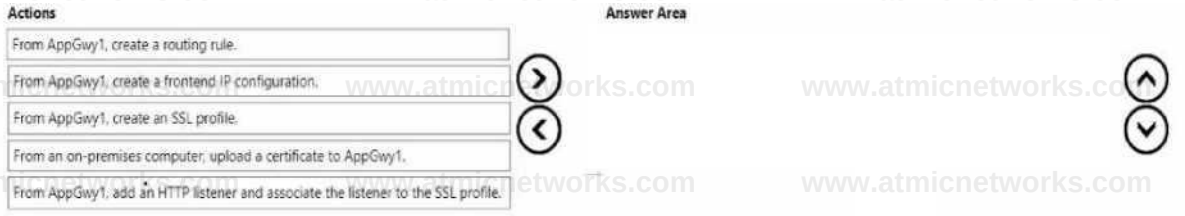
You have an Azure subscription.

You deploy an Azure application gateway named AppGwy1 and perform the following actions:

- Configure an HTTP listener.
- Associate a routing rule with the listener.

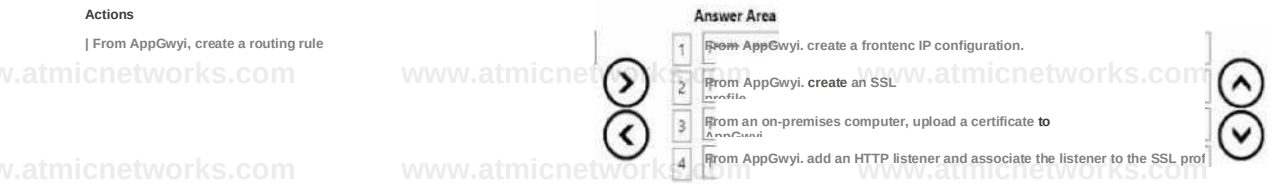
You need to configure AppGwy1 to perform mutual authentication for requests from domain-joined computers to contoso.com.

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



Answer:

Explanation:



■d

Question: 154

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNeti	Virtual network	Contains a subnet named Subnetl
Subnetl	Virtual subnet	Pan of VNetl
NSGI	Network security group MSG)	Linked to Subnetl
1 ASG-	Application security group	Not linked

Subshell contains Three virtual machines that host an app named App1. App1 is accessed by using the SFTP protocol.

From NSG1. you configure an inbound security rule named Rule2 that allows inbound SFTP connections to ASG1.

You need to ensure that the inbound SFTP connections are managed by using ASG1. The solution must minimize administrative effort.

What should you do?

A. From NSG1. modify the priority of Rule2.
B. From each virtual machine, associate the network interface to ASG1
C. From Subnet1 create a subnet delegation.
D. From ASG1, modify the role assignments.

Answer: B

Explanation:

Question: 155

You have an Azure subscription that contains a virtual network name Vnet1. Vnet1 contains a virtual machine named VM1 and an Azure firewall named FW1.

You have an Azure Firewall Policy named FP1 that is associated to FW1.

You need to ensure that RDP requests to the public IP address of FW1 route to VM1.

What should you configure on FP1?

A. an application rule
B. a network rule
C.URL filtering
D. a DNAT rule

Answer: D

Explanation:

Question: 156

HOTSPOT

Your company has 40 branch offices across North America and Europe. You have an Azure subscription that contains the following virtual networks:

- Two networks in the East US Azure region
- Three networks in the West Europe Azure region

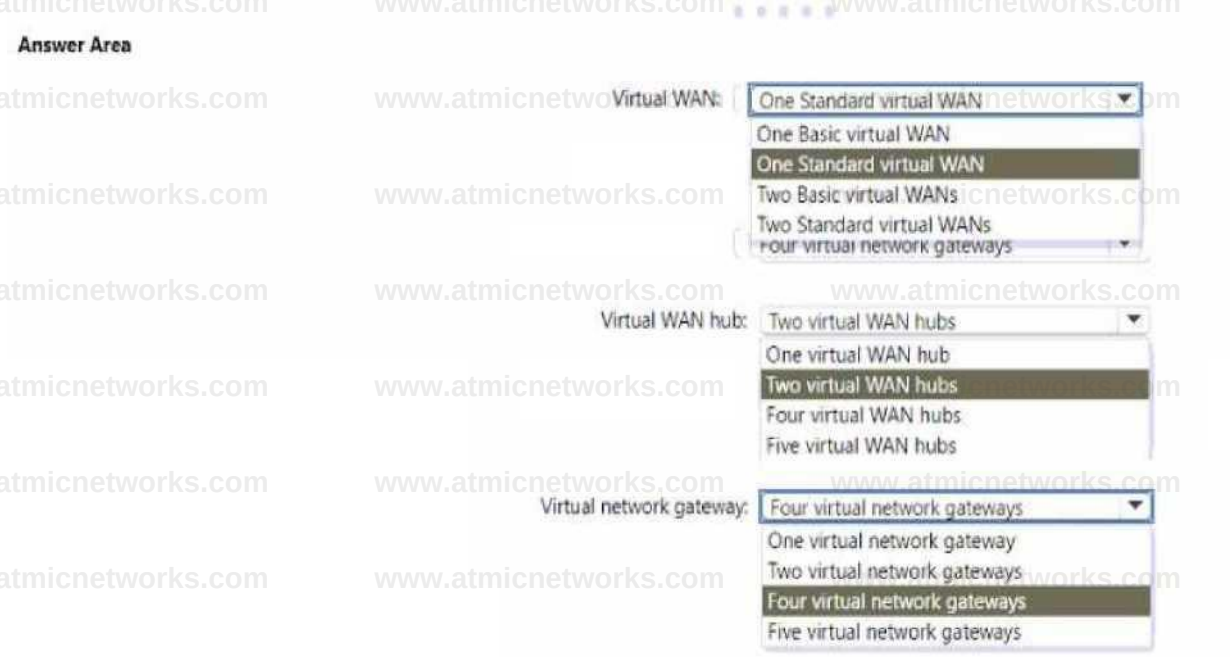
You need to implement Azure Virtual WAN. The solution must meet the following requirements:

- Each branch office in North America must have an ExpressRoute circuit and a Site-to-Site VPN that connects to the East US region.
- Each branch office in Europe must have an ExpressRoute circuit and a Site-to-Site VPN that connects to the West Europe region.
- Transitive connections must be supported between all the branch offices and all the virtual networks.
- Costs must be minimized.

What is the minimum number of Virtual WAN resources required? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Virtual WAN: One Standard virtual WAN

Virtual WAN hub: Two virtual WAN hubs

Question: 157

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
FW1	Azure Firewall Premium	Has a network intrusion detection and prevention system (IDPS) enabled
HP1	Azure Virtual Desktop host pool	All outbound traffic from HP1 to the subscription s resources route through FW1
Serveri	Virtual machine	Hosts an application named App1
KV1	Azure Key Vault	*None*

Users on HP1 connect to App1 by using a URL of https://app1 .comoso.com.

You need to ensure that the IDPS on FW1 can identify security threats in the connections from HP1 to Server1.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable TLS inspection for FW1.
B. import a server certificate to KV1.
C. Enable threat intelligence for FW1.
D. Add an application group to HP1.
E. Add a secured virtual network to FW1.

Answer: A, B

Explanation:

Question: 158

HOTSPOT

You have an Azure subscription. The subscription contains virtual machines that host websites as shown in the following table.

Name	Public host name	Location
VM1	site 1 us.contoso.com	Cast US
VM2	sitel. uk.cootoso.com	UK West
VMS	site? us.conto5o.com	East US
VM4	site? ijkxontoso.com	UK West
VMS	siteZjapan contoso.com	Japan West

You have the Azure Traffic Manager profiles shown in the following table.

Name	Routing method	DNS name	Hosted on
Tml	Performance	site Lcontoso com	VM1 and VM2
Tm2	Priority	siteZcontoso.com	VMS.VM4. and VM5

You have the endpoints shown in the following table.

Name	Traffic Manager profile	Azure end point	Routing method parameter	Status
Epi	Tml	VM1	1	Degraded
Ep2	Tml	VM2	2	Online
Ep3	'He	VMS	1	ChectangEndpoint
£p4	Tm2	VM4		Online
Ep5	Tm2	VM5	3	Online

For each of the following statements, select Yes if the statement is true. Otherwise select No.
NOTE: Each connect selection is worth one point.

Answer Are*

Statements	Yer	No
A user that requests site[1] xontoso.com from the East US Azure region will connect to site 1 us.contoso.com.		
A user that requests site2.contoso.com from the East US Azure region will connect to site2.uk.contoso.com		
A user that requests siteZcontoso.com from the japan East Azute region will connect to srte2iapan.conto5o.com		

Answer:

Explanation:

Answer Are®

Statements	Yer	No
A user that reouests 51tel.contoso.com from the East US Azure region will connect to sitel uscontoso.com.	'	•
A user that requests site2.contoso.com from the East US Azure region will connect to srte2 ulccontosoxoni	C	•
A user that requests stteZcontoso.com from the Japan East Azure region will connect to srtei iapan.conto5o.com	.	•

Question: 159

You plan to implement an Azure virtual network that will contain 10 virtual subnets. The subnets will use IPv6 addresses. Each subnet will host up to 200 load-balanced virtual machines.

You need to recommend a load balancing solution for the virtual network. The solution must meet the following requirements:

- The virtual machines and the load balancer must be accessible only from the virtual network.
- Costs must be minimized.

What should you include in the recommendation?

A. Basic Azure Load Balancer
B. Azure Application Gateway v1 Azure Application Gateway v2
C. Azure Standard Load Balancer
D. Azure Application Gateway v2

Answer: C

Explanation:

Question: 160

You have three on-premises networks.

You have an Azure subscription that contains a Basic Azure virtual WAN. The virtual WAN contains a single virtual hub and a virtual network gateway that is limited to a throughput of 1 Gbps.

The on-premises networks connect to the virtual WAN by using Site-to-Site (S2S) VPN connections.

You need to increase the throughput of the virtual WAN to 3 Gbps. The solution must minimize administrative effort.

What should you do?

A. Upgrade the virtual WAN lo the Standard SKU.
B. Add an additional VPN gateway to the Azure subscription,
C. Create an additional virtual hub.
D. Increase the number of gateway scale units.

Answer: D

Explanation:

Question: 161

Your company has four branch offices and an Azure Subscription. The subscription contains an Azure VPN gateway named GW1.

The branch offices are configured as shown in the following table.

Name	Local router	Local network gateway	Connection	VPN gateway
Branchi	RTR1	LNG1	Connection 1	GW1
Branch?	RTR2	LNG2	Connection?	GW1
BranchB	RTR3		Connection}	GW1
BrancM	RTM	LNG4	Connection	GWI

The branch office routers provide internet connectivity and Site-to-Site VPN connections to GW1. The users in Branch1 report that they can connect to internet resources, but cannot access Azure resources.

You need to ensure that the Branch1 users can connect to the Azure Resources. The solution must meet the following requirements:

- Minimize downtime for all users.
- Minimize administrative effort.

What should you do first?

A. Reset RTR1.
B. Reset Connection1.
C. Reset GW1.
D. Recreate LNG1.

Answer: B

Explanation:

Question: 162

HOTSPOT

You have an Azure subscription

You plan to use Azure Virtual WAN.

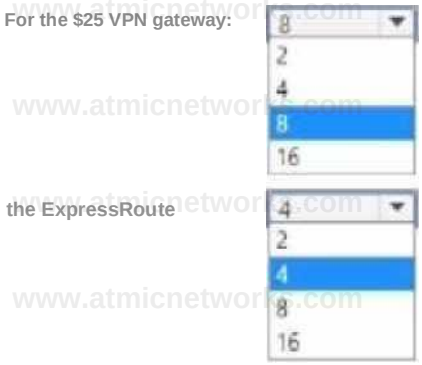
You need to deploy a virtual WAN hub that meets the following requirements:

- Supports 4 Gbps of Site-to-Site (S2S) VPN traffic
- Supports 8 Gbps of ExpressRoute traffic
- Minimizes costs

How many scale units should you configure? To answer select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Are*

For the 525 VPN gateway:

For the ExpressRoute gateway: 4

Question: 163

HOTSPOT

You have an Azure subscription that contains an app named Appl. App1 is deployed to the Azure App Service apps show in the following table.

Name	Location	Worker instances
Appt-East	Last US 1	4
Appi-West	West US 1	4

You need to publish App1 by using Azure Front Door. The solution must ensure that all the requests to App1 are load balanced between all the available worker instances.

What is the minimum number of origin groups and origins that you should configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Origin groups 1 (1, 2, 4, 8)

Orpins 4 (1, 2, 4, 8)

Answer:

Explanation:

Answer Area

nr

Origin groups

Origins 4

Question: 164

HOTSPOT

You have an on-premises network.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
Vnetl	Virtual network	*None*
VM1	Virtual machine	Connected to Vnetl
VM2	Virtual machine	Connected to Vnetl
SQL1	Azure SQL Database	internet accessible

You need to implement an ExpressRoute circuit to access the resources in the subscription. The solution must ensure that the on-premises network connects to the Azure resources by using the ExpressRoute circuit.
Which type of peering should you use for each connection? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Connection to Vnetl: Private peering / Microsoft peering

Connection to SQL1: Microsoft peering

Private peering
Public peering
Virtual network peering

Microsoft peering
Private peering
Public peering
Virtual network peering

Answer:

Explanation:

Answer Area

Connection to Vnetl: Private peering »

Connection to SQL1: [Microsoft peering

Question: 165

You have the Azure virtual networks shown in the following table.

Name	Resource group	Location
Vnetl	RG1	East US
Vnet2	RG1	UK West
Vnet3	RG1	East US
Vnet4	RG1	UK West

You have the Azure resources shown in the following table.

Name	Type	Virtual network	Resource group	Location
VM1	Virtual machine	Vnetl	RG1	East US
VM2	Virtual machine	Vnet2	RG2	UK West

VM3	Virtual machine	Vnet3	RG3	East US
App1	App Service	Vnetl	RG4	East US
stl	Storage account		RG5	UK West

You need to check latency between the resources by using connection monitors in Azure Network Watcher.
What is the minimum number of connection monitors that you must create?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C

Explanation:

Question: 166

You have an Azure virtual machine named VM1.
You need to capture all the network traffic of VM1 by using Azure Network Watcher.
To which locations can the capture be written?

A. a file path on VM1 only
B. blob storage only
C. a premium storage account only
D. blob storage and a file path on VM1 only
E. blob storage and a premium storage account only
F. blob storage, a file path on VM1, and a premium storage account

Answer: D

Explanation:

Question: 167

HOTSPOT
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
appservicel	Azure App Service	Hosts an app named App1
contoso.com	Azure DNS zone	Resolves name requests from the internet
FD1	Azure Front Door	Standard profile with Appl configured as the origin
KeyVaultl	Azure Key Vault	Key vault with Permission model set to Vault access policy
KeyVault2	Azure Key Vault	Key vault with Permission model set to Azure role-based access control

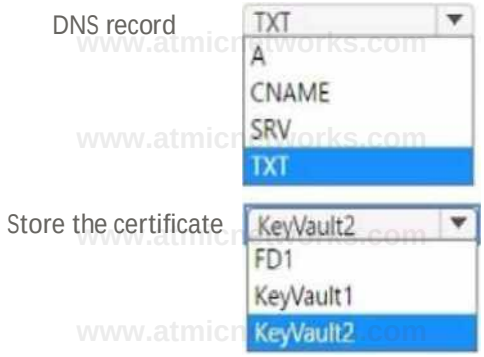
You purchase a certificate for app1.contoso.com from a public certification authority (CA) and install the certificate on appservice1.

You need to ensure that App1 can be accessed by using a URL of https://app1.contoso.com. The solution must ensure that all the traffic for App1 is routed via FD1.

Which type of DNS record should you create, and where should you store the certificate? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Area



Answer:

Explanation:

Answer Area

DNS record type: [TXT

Store the certificate in: KeyVault2

Question: 168

You have an Azure application gateway configured for a single website that is available at https://www.contoso.com.

The application gateway contains one backend pool and one rule. The backend pool contains two backend servers. Each backend server has an additional website that is available on port 8080.

You need to ensure that if port 8080 is unavailable on a backend server, all the traffic for https://www.contoso.com is redirected to the other backend server.

What should you do?

A. Create a health probe.
B. Add a new rule.
C. Add a new listener.
D. Change the port on the listener.

Answer: A

Explanation:

Question: 169

HOTSPOT

You have an Azure subscription that contains an Azure key vault named Vaultl and an app registration for an Azure AD app named App1.

You have a DNS domain named contoso.com that is hosted by a third-party DNS provider.

You plan to deploy App1 by using Azure App Service. App1 will have the following configurations:

- App1 will be hosted across five App Service apps.
- Users will access App1 by using a URL of https://app1.contoso.com.
- The user traffic of App1 will be managed by using Azure Front Door.
- The traffic between Front Door and the App Service apps will be sent by using HTTP.
- App1 will be secured by using an SSL certificate from a third-party certificate authority (CA).

You need to support the Front Door deployment.

Which two DNS records should you create, and to where should you import the SSL certificate for App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

DNS records: A CNAME record and a TXT record

An A record and a SRV record
An A record and a CNAME record
A TXT record and a SRV record

Import the certificate to:

The app registration for Appl
The App Service apps

Answer

Explanation:

Answer Area

DNS records: A CNAME record and a TXT record

Import the certificate to:

Question: 170

You have an internal Basic Azure Load Balancer named LB1 That has two frontend IP addresses. The backend pool of LB1 contains two Azure virtual machines named VM1 and VM2.

You need to configure the rules on LB1 as shown in the following table.

Rule	Frontend IP address	Protocol	ILB1 port	Destination	VM port
1	65.52.0.1	TCP	80	IP address of the NIC of VM1 and VM2	80
2	65.52.02	TCP	80	IP address of the NIC of VM1 and VM2	80

What should you do for each rule?

A. Enable Floating IP.
B. Disable Floating IP.
C. Set Session persistence to Enabled.
D. Set Session persistence to Disabled

Answer: A

Explanation:

Question: 171

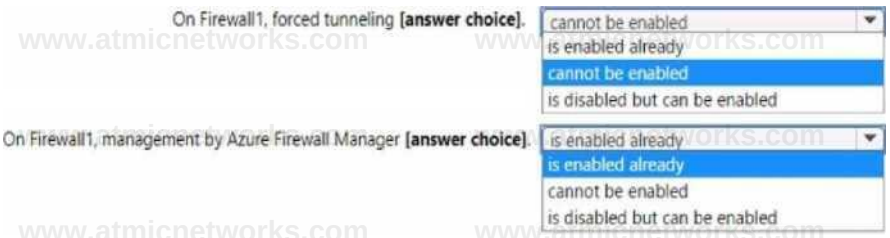
HOTSPOT

You have the Azure firewall shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

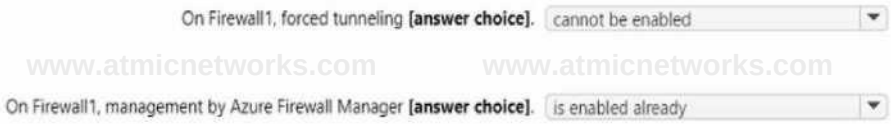
Answer Area



Answer:

Explanation:

Answer Area



Question: 172

DRAG DROP

You have an Azure subscription that contains an Azure Firewall Premium policy named FWP1.

To FWP1, you plan to add the rule collections shown in the following table.

Which priority should you assign to each rule collection? To answer, drag the appropriate priority values to the correct rule collections- Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Priorities

100

200

300

Answer Area

RC1: [ ]

RC2: [ ]

RC3: [ ]

Answer:

Explanation:

Question: 173

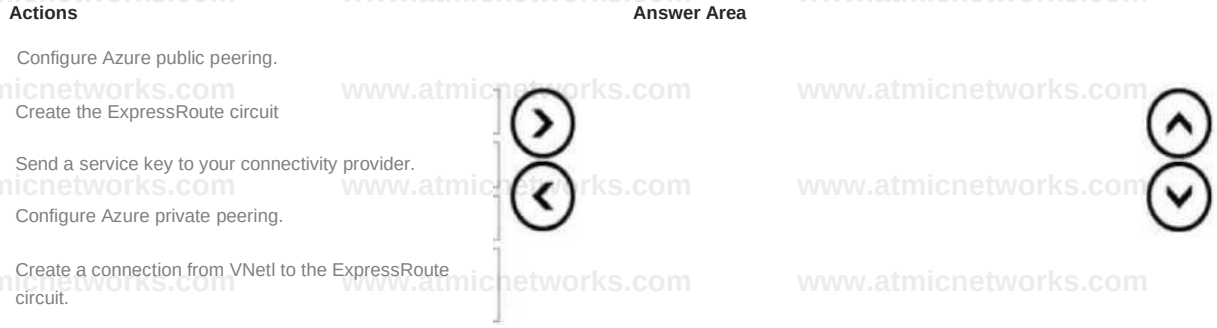
DRAG DROP

You have an on-premises network.

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains an ExpressRoute gateway.

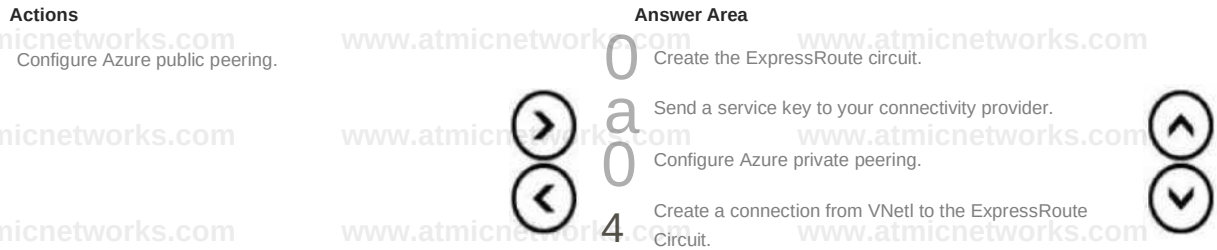
You need to connect VNet1 to the on-premises network by using an ExpressRoute circuit.

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



Answer:

Explanation:



Question: 174

DRAG DROP

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
Gateway 1	NAT gateway	Unconfigured
NIC1	Network interface	A network interface with a statically assigned public IP address named PIP1
PIP1	Public IP address	A Basic SKU public IP address
VNetl	Virtual network	Contains a subnet named Subnetl
Subnet 1	Virtual subnet	Part of VNetl
VM1	Virtual machine	Connected to Subnetl via N'C1

You need to associate Gateway 1 with Subnet1. The solution must minimize downtime on VM1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Change the PIP1 SKU to **Standard**

Start VM1.

Shut down VM1

Disassociate PIP1 from NICi.

Change Assignment to Dynamic for PIP1.

Associate PIP1 to NIC1.

Answer Area

Answer:

Explanation:

Actions

Change the PIP1 SKU to **Standard**.

Start VM1.

Shut down VM1.

Answer Area

1 Disassociate PIP1 from NIC1.

2 Change Assignment to Dynamic for PiP1.

3 \ Associate PIP1 to NIC1.

Question: 175

HOTSPOT

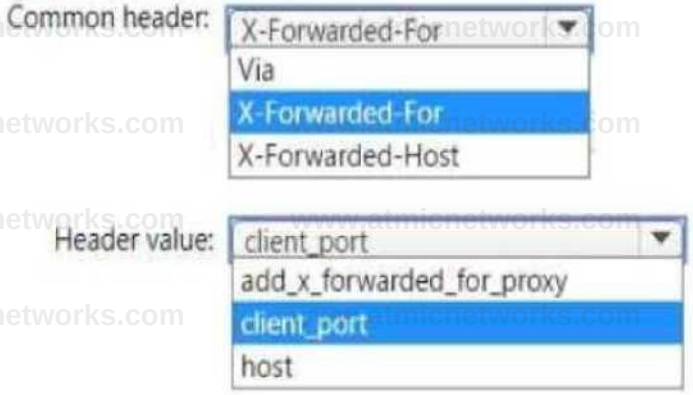
You have an Azure application gateway.

You need to create a rewrite rule that will remove the origin port from the HTTP header of incoming requests that are being forwarded to the backend pool.

How should you configure each setting? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Common header X-Forwarded-For

Header value: client.port

Question: 176

HOTSPOT

Your on-premises network contains the subnets shown in the following table.

Name	IPv4 network address
Subnet 1	192.168.10.0/24
Subnet2	192.168.20.0/24

The network contains a firewall named FW1 that uses a public IP address of 131.107.100.200.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNetl	Virtual network	Uses an address space of 10.1.0.0/16
GW1	Virtual network gateway	• Uses a public IP address of 20.231231.174 • Uses a pnvate IP address of 10.1.255.10
GatewaySubnet	Subnet	Uses an address space of 10.1.255.0/27
LNG1	Local network gateway	*None*

You plan to configure a Site-to-Site (S2S) VPN named VPN1 that will connect GW1 to FW1.

You need to configure LNG1 to support VPN1. The solution must meet the following requirements:

- Ensure that the resources on Subnet1 and Subnet2 can communicate with the resources on VNe1l.
- Minimize administrative effort.

How should you configure LNG1? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Address space: 10.1255.0/27

IPaddress: 202 31231.174

Question: 177

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 an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAF1.

You need to configure a rate limit for incoming requests to AFD1.

Solution: You configure a managed rule for WAF1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 178

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 an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAF1.

You need to configure a rate limit for incoming requests to AFD1.

Solution: You modify the policy settings of WAF1.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Question: 179

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 an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAFT.

You need to configure a rate limit for incoming requests to AFD1.

Solution: You configure a custom rule for WAF1.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 180

HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

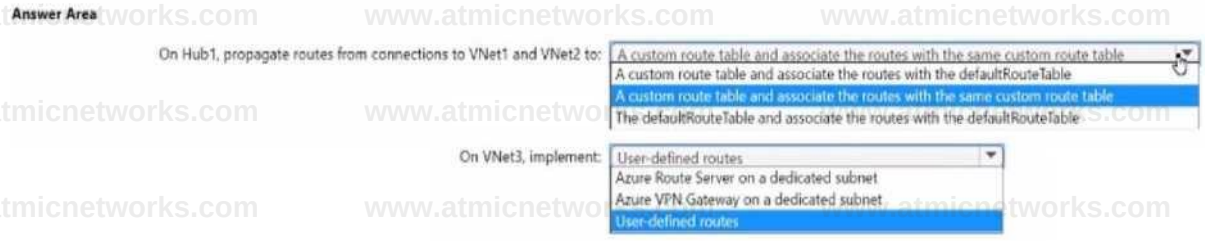
Name	Type	Description
VWAN1	Azure Virtual WAN	Standard Virtual WAN
Hubl	Azure Virtual WAN hub	Hub for VWAN1
VNetl	Virtual network	Connected to Hubl
VNet2	Virtual network	Connected to Hubl
VNet3	Virtual network	Peered with VNet2
NVA1	Virtual machine	Hosts a routing appliance deployed to VNetZ

You establish BGP peering between NVA1 and Hub1.

You need to implement transit connectivity between VNet1 and VNet3 via Hub1 by using BGP peering. The solution must minimize costs.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Question: 181

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a subnet named Subnet1

You deploy an instance of Azure Application Gateway v2 named AppGw1 to Subnet1. You create a network security group (NSG) named NSG1 and link NSG1 to Subnet1.

You need to ensure that AppGw1 will only load balance traffic that originates from VNet1. The solution must minimize the impact on the functionality of AppGw1.

What should you add to NSG1?

A. an outbound rule that has a priority 100 and blocks all internet traffic

B. an outbound rule that has a priority of 4096 and blocks all internet traffic
C. an inbound rule that has a priority of 4096 and blocks all internet traffic
D. an inbound rule that has a priority of 100 and blocks all internet traffic

Answer: C

Explanation:

Question: 182

HOTSPOT
You have an Azure subscription that contains an Azure Firewall policy named FWPolicy1. You need to configure FWPolicy1 to meet the following requirements

- Allow traffic based on the FQDN of the destination.
- Allow TCP traffic based on the source.

Which types of rules should you use for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer

Explanation:

Answer Area

Alien* traffic ba^d on the FQDN of th® destination: Application only

Allow TCP traffic based on the source: Network only

Question: 183

HOTSPOT
You have art Azure subscription that contains the resources shown in the following table.

Name	Type	Location	Description
VNetI	Virtual network	East US	Contains a subnet named SubnetI

storage!	Storage account	East US	Uses read-access geo-redundant storage (RA-GRS) redundancy
sqll	Azure SQL server	East US	Hosts a database named SQLDB1

You need to restrict access to storage1 and sql1 by using service endpoints. The solution must meet the following requirements:

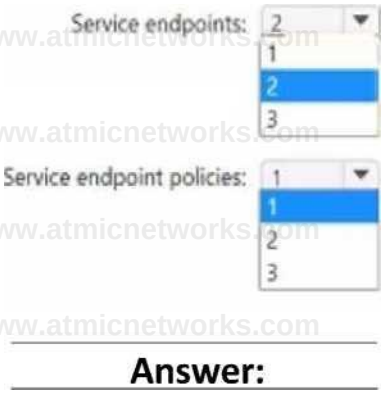
- Allow access from Subnet1 to SQIDB1
- Implement service endpoint policies to restrict access to supported resources.
- Allow access from Subnet1 to storage1 and the read-only replica of storage1 in the paired Azure region.

What is the minimum number of service endpoints and service endpoint policies you should create?

To answer, select the appropriate options m the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Explanation:

Answer Area

Service endpornts: 2

Service endpoint policies: 1

Question: 184

DRAG DROP

You have art Azure subscription.

You plan to deploy Azure Front Door with Azure Web Application Firewall (WAF).

You plan to implement custom rules and managed rules that meet the following requirements:

- Block malicious bots.
- Throttle client IP addresses that exceed 100 connections per minute.

You need to identify which Front Door SKU to configure, and which type of rule to configure for each

requirement. The solution must minimize administrative effort and costs.

What should identify? To answer, drag the appropriate options to the correct targets. Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Options

A custom rule

A managed rule

Classic

Premium

Standard

Answer Area

^^g. i

Block malicious bots:

Throttle client IP addresses

Answer:

Explanation:

Options

A custom rule

A managed rule

Classic

Standard

Answer Area

sm Pre-mmm

Block malicious bots: A managed rule

Throttle client IP addresses A custom rule Premium

Question: 185

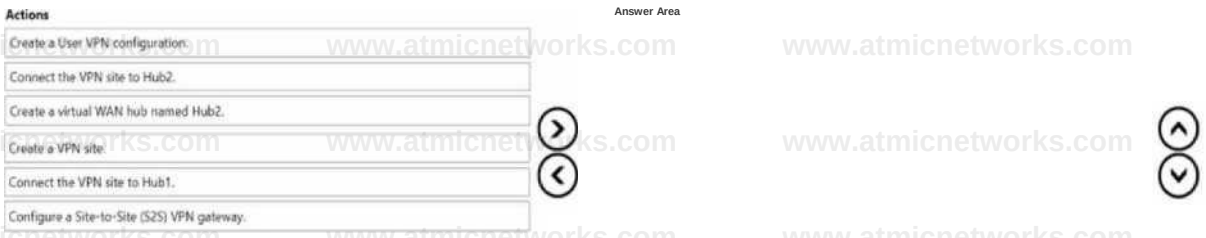
DRAG DROP

You have an on-premises network.

You have an Azure subscription that contains a virtual network named VNet1. VNet1 is connected to an Azure Virtual WAN hub named Hub1.

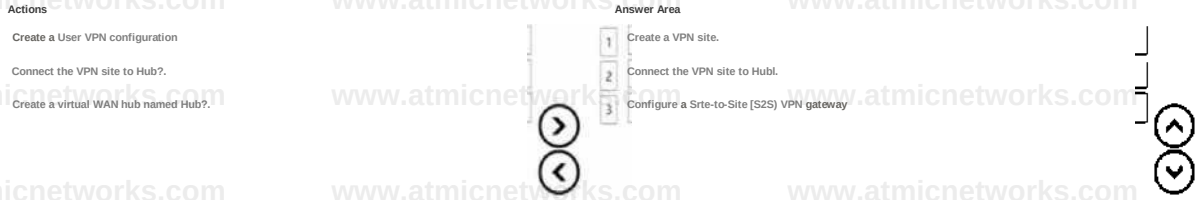
You need to enable connectivity between the on-premises network and VNet1 by using Hub1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Explanation:



Question: 186

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 an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1. Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement an Azure Front Door profile.

Does this meet the requirement?

A. Yes

B. No

Answer: B

Explanation:

Question: 187

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 on Azure subscription that contains on Azure Virtual WAN named VWAN1.VWAN1 contains a hub named Hub1.

Hub! has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure Firewall.

Does this meet the requirement?

A. Yes

B. No

Answer: B

Explanation:

Question: 188

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 on Azure subscription that contains an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub! has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure NAT Gateway.

Does this meet the requirement?

A. Yes

B. No

Answer: B

Explanation:

Question: 189

You have an Azure subscription that contains an Azure Front Door named FD1. FD1 is configured as shown in the following exhibit.

^ Purge-cache Q Origin response timeout M Deete Refresh

A Essentials /SON View

Resource group /move)	! RGb
Status	: Active
Location	: Global
Subscription [move}	• Ayute P3$s • Spon^rsNp
Subscription ID	; 9651bd2a 3E94-4fd9-?dbf 915f7d&61aJe
Name	: HM
Pricing Tret	; Azure Front Doot Standard
Front Door ID	; a4019e23-cd4e-4440-8792-4f«bc3a4<070
Origin response timeout	; W Seconds
Tags (edit!	: a£kt2£Sd£ui£ld-I$9;

Properties Monitoring Recommendations

3 Endpoints

Endpoint hostname	Endpoint 1-N;gyhnhbdthqc2es zOl aaurefd.net O Provision succeeded O Enabled

S Custom aomams

^ Security policy

3 Rout

Route name	default
(Enapomtt-fwi	gynnhMm«2esz0l.aiurefd.n«)₀ p^,^ succeeded O Enabled

^ Origin groups

Ongm group name	default origin group O Provision succeeded

You need to enable Azure Private Link for FD1.

What should you do first?

A. Create an origin group.
B. Add an endpoint.

C. Change Pricing Tier to Azure Front Door Premium.
D. Create a custom route.

Answer: C

Explanation:

Question: 190

DRAG DROP

Your on-premises network contains two subnets named Subnet1 and Subnet2. Subnet2 contains a Hyper-V host that contains two virtual machines named VM1 and VM2. VM1 and VM2 are connected to Subnet2.
You have an Azure virtual network named VNet1 that contains GatewaySubnet and a subnet named VSubnet1. VNet1 is connected to the on-premises network by using a Site-to-Site (S2S) VPN connection.
You plan to migrate VM1 to VNet1 and maintain the existing IP address of VM1. VM2 will remain on Subnet2.
You need to prepare the environment to ensure that VM1 can communicate with VM2 once the migration is complete.
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.'

Actions

Extend the IP address space of VNetl to include the IP address range of Subnetl.

To VNetl add a subnet named VSubnet? that uses the same address range as Subnetl.

Extend the P address space of VNetl to include the IP address range of SubnetZ

To VNetl add a subnet named VSubnet2 that uses the same address range as Subnet2

Deploy an Azure virtual machine that runs Windows Server Azure Edition and has two NICs connected to VSubnetl and VSubnetZ

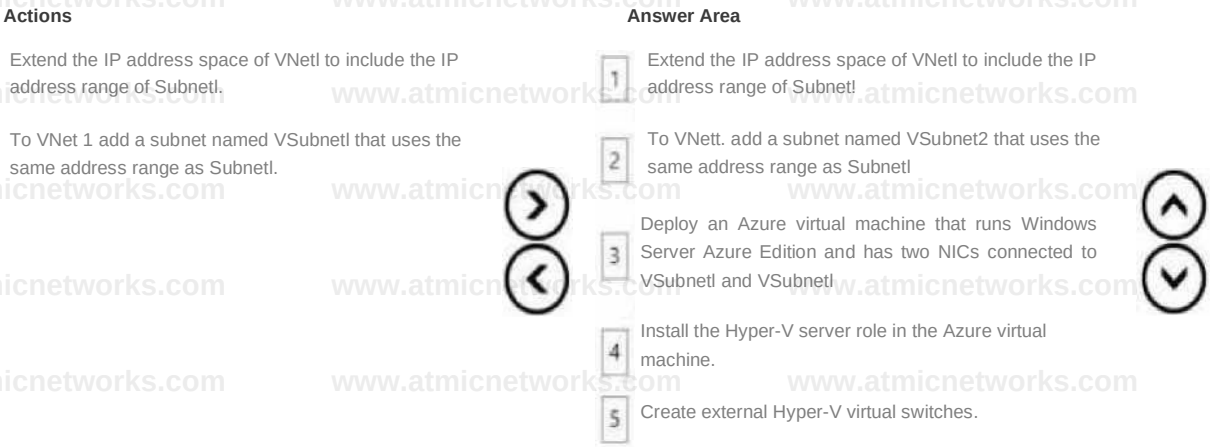
Install the Hyper-V server role in the Azure virtual machine.

Create external Hyper-V virtual switches

Answer Area

Answer:

Explanation:



Question: 191

DRAG DROP

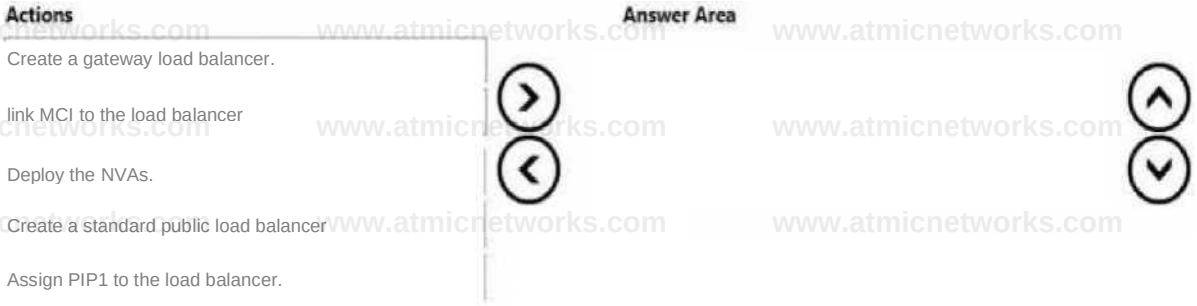
You have an Azure subscription that contains a virtual machine named VM1. VM1 contains a NIC named NIC1 and a public IP address named PIP1.PIP1 is assigned to NIC1.

You plan to deploy four Network Virtual Appliances (NVAs).

You need to ensure that all the inbound traffic from the internet to PIP1 is inspected by the NVAs.

The solution must ensure that the NVA deployment is highly available.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Explanation:

Question: 192

HOTSPOT

You have an Azure subscription that contains a dual-stack virtual network named VNet1. VNet1 has the following IP address spaces:

- IPv4:192.168.0.0/24
- IPv6: fd0adbftdeca: deed: y48

You plan to deploy an Azure VPN gateway and multiple virtual machines to VNet1.

You need to configure the subnet masks for VNet1. The solution must meet the following requirements:

- Maximize the number of usable IP addresses.
- Support the deployment of the VPN gateway and the virtual machines.

Which subnet mask should you use for each address space? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

IPv4: /26 *

IPv6: /64 *

Question: 193

HOTSPOT

You have an on-premises network.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
Subnetl	On-premises subnet	Assigned an IP address of 10.11.0/24
Subnet?	On-premises subnet	Assigned an IP address of 10 1.2.0/24
SubneB	Azure virtual subnet	Assigned an IP address of 10.1.3.0/24
Subnet4	Azure virtual subnet	Assigned an IP address of 10.11.0/24
VNetl	Azure virtual network	Contains Subnets and Subnet4
Serveri	Windows Server 2022	On-premises server that is connected to Subnetl and Subnet?
VM2	Windows Server 2022	Azure virtual machine that is connected to Subnets and Subne'4
S2SVPN1	Site-to-Site IS2S) VPN	Connects the on-premises network to VNetl

You need to ensure that on-premises devices can communicate with Azure resources that are connected to Subnet4.

What should you do on each resource? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Server!: Configure an Azure Network Adapter,

- M2. Deploy the Routing and Remote Access service.

Question: 194

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 an Azure Virtual WAN named VWAN1. VWAN1 contains a hub named Hub1.

Hub1 has a security status of Unsecured.

You need to ensure that the security status of Hub1 is marked as Secured.

Solution: You implement Azure Web Application Firewall (WAF).

Does this meet the requirement?

A. Yes
B. No

Answer: B

Explanation:

Question: 195

HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNetl	Virtual network	In the West Europe Azure region
VNet2	Virtual network	In the East US Azure region
VMI	Virtual machine	On VNett
VM2	Virtual machine	On VNetl
[VM3	Virtual machine	On VNetz
| VM4	Virtual machine	On VNetZ

You plan to deploy an app named App1 to meet the following requirements.

- External users must be able to access App1 from the internet.
- App1 will be load balanced across all the virtual machines.
- App1 will be hosted on VM1, VM2. VM3. and VM4.
- App1 must be available if an Azure region fails.
- Costs must be minimized.

You need to implement a global load balancer solution for App.

What should you configure? To answer, select the appropriate options in the answer area NOTE: Bach correct answer is worth one point.

Answer Area

0"t con region OJO balancer and two rtawl load baarreers only
One cross region load balancer only
One cross region load balancer and one regional load balancer only
One cross region load balancer and two regional load balancers only
| Two cross-region load balancers and two regional load balancers only

load balancer SKU I Standard * I
1Basic
| Gateway
Standard

Answer:

Explanation:

Answer Area

Number and type of load balancers One cross region load balancer and two regional load balancers only

load balancer SKU Standard

Question: 196

You have an Azure Private Link service named PL1 that uses an Azure load balancer named LB1. You need to ensure that PL1 can support a higher volume of outbound traffic. What should you do?

A. Redeploy LB1 with a different SKU.
B. Increase the number of NAT IP addresses assigned to PL1.
C. Deploy an Azure Application Gateway v2 instance to the source NAT subnet.
D. Increase the number of frontend IP configurations for LB1.

Answer: B

Explanation:

Question: 197

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the following subnets.

- AzureFirewallSubnet
- GatewaySubnet
- Subnet 1
- Subnet2
- Subnet3

Subnet2 has a delegation to the Microsoft.Web/serverfarms service. The subscription contains the resources shown in the following table.

Name	typ*	Connected to
AZVNGW1	Azure VPN Gateway	GatewaySubnet
AZFWI	Azure Firewall Premium	AzureF irewallSubnet
I VMSS1	Virtual machine Kale Kt	Subnet 1

You need to implement an Azure application gateway named AG1 that will be integrated with an Azure Web Application Firewall (WAF). AG1 will be used to publish VMSS1.
To which subnet should you connect AG1?

A. Subrwt2
B. Subnet 1
C. Subnet3
D. AzureFjrewall Subnet
E. GatewaySubnet

Answer: C

Explanation:

Question: 198

DRAG DROP
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure App Service app	Accessed by using a URL of https//appl.contoso.com/
FD1	Azure Front Door Premium profile	Configured as an endpoint for App 1
conto5o.com	Azure DNS zone	Contains a DNS CNAME record for App1 that resolves to an FQDN of app 1 .azurewebsites net

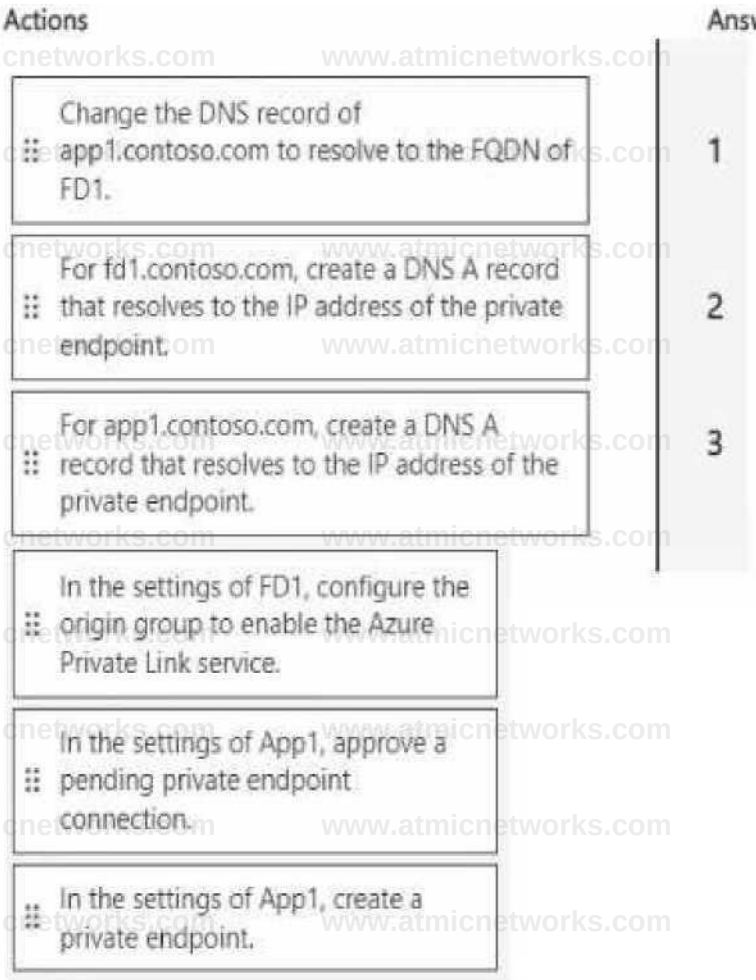
You discover that users connect directly to App1.
You need to meet The following requirements:

- Administrators must only access App1 by using a private endpoint.

- All user connections to App1 must be routed through FD1.
- The downtime of connections to App1 must be minimized.

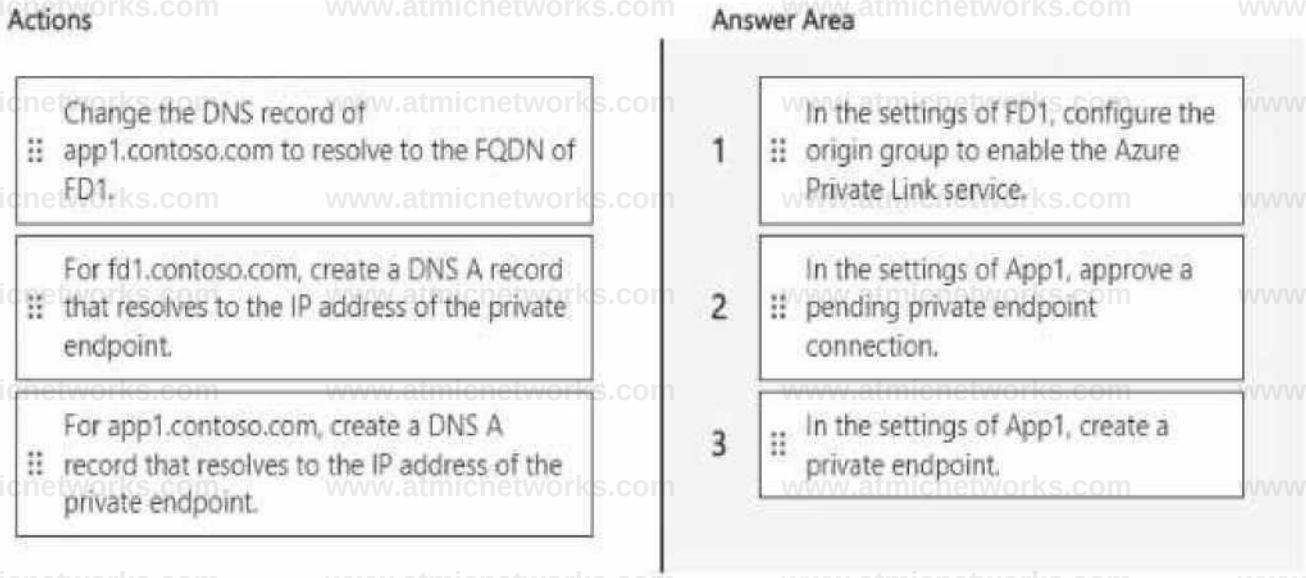
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



Answer:

Explanation:



Question: 199

You have an instance of Azure Web Application Firewall (WAF) on Azure Front Door.
You plan to create a WAF rule that will block high rates of requests from a single IP address.
You need to query Log Analytics to identify the optimal threshold for the rule.
Which table should you query in Log Analytics?

A. AZFWThreatInte1 B. AzureDiagnostics C. SecurityDetection D. AGWFirewallLogs

Answer: B

Explanation:

Question: 200

You have the Azure subscriptions shown in the following table.

Name	Microsoft Entra ID tenant	Contains resources in Azure region	Virtual network
Sub1	contoso.com	East US, West US	VNetl, VNet2
Sub2	contoso.com	Europe North, Europe West	VNet3, VNet4
Sub3	fabrikam.com	Europe North, West US	VNet5, VNetG

Each virtual network contains 20 internet-accessible resources that are assigned public IP addresses. You need to implement Azure DDoS Network Protection to protect the resources. The solution must minimize costs.
What is the minimum number of DDoS Network Protection plans you should deploy?

A. 1
B. 2
C. 3
D. 6

Answer: B

Explanation:

Question: 201

HOTSPOT

You plan to implement an Azure Virtual WAN named VWAN1 that will contain a hub named Hub1.

VWAN1 will include the virtual networks shown in the following table.

Name	IP address space	Description
VNetl	10.1.0.0/24	Connected directly to Hubl by using a connection named Connl
VNet2	10.2.0.0/24	Connected directly to Hubl by using a connection named Conn2 and hosting a Network Virtual Appliance (NVA) named NVA2 that has an IP address of 10.2.0.5
VNet3	10.2.3.0/24	Connected to VNet2 by using a virtual network peering named Peering 1

You need to ensure that hosts connected to VNet1 can communicate with hosts connected to VNet3. How should you configure the routing tables for VWAN1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Default route table: From destination 10.2.0.0/16 to next hop Conn2 _____

- **From destination 10.2.0,0/16 to next hop Conn?**
- From destination 10.2.3.0/24 to next hop 10.2.0.5
- From destination eastusconn to next hop 10.2.0.0/16

Route table for Connl: From destination 10.2.0.0/16 to next hop Conn?

- **From destination 102.0.0/16 to next hop Conn?**
- From destination 10,2.3.0/24 to next hop 10.2.0.5
- From destination eastusconn to next hop 10.2.0.0/16

Answer:

Explanation:

Answer Area

Default route table: From destination 102.0.0/16 to next hop Conn2

Route table for Connl: From destination 102.0.0/16 to next hop Conn2

Question: 202

HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNetl	Virtual network	Has an IP address space of 192.168.0.0/23
VNet2	Virtual network	Has an IP address space of 192.1682.0/23
VNet3	Virtual network	Has an IP address space of 10.0.0.0/20
Peering12	Virtual network peering	Peered between VNet! and VNet2
PeeringJI	Virtual network peering	Peered between VNet2 ana VNetl

Each virtual network contains 20 virtual machines and a subnet that has an IP address space of /24. You need to ensure that you can access the virtual machines from the internet by using Azure Bastion.

What is the minimum number of bastion subnets you should deploy, and what is the smallest supported IP address space for each bastion subnet? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Bastion subnets: 3 ▼

2

IP address space: /26 ▼

Z24 /25

Answer:

Explanation:

Answer Area

Bastion subnets: 3

IP address space' /26

Question: 203

HOTSPOT

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location	Description
SQLMI1	Azure SQL Managed Instance	US East	Managed instance connected to VNetl
contosoxom	Microsoft Entra Domain Services	US East	Domain connected to VNet2
VNetl	Virtual network	US East	*None*
VNet2	Virtual network	US East	*None*
storagel	Storage account	US East	*None*

You need to ensure that network traffic is routed over the Azure backbone network for the following scenarios:

- Traffic from SQIMI1 to storage1
- Traffic from domain joined servers on VNet2 to storage1

The solution must minimize costs.

What should you configure for each scenario? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Traffic from SQLMI1 to storagel: A private endpoint | A Managed Instance link

A private endpoint

| A service endpoint policy

Traffic from domain joined servers on VNet2 to storagel: A service endpoint policy | A private endpoint

A service endpoint policy

| Microsoft Entra Private Access

Answer:

Explanation:

Answer Area

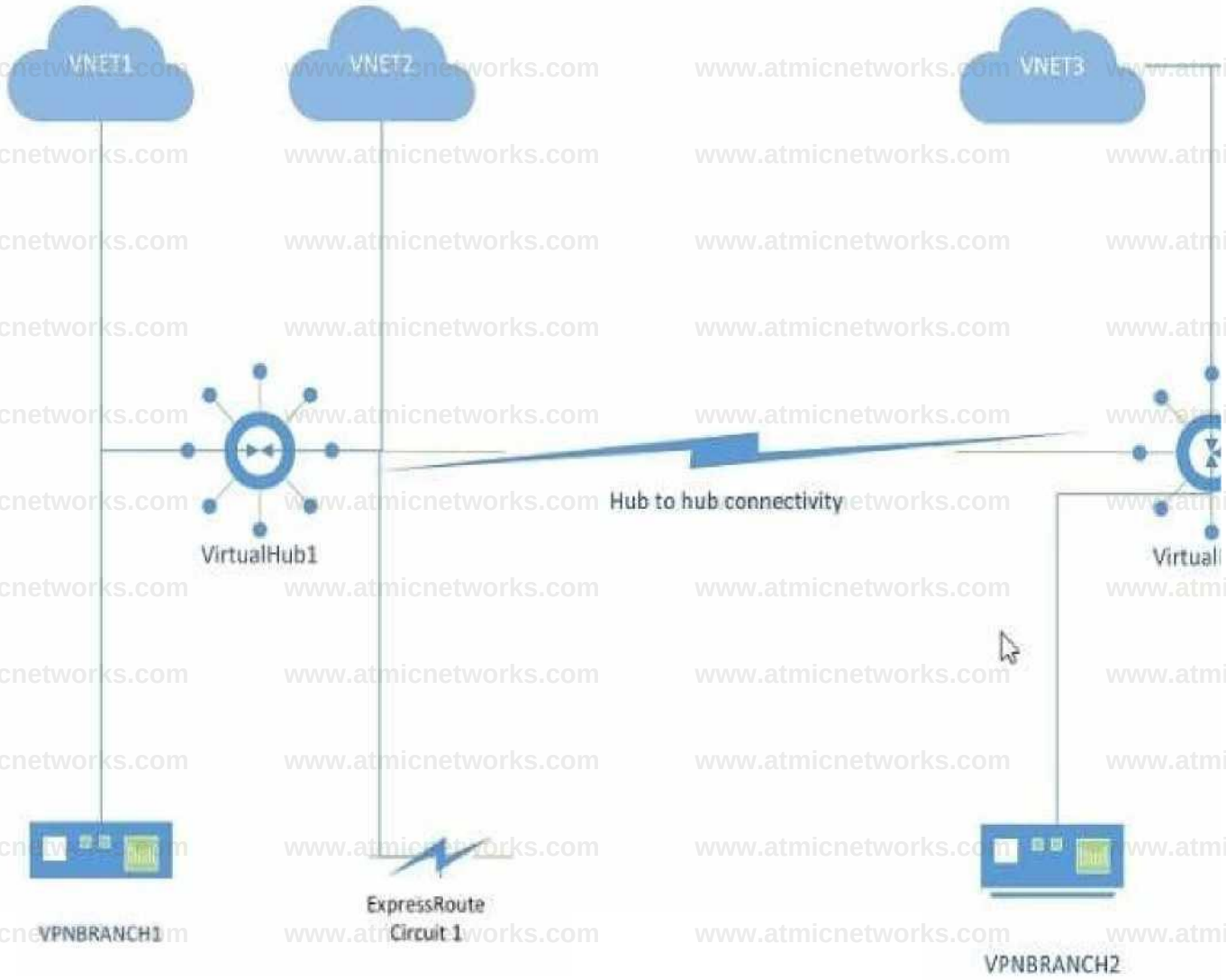
Traffic from SQLMI1 to storage!: A private endpoint

Traffic from domain joined servers on Wet2 to storage!: A service endpoint policy

Question: 204

You have an Azure subscription.

You plan to implement Azure Virtual WAN as shown in the following exhibit.



What is the minimum number of route tables that you should create?

A. 1
B. 2
C. 4
D. 6

Answer: B

Explanation:

Question: 205

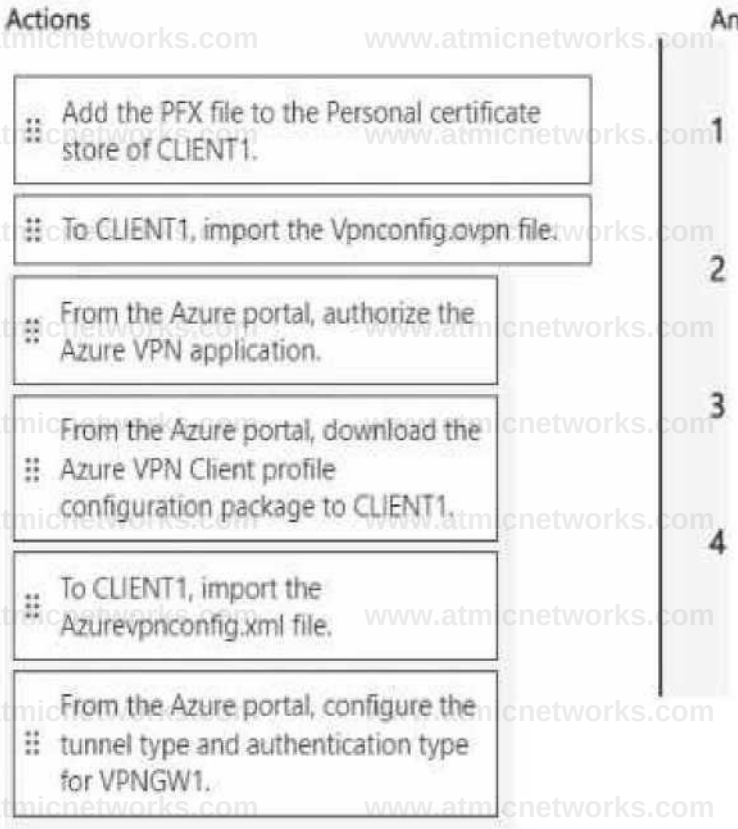
DRAG DROP

You have a computer named CLIENT! that runs Windows 11 and has the Azure VPN Client installed.

You have an Azure virtual network gateway named VPNGW1.

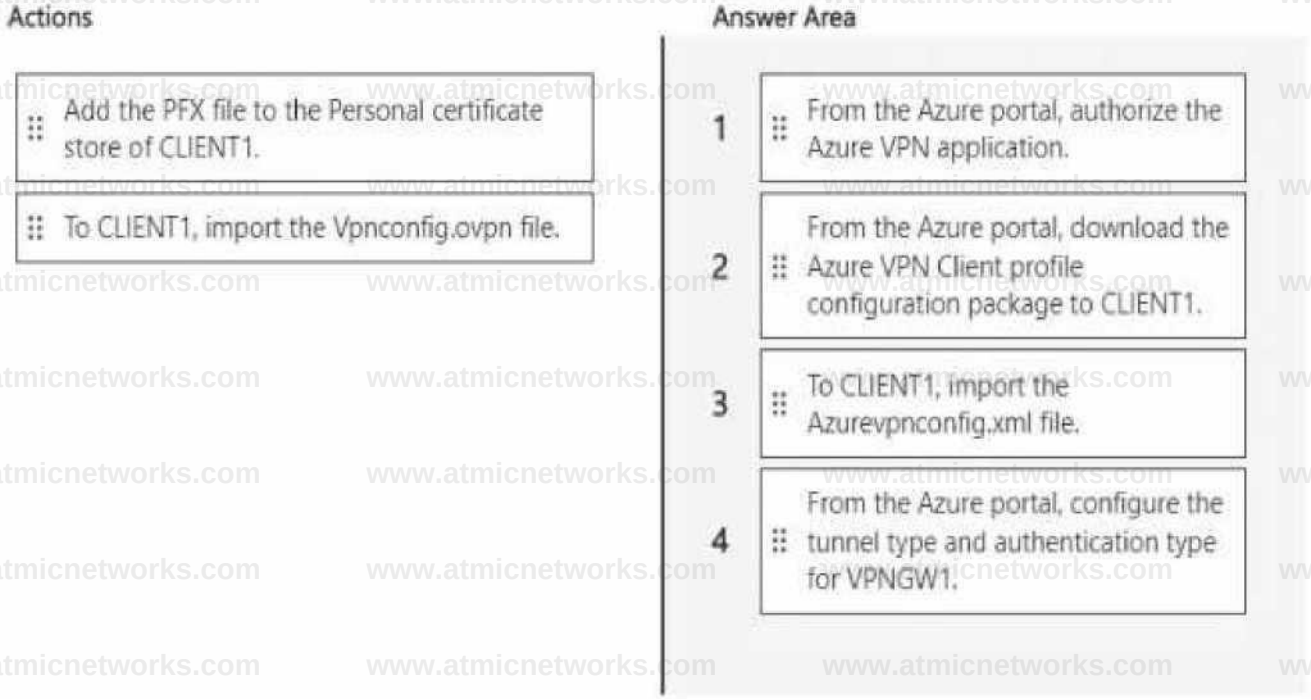
You need to ensure that you can connect CLIENT1 to VPNGW1. The solution must support Microsoft Entra authentication.

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



Answer:

Explanation:



Question: 206

You have an on-premises datacenter named Site1 that contains a firewall named FW1. FW1 connects to the internet.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNetl	Virtual network	*Notv*
WAN1	Azure Virtual WAN	Standard Virtual WAN connected to Hub1
Hub!	Azure Virtual WAN hut	Contains a Site-to-Site (S2S) VPN gateway

You plan to connect Site1 to Hub1 by using a site-to-site connection.

You need to configure the site-to-site connection to FW1.

What should you create in VWAN1?

A. a VPN site
B. a virtual network connection
C. a network virtual appliance (NVA)
D. a User VPN configuration

Answer: A

Explanation:

Question: 207

You have an on-premises network named Site1.

You have an Azure subscription that contains a storage account named storage1 and a virtual network named VNet1. VNet1 contains a subnet named Subnet1. A private endpoint for storage1 is connected to Subnet1 Site1 is connected to VNet1 by using a Site-to-Site (S2S) VPN.

You need to control access to storage1 from Site1 by using network security groups (NSGs). What should you do first?

A. Associate a route table with Subnet1.
B. Associate a NAT gateway with Subnet1.
C. Configure a network policy for private endpoints on Subnet1.
D. Create a subnet delegation on Subnet1.

Answer: C

Explanation:

Question: 208

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a subnet named Subnet1.

You plan to add a private endpoint to Subnet1.

You need to ensure that you can route traffic between the private endpoint and the Azure Private Link service by using a user-defined route.

What should you do first on Subnet1?

A. Enable network policy.
B. Enable delegation.
C. Create a service endpoint.
D. Provision a Standard Azure load balancer.

Answer: B

Explanation:

Question: 209

You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a virtual machine named VM1.

You plan to make VM1 available to the resources in Sub2 by using Azure Private Link.

You need to ensure that the private link service can be configured to provide access to VM1.

What should you configure in Sub1 first?

A. a service endpoint
B. an Azure Private DNS zone
C. a private endpoint
D. an Azure load balancer

Answer: C

Explanation:

Question: 210

You have two Azure virtual networks named VNet1 and VNet2 that are peered with each other. VNet1 hosts 10 virtual machines that contain web servers. VNet2 hosts five virtual machines that contain database servers.

You need to configure a security solution that meets the following requirements:

- Ensures that the database servers can accept connections only from the web servers
- Ensures that the web servers can initiate connections only to the database servers
- Ensures that all network security groups (NSGs) are associated only with subnets
- Use application security groups to implement the solution

What is the minimum number of application security groups required?

A. 1
B. 2
C. 4
D. 8

Answer: B

Explanation:

Question: 211

HOTSPOT

You have an Azure subscription. The subscription contains multiple Azure SQL Database resources and a virtual network named VNet1 that has five subnets. All the subnets are associated with a network security group (NSG) named NSG1. NSG1 blocks all outbound traffic, unless specifically allowed by a rule.

Each subnet contains 50 virtual machines. Multiple virtual machines host instances of SQL Server on Virtual Machines and will be configured to replicate with the Azure SQL Database resources.

You need to configure a new outbound rule in NSG1 to allow the SQL Server on Virtual Machines instances to connect to the Azure SQL Database resources. The solution must meet the following requirements:

- Minimize modifications to NSG1 when additional instances of SQL Server on Virtual Machines are deployed.
- Ensure that only SQL Server on Virtual Machines instances can connect to the Azure SQL Database resources.

How should you configure each setting for the new outbound rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Explanation:

Answer Area

Source: Application security group

Destination: Service Tag

Question: 212

You have an Azure subscription that contains 100 network security groups (NSGs).

You need to ensure that you log the application of specific NSG rules.

Which type of log should you configure?

A. flow log
B. activity log
C. Azure resource log
D. audit log

Answer: A

Explanation:

Question: 213

You are planning an Azure deployment that will contain three virtual networks in the East US Azure region as shown in the following table.

Name	Description
Vnet'	Hub virtual network for shared services
Vnet2	Virtual machines for the H department
Vnet3	Virtual machines for the research department

A Site-to-Site VPN will connect Vnet1 to your company's on-premises network.

You need to recommend a solution that ensures that the virtual machines on all the virtual networks can communicate with the on-premises network- The solution must minimize costs.
What should you recommend for Vnet2 and Vnet3?

A. service endpoints
B. route tables
C. VNet-to-VNet VPN connections
D. peering

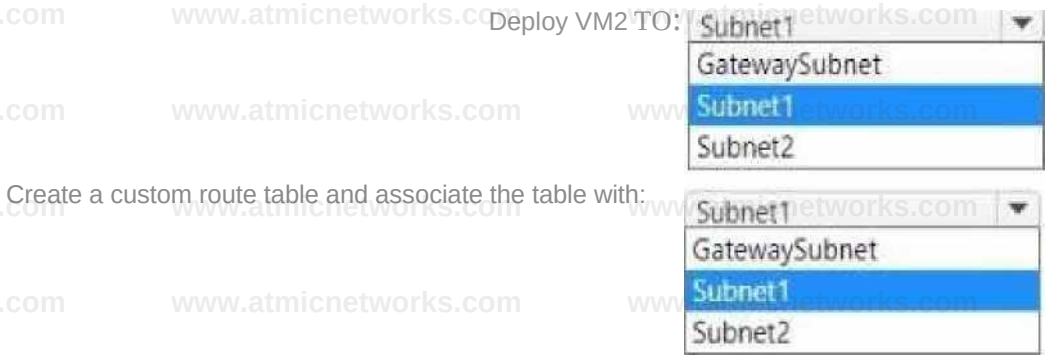
Answer: D

Explanation:

Question: 214

HOTSPOT
You have an Azure subscription that contains a virtual machine named VM1 and a virtual network named Vnet1. Vnet1 contains three subnets named Subnet1, Subnet2 and GatewaySubnet. VM1 is connected to Subnet 1.
You plan to deploy a new virtual machine named VM2 that will perform network traffic routing and inspection.
You need to ensure that all the traffic from VM1 to the internet will be routed through VM2.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Question: 215

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
storagel	Storage account	*None*
storage2	Storage account	*None*
DB1	Azure SQL Database	*None*
VNet!	Virtual network	Peered with VNet2 Contains two subnets that each contains 10 virtual machines
VNet?	Virtual network	Peered with VNet! Contains two subnets that each contains 10 virtual machines

You need to ensure that the virtual machines can access storage1, storage2, and DB1 by using service endpoints.

What is the minimum number of service endpoints you should create?

A. 2
B. 3
C. 4
D. 12

Answer: B

Explanation:

Question: 216

DRAG DROP

You have two Azure subscriptions named Sub1 and Sub2 that contain the resources shown in the following table.

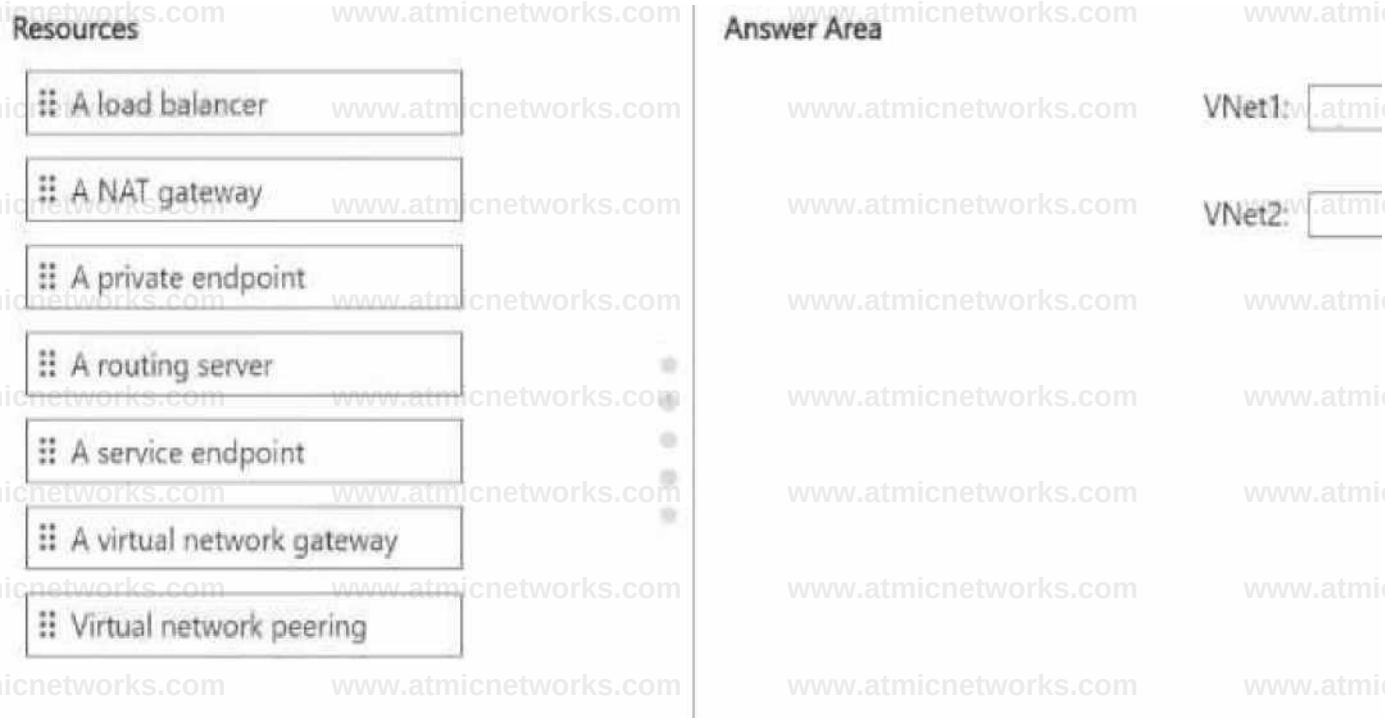
Name	Subscription	Type	Description
VNetl	Sub1	Virtual network	*None*
VM1	Sub1	Virtual machine	Connected to VNetl
VNet2	Sub2	Virtual network	*None*
VM2	Sub?	Virtual machine	Connected to VNet?
VM3	Sub2	Virtual machine	Connected to VNet2
VM4	Sub2	Virtual machine	Connected to VNet2

VNet1 and VNet2 are NOT connected.

You plan to create an Azure Private Link service named Link1 that will be used to connect VNet1 and VNet2. You need to ensure that Link1 meets the following requirements:

- Ensures that VM1 can connect only to a web app hosted on VM2
- Prevents VM1 from connecting to the other resources that are connected to VNet2

Which additional resources should you create for each virtual network? To answer, drag the appropriate resources to the correct virtual networks. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Resources

:: A load balancer

:: A NAT gateway

:: A private endpoint

:: A routing server

J:: A service endpoint

|:; A virtual network gateway

:: Virtual network peering

Answer Area

VNet! [A private endpo

VNet2 Virtual network

Question: 217

HOTSPOT

You have an Azure subscription that contains a virtual network named VNet1. VNet1 uses an IP

address space of 192.168.0.0/24. You plan to deploy Azure virtual machines and Azure Bastion to VNet1.

You need to recommend an IP subnetting configuration for VNet1. The solution must maximize the number of IP addresses that can be assigned to the virtual machines

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Bit mask for the larger virtual machine subnet

Maximum number of IP addresses available for assignment to the virtual machines:

Answer:

Explanation:

Answer Area

Bit mask for the larger virtual machine subnet' /26

Maximum number of IP addresses available for assignment to the virtual machines: 182

Question: 218

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains an Azure Virtual Desktop host pool named Pool1.

You need to implement Azure Firewall and TLS inspection for all the outbound traffic from Pool1. Which two resources should you configure? Each correct answer present part of the solution. NOTE: Each correct answer is worth one point

A. an Azure Private DNS zone
B. a private endpoint
C. an Azure key vault
D. an Azure NAT gateway
E. a Microsoft Entra enterprise app
F. a managed identity

Answer: D, F

Explanation:

Question: 219

DRAG DROP

You have two on-premises datacenters.

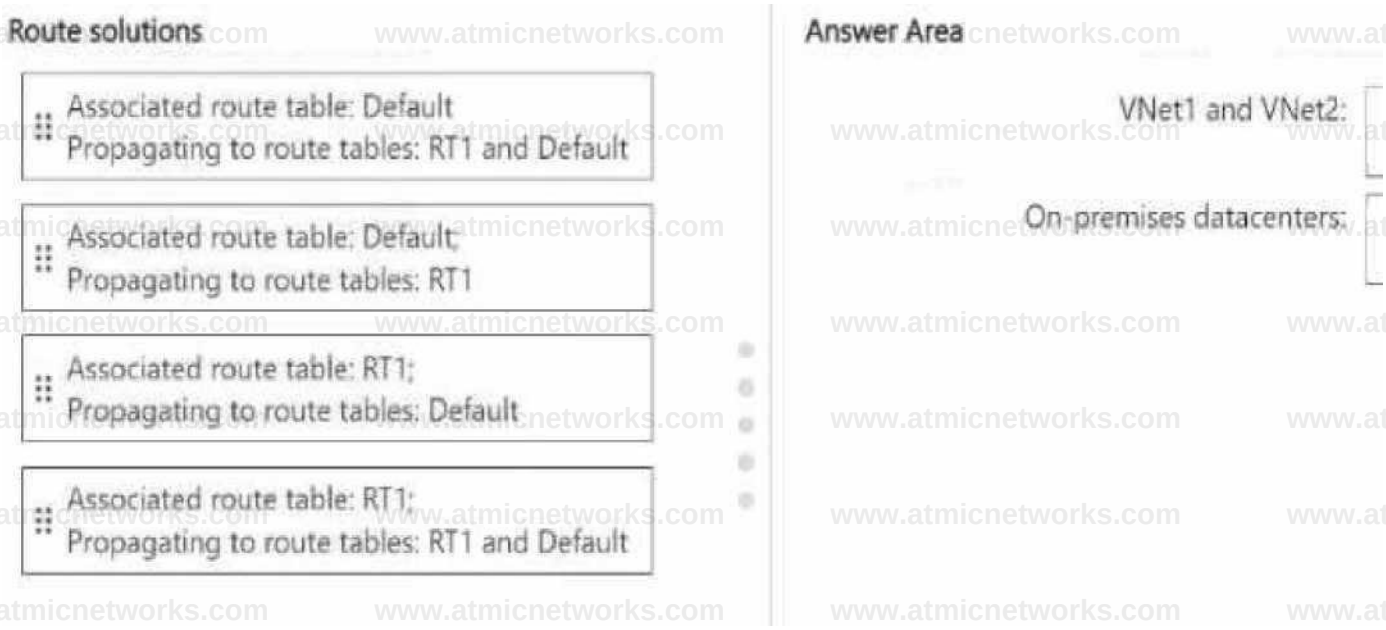
You have an Azure subscription that contains four virtual networks named VNet1 VNet2, VNet3, and VNet4 You create an Azure virtual WAN named VWAN1. VWAN1 contains a single virtual hub that is connected to both on-premises datacenters and all the virtual networks in a full mesh topology. You create a route table named RT1.

You need to configure VWAN1 to meet the following requirements:

- Connectivity between VNet1 and VNet2 and both on-premises datacenters must be allowed.
- Connectivity between VNet3 and VNet4 and both on-premises datacenters must be allowed.
- VNet1 and VNet2 must be isolated from VNet3 and VNet4.

How should you configure routing for VNet1 and VNet2 and for both on-premises datacenters? To answer, drag the appropriate route tables and route table propagation to the correct requirements. Each route table and route table propagation may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Question: 220

DRAG DROP

Your on-premises network uses an IP address space of 10.0.0.0/20.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
RT1	Route table	*None*
HubVNet	Virtual network	Uses an IP address space of 1*12* 160 0/20 Peered to SpokeVNet
SpokeVNet	Virtual network	Uses an IP address space of 192 168,0.0/20

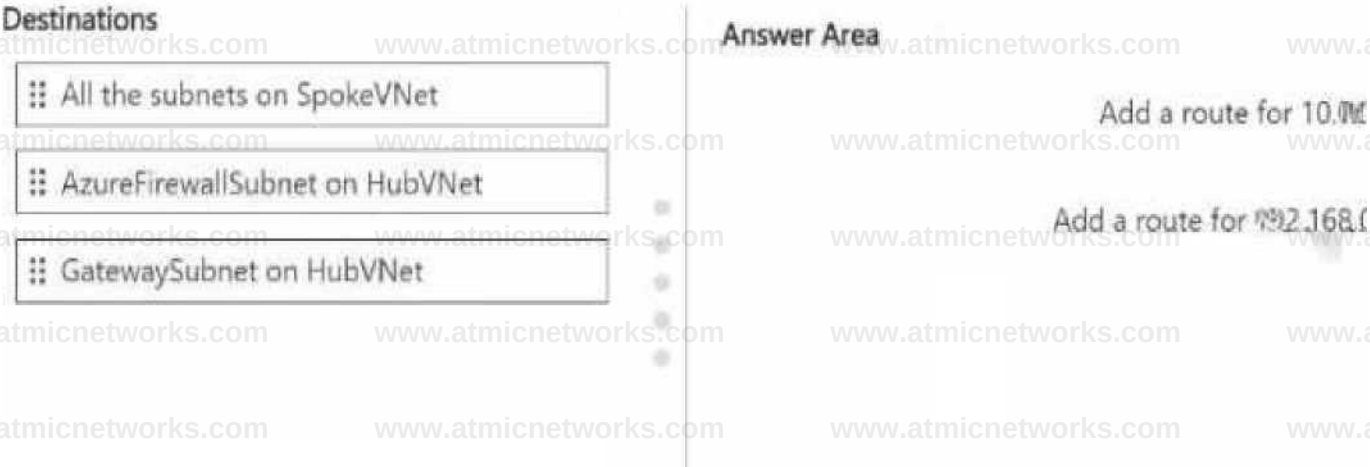
The on-premises network is connected to HubVnet by using a Site-to-Site (S2S) VPN.

You deploy an Azure firewall named AZFW1 to HubVNet.

You need to ensure that AZFW1 can inspect all the traffic between the on-premises network and SpokeVNet.

What should you do in RT1? To answer, drag the appropriate destination to the correct route. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Destinations

;; Ail the subnets on SpokeVNet

IS AzurePirewjllSubnet on HubVNet

Answer Area

Add a route for 1O.'W 0/2)uTid specify AZFW1 as the next hop for: IAllthesubrrahs'n^^

Add a route for '^2 J6LD.0/20 and specify AZFW1 as the next hop foe [Gaiew^Ltat^^

■■ GatewaySubnet on HubVNet

Question: 221

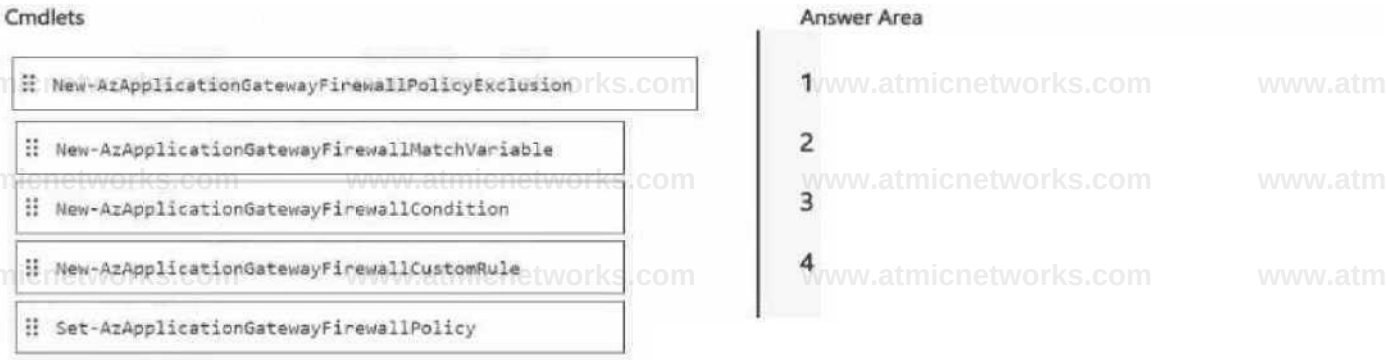
DRAG DROP

You have an Azure Web Application Firewall (WAF) v2 tier named AG1 on an Azure application gateway. AG1 has a policy named Policy 1.

You need to add a custom rule to Policy 1. The rule must block all requests from IP addresses in a specific IP address range.

Which four PowerShell 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.

- TLS inspection



Answer:

Explanation:

Cm diets

:: New-AzApplicationGattwayFir«kallPolicyExclusion

Answer Area

1 :: New-AzApplicationGatawayFirewallMatchVariabla

2 :: New-AzApplicationGatewayFirewallCondition

3 :: New*AzApplicationG<tewayFirewallCustMiRule

4 :: Set-AzApplicationGatewayFirewallPolicy

Question: 222

You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFW1.

You plan to enable the following:

- Threat intelligence
- A network intrusion detection and prevention system (IDPS) What can you enable by using AzFW1?

A. TLS inspection only
B. threat intelligence only
C. TLS inspection and the IDPS only
D. threat intelligence and the IDPS only
E. TLS inspection, threat intelligence, and the IDPS

Answer: E

Explanation:

Question: 223

You have an on-premises DNS server named Server1 that hosts a primary DNS zone named fabrikam.com.
You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNetl	Virtual network	In the US West Azure region
VNet2	Virtual network	In the US West Azure region
VNet3	Virtual network	In the West Europe Azure region
VNet4	Virtual network	In the West Europe Azure region
contoso.com	Azure Private DNS zone	In the West Europe Azure region and linked to VNetl. VNet2 VNet3, and VNet4

Users on the on-premises network access resources on all the virtual networks by using a Site-to-Site (S2S) VPN. You need to deploy an Azure DNS Private Resolver solution that meets the following requirements:

- Resources connected to the virtual networks must be able to resolve DNS names for fabrikam.com.
- Server1 must be able to resolve the DNS names of the resources in contoso.com.
- The solution must minimize costs and administrative effort.

What is the minimum number of resolvers you should deploy?

A. 1
B. 2
C. 3
D. 4

Answer: B

Explanation:

Question: 224

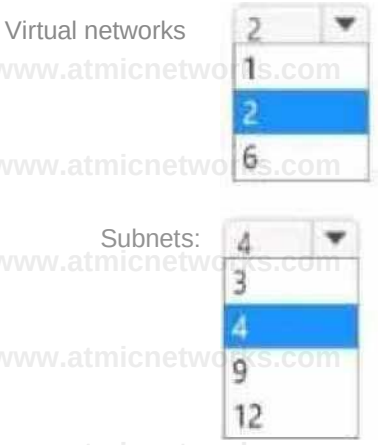
HOTSPOT
You have two Azure subscriptions.
You need to perform the following actions in the East US Azure region of each subscription:

- Deploy 50 virtual machines to availability zone 1.
- Deploy 50 virtual machines to availability zone 2.
- Deploy 50 virtual machines to availability zone 3.

What is the minimum number of virtual networks and /25 subnets you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Virtual networks: 2

Subnets: 4

Question: 225

HOTSPOT

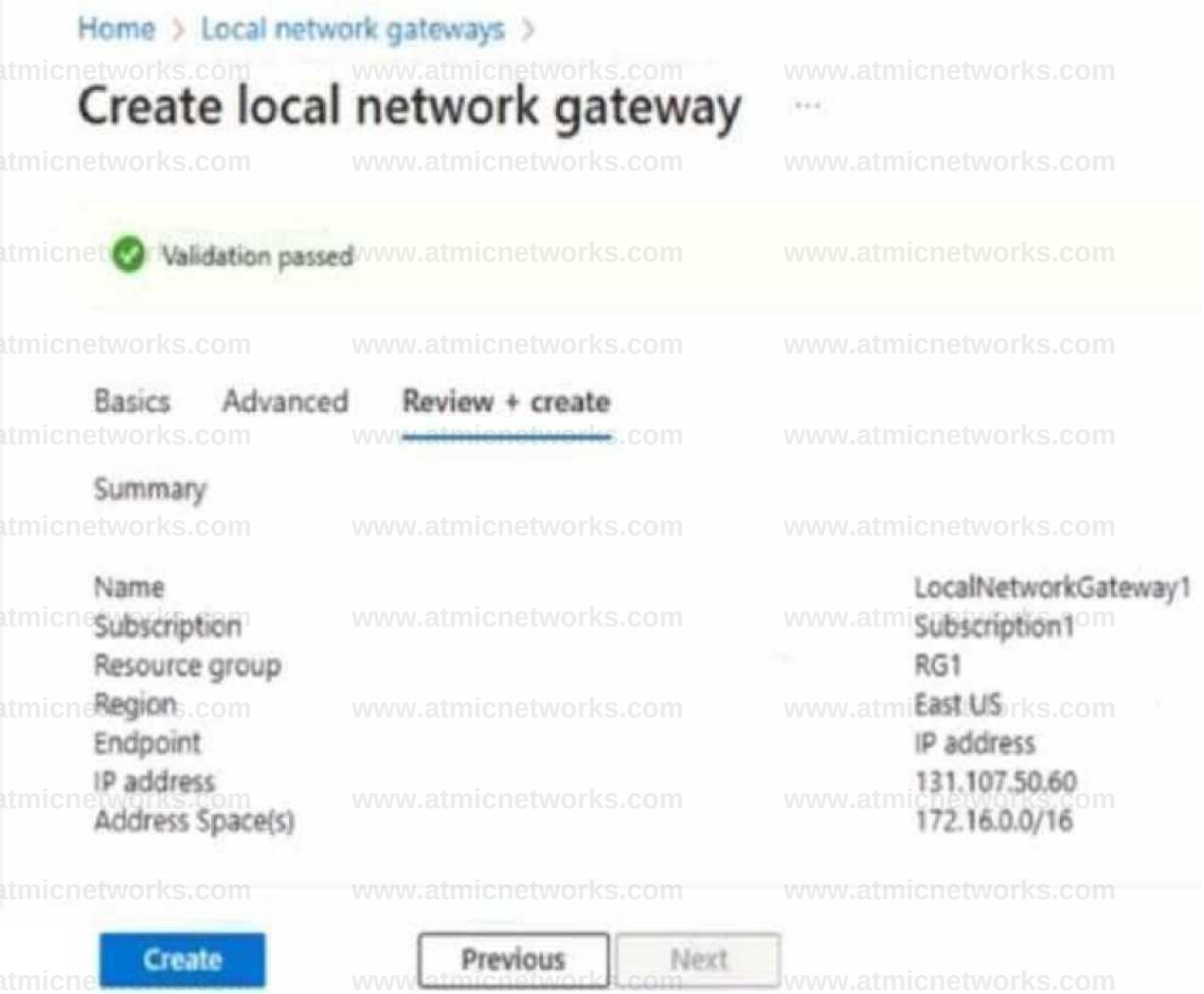
You have an on-premises network that includes the sites shown in the following table.

Site	Site Address space	Firewall private IP	Firewall public 1P address
Paris	172 16.0.0/24	17216.0 1	131.10750.60
Amsterdam	17216.1.0/24	172.16.1.1	131 10770.80
Berlin	172 16 2 0/24	172 16.2 1	131 107.90,100

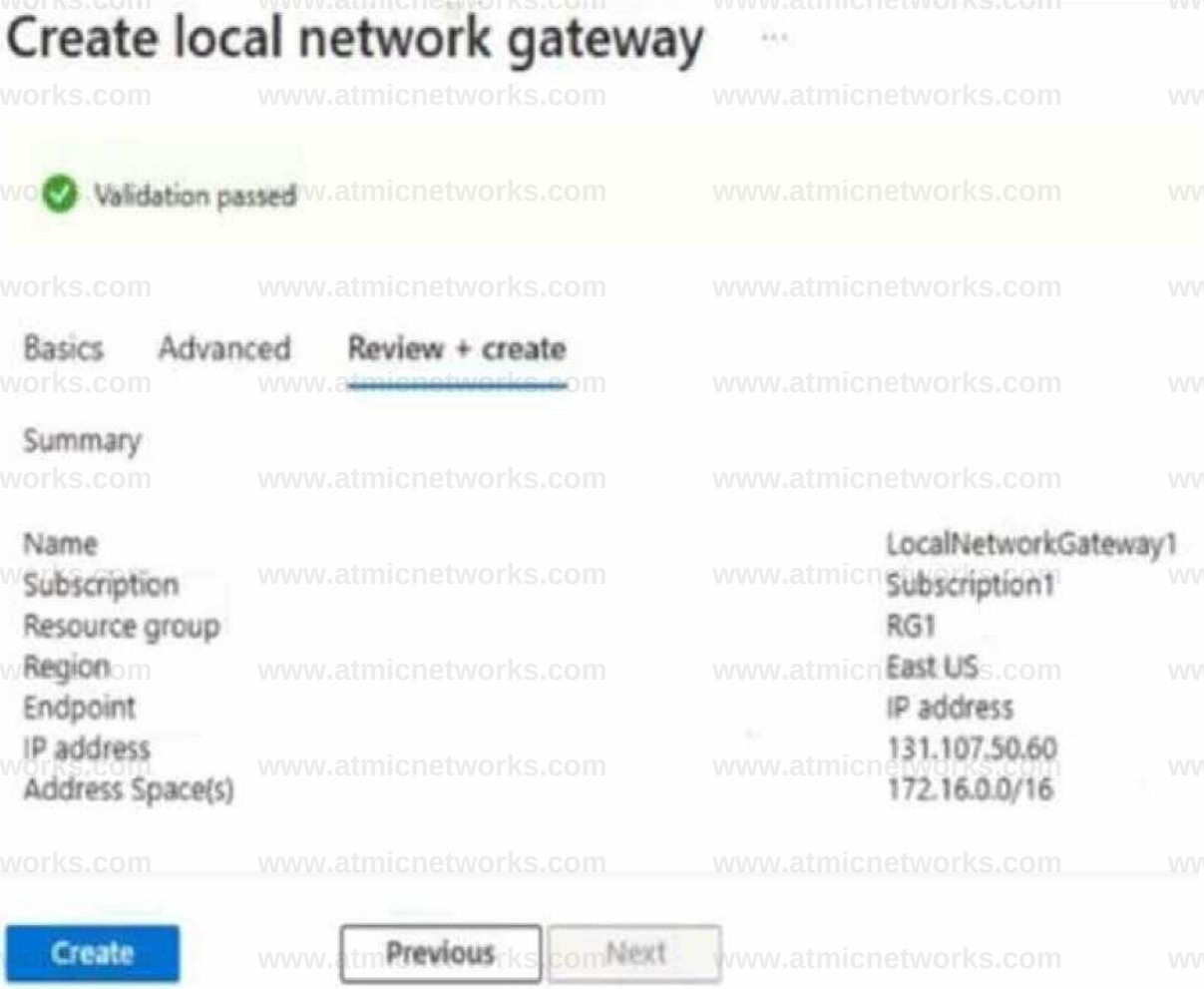
Each site is connected to the Internet by a firewall. All sites are connected to an SD-WAN. Each site is configured to propagate routes by using BGP.

You have an Azure subscription that includes a virtual network named Vnet1 that contains a Virtual Network Gateway named Gateway 1.

You create a local network gateway with the configuration shown in the gateway exhibit (Click the Gateway tab.)



You create a Site-to-Site (S2S) connection with the configuration shown in connection exhibit. (Click the Connection tab)



For each of the following statements, select Yes if the statement is true Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Users in the Berlin site can connect to resources in Vnetl via VPN1		
To create a direct Site-to-Site connection to the Berlin site an additional Local Network Gateway is required.		
To enable users in the Paris site to connect to Vnetl. the IP address of LocalNetworkGatewayl must be changed to 172 16.0 1	O	Q

Answer:

Explanation:

Answer Area

Statements	Yes	No
Users in the Berlin site can connect to resources in Vnetl via VPN1	8	
To create a direct Site-to-Site connection to the Berlin site an additional Local Network	3	I

Gateway is required.

To enable users in the Pans site to connect to Vnetl, the IP address of Local NetworkGatewayl must be changed to 17216.01

Question: 226

HOTSPOT

You have an Azure subscription that contains multiple virtual machine scale sets and multiple Azure load balancers. The load balancers balance traffic across the scale sets.

You plan to deploy Azure Front Door to load balance traffic across the load balancers.

You need to identify which Front Door SKU to configure, and what to use to route the traffic to the load balancers. The solution must minimize costs.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

SKU: Premium

Classic

Standard

Use Azure Private Link

Azure Private Link

Azure Route Server

A service endpoint

Answer:

Explanation:

Answer Area

SKU Premium

Use' Azure Private Link

Question: 227

You have an Azure subscription. The subscription contains a locally-redundant storage 1LRS) account named stoiage1 that is deployed to the US East Azure region and has a Microsoft Storage service endpoint.

You set Redundancy for storage 1 to Read-access geo-redundant storage (RA-GRS)

You need to ensure that the contents of storage1 will be accessible by using a service endpoint in a paired region. The solution must minimize administrative effort What should you do first?

A. Create an object replication rule for storage1.
B. From storage1. select Secure transfer required.

C. Create a service endpoint policy.
D. Delete the existing service endpoint.

Answer: D

Explanation:

Question: 228

You have an on-premises network named Site1.

You have an Azure subscription that contains a virtual network named VNet1 and a storage account named storage1.
Site1 and VNet1 are connected by using a Site-to-Site (S2S) VPN.

You need to ensure that the servers in Site! can connect to storage! by using the S2S VPN The solution must minimize administrative effort.
What should you create on VNet1?

A. an Azure application gateway
B. an Azure Private Link service
C. a private endpoint
D. a service endpoint

Answer: C

Explanation:

Question: 229

You have an Azure subscription that contains a virtual network named VNet1.
You deploy several web apps and configure the apps to use private endpoints on VNet1.
You need to identity which DNS records the web apps registered automatically.
Where will the records be created?

A. an Azure DNS zone named azurewebsites net
B. an Azure Private DNS zone named azurewebsites.net
C. an Azure DNS zone named privatelink.azurewebsites.net
D. an Azure Private DNS zone named piivatelink.azurewebsites.net

Answer: D

Explanation:

Question: 230

You have an Azure subscription.

You plan to deploy Azure Firewall Premium, enable all the Premium features, and configure both network and application

rules.

Which type of rule will the firewall process first?

A. infrastructure
B. network
C. threat intelligence
D. application

Answer: B

Explanation:

Question: 231

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
Vnetl	Virtual network	In the US East Azure region
LB1	Load balancer	Basic SKU
VM1	Virtual machine	Connected to Vnetl Member of the backend pool of LB1
VM2	Virtual machine	Connected to Vnet 1 Member of the backend pool of LB1

You create a virtual network named Vnet2 in the West US region.

You plan to enable peering between Vnet1 and Vnet2.

You need to ensure that the virtual machines connected to Vnet2 can connect to VM1 and VM2 via LB1.

What should you do?

A. Change the Floating IP configurations of LB1.
B. From the Peerings settings of Vnet2. set Traffic forwarded from remote virtual network to Allow
C. Change the SKU of LB1
D. From the Peerings settings of Vnet1, set Traffic forwarded from remote virtual network to Allow.

Answer: C

Explanation:

Question: 232

DRAG DROP

You have a DNS domain named contoso.com that is hosted by a thud party domain name registrar.

You have an Azure subscription.

You need to ensure that all DNS queries for the contoso.com domain are resolved by using Azure DNS.

What should you create in the registrar, and what should you create in Azure? To answer, drag the appropriate options to the correct targets Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Options

- A delegation
- A DNS subdomain
- A forwarder
- A primary DNS zone
- A private DNS zone
- A public DNS zone
- A secondary DNS zone

Answer Area

Answer:

Explanation:

Question: 233

HOTSPOT

You have an Azure subscription that contains 1.000 virtual machines.

You collect network security group (NSG) flow logs.

You need to identify all the virtual machines that have interacted with non-Azure public IP addresses during the last 30 days

How should you complete the query? To answer, select the appropriate options in the answer area

NOTE; Each correct selection is worth one point.

Answer Area

```
AxU'eNetwoikAnatytics ᵀ CI
SS^SEiSi
NetwockAccessTraffic
NTANetAnalytics
| where SubType s ~ "flowlog' and FlowStarttIne
| project vLrtualwchine • vmi s
| distinct virtualMchine
```

Ro<

FlowType_s
AllowedOutFlows_d
FlowType_s
ThreatType

Answer:

Explanation:

Answer Area

```
AzureNetwotkAnalytics ' _CI
| »lwre Sublyp* » — "flowlog" and F|ow$startt|Me t >- ago(tod) and FlowType
| project virtuahHKhine • vmts
| distinct virtualnuchine
```

Question: 234

HOTSPOT

You have an on premises web server that hosts a web app named App1 and has the following configurations:

- IP address 131.107.50.60
- FQDN server1.contoso.com

You have an Azure subscription.

You need to publish App1 by using Azure Front Door. The solution must meet the following requirements:

- Ensure that internet users can connect to App1 by using an FQDN of appl.contoso.com.
- Minimize the changes required to the configuration of Front Door if Server 1 is migrated to Azure.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Set the DNS record for appl contoso.com to: I A CNAME record of appt • < GUIC
An A record of 131 107 50 60
A CNAME record of servefl contc

From the Front Door profile, set the origin host name to. jpp| contosocom *
131 107S060[

server 1 contoso com

Answer:

Explanation:

Answer Area

Set the DNS record for appl contoso.com to: A CNAME record of app1-<GUID

From the Front Door profile, set the origin host name to appl contoso com *

Question: 235

DRAG DROP

You have the resources shown in the following table.

Name	Type	Description
Group1	Microsoft Entra group	*None*
Group?	Microsoft Entra group	*None*
VPNGW1	Azure VPN Gateway	Supports Point to Site |P2S) VPN connections
VPNGW?	Azure VPN Gateway	Supports Point to Site (P?S) VPN connections

From the Microsoft Entra admin center, you register the Azure VPN application as an enterprise application.

You need to enable Microsoft Entra authentication for the P2S VPN connections. The solution must meet the following requirements;

- Ensure that only the members of Group1 can establish VPN connections to VPNGW1.

- Ensure that only the members of Group2 can establish VPN connections to VPNGW2.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Actions

From the Microsoft Entra admin center, register two apps named Appl and App? Assign Groupl to Appl and assign Group? to App?

From the Microsoft Entra admin center, add a scope to Appl and App?

From the Microsoft Entra admin center, add a client app to Appl and App?

From the Azure portal, configure the Point to site configuration settings for VPNGW1 and VPNGW2

Answer Area

Answer:

Explanation:

Actions

Answer Area

From the Microsoft Entra admin center, register two apps named Appt and App? Assign Group! to App1 and assign Group? to App?

From the Microsoft Entra admin center add a scope to App! and App?

.. horn the Microsoft Entra admin center, add a client app to Appt " and App?

4 From the Azure portal, configure the Point to site configuration settings lor VPNGW1 andVPNGW?

Question: 236

You have an Azure subscription that contains a virtual network named VNet1 and the virtual machines shown in the following table.

Name	IP address	Hosted application protocol
VMI	101 1 11	HTTPS (TCP port 443)
VM2	101 1 21	SMTP (TCP port 25)
VM3	101.1.31	SFTP (TCP port 22)

All the virtual machines are connected to VNet1.

You need to ensure that the applications hosted on the virtual machines can be accessed from the internet. The solution must ensure that the virtual machines share a single public IP address What should you use?

A. a NAT gateway
B. an internal load balancer

C. a public load balancer
D. Azure Application Gateway

Answer: C

Explanation:

Question: 237

You have the on-premises networks shown in the following table.

Name	ASN	IP address space	Connection tt*	Description
Stanch 1	64551	10.50 0 0/24 10.61.00/16	VPN	Is an on premises datacenter
Stanch?	64551	10 50 0 0/16,1061 00/16	VPN and ExptessRoute	AS Path has a prefix of 64551 64551,64551
Branch3	64551	10 50 2 0/24,10.61 00/16	ExpressRoute	*None*

You have an Azure subscription that contains an Azure virtual WAN named VWAN1 and a virtual network named VNet1 VWAN1 is connected to the on-premises networks and VNet1 in a full mesh topology. The virtual hub routing preference for VWAN1 is AS Path.

You need to route traffic from VNet1 to 10.61.1.5.

Which path will be used?

A. the ExpressRoute connection to Branch2
B. the ExpressRoute connection to Branch3
C. the VPN connection to Branch1
D. the VPN connection to Branch2

Answer: D

Explanation:

Question: 238

DRAG DROP

You have an Azure subscription that contains an Azure VPN gateway named GW1. GW1 provides Point-to Site (P2S) VPN connectivity.

Users connect to GW1 from a Windows 11 device by using an SSTP connection.

You need to ensure that the P2S VPN connections support Microsoft Entra authentication.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for and of the correct orders you select.

Actions

Answer Area

Register the Microsoft Hybrid Network resource provide

For the point to site configuration of GW1. set Authentication type to Microsoft Entra and set Tunnel type to OpenVPN (SSL)

Grant the Azure VPN application admin consent to the Microsoft Entra tenant

Fer the point to site configuration of GW1 set Authentication type to Microsoft Entra and set Funnel type to IKEv2 and SSTP (SSL)

Download the Azure VPN Client profile configuration package and distribute the package to the users

Answer:

Explanation:

Actions

:: Register the Microsoft HybridNetwork resource provider

„ For the point to site configuration of GW1, set Authentication type to ” Microsoft Entra and set Tunnel type tc OpenVPN (SSL)

Answer Area

„ Grant the Azure VPN a ” Entra tenant

For the point to site ci 2 :: type to Microsoft Entri (SSL)

- .. Download the Azure V *' and distribute the pad

Question: 239

HOTSPOT

You create an ExpressRoute circuit named ERC1 that is enabled by your connectivity provider.

You need to ensure that the routes for Azure Backup and Azure Cosmos DB are advertised to the onpremises network via ECR1. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

On the EiptfssRoutt circuit, configure

Microsoft peering
Azure private peerin g
Microsoft peering

Assoc ate the ExpressRoute circuit with

xite filter and a single filter rule
A route filter and a single filter rule
A route filter and two filter rules
Two route filters and a single filter rule

Answer:

Explanation:

Answer Area

On the ExpressRoute circuit, configure: Microsoft peering

Associate the ExpressRoute circuit with A route filter and a single filter rule

Question: 240

DRAG DROP

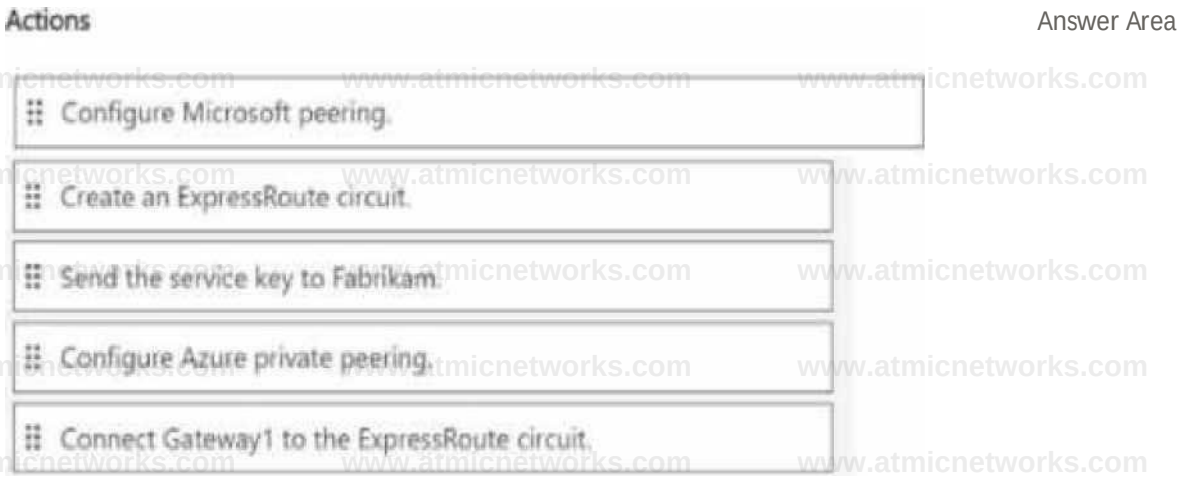
You have an on-premises network

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains an ExpressRoute gateway named Gateway 1.

You need to implement an ExpressRoute solution from a third-party provider named Fabrikam, Inc.

The solution must ensure that devices on the on-premises network can connect to the Azure resources on VNet1.

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



Answer:

Explanation:

Actions

Configure Microsoft peering

Answer Area

1 Create an ExpressRou
2 Send the service key t
3 Configure Azure priva
4 Connect Gateway1 to

Question: 241

DRAG DROP

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2.

You plan to deploy the resources shown in the following table.

Name	Type	On virtual network	Description
VMSS1	Virtual machine scale set	VNetl	Each virtual machine hosts an application named Appl
VM1	Virtual machine	VN«2	Is a network virtual appliances (NVA)
VM2	Virtual machine	VNet2	Is a network virtual appliance (NVA

You need to deploy two load balancers to manage the traffic for VMSS1, VM1. and VM2. The solution must meet the following requirements:

- Either VM1 or VM2 must inspect all the traffic from the internet to App1.
- All user connections from the internet to App1 must be load balanced.
- Costs must be minimized.

Which load balancer SKU should you include in the solution? To answer, drag the appropriate SKUs to the correct resources. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

SKUs

Basic | Gateway | Standard

Answer Area

VMSS1:

VM1 and VM2:

Answer:

Explanation:

SKUs

Basic | Gateway | Standard

Answer Area

VMSS1 [Basic

VM1 and VM2

Gateway

Question: 242

You have an Azure subscription that contains the resources shown in the following table.

Name	Description
App1	Web app
FD1	Azure Front Door Premium profile that has an endpoint and an origin group

You need to configure a solution to meet the following requirements;

- App1 must be assigned a private endpoint
- Access to App1 from the internet must be routed via FD1.

What should you configure on FD1?

A. a rule that has the route configuration override action
B. a route that redirects traffic
C. an origin that enables the Azure Private Link service
D. a security policy that redirects traffic

Answer: C

Explanation:

Question: 243

You have an on-premises server named Server1 that runs Windows Server.

You have an Azure subscription that contains a virtual network named VNet1.

You plan to connect Server1 to VNet1 by using Azure Network Adapter.

You need to minimize how long it takes to deploy the adapter to Server1. What should you create first?

A. an Azure VPN gateway
B. a route server
C. a private endpoint
D. an Azure Bastion host

Answer: A

Explanation:

Question: 244

HOTSPOT

You have an Azure subscription.

You plan 10 implement an Azure application gateway named AGW1.

You need to implement an external TLS certificate store for AGW1. The solution must meet the following requirements:

- Keys must be stored by using the highest possible security.
- Administrative effort must be minimized.

Which type of certificate store should you use, and which type of identity should you use to access the store?

To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

Certificate store type Azure Key VaulcManaged HSM L.

Azure Dedicated HSM

Azure Key Vault

Azure Key Vault Managed HSM

Identity type. Security principal

Security principal

System-assigned managed identity User-assigned managed identity

Answer:

Explanation:

Answer Area

Certificate store type Azure Key Vault Managed HSM

Identity type- Security principal

Question: 245

HOTSPOT

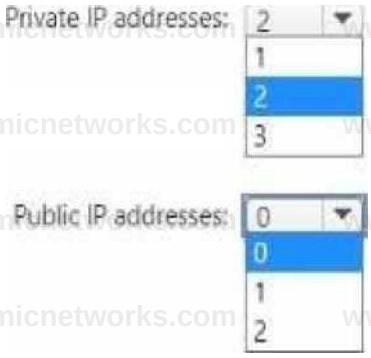
You have an Azure subscription that contains a virtual network named VNet1.

You need to deploy an instance of Azure Application Gateway v2 named AppGw1 to VNet1. AppGw1 will include one basic listener and two multi-site listeners. The listeners will be accessible only from VNet1.

What is the minimum number of IP addresses required for AppGw1? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Private IP addresses: 2

Public IP addresses. 0

Question: 246

HOTSPOT

You have an Azure subscription. The subscription contains 500 virtual machines that run either Windows 11 or Linux.

You need to identify which Linux virtual machines are accessible from the internet. The solution must minimize administrative effort.

What should you use, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use: Cfoudsecurity explorer in Micros:" _ -. - , - -- J^Q *

¡ Attack path analysis in Microsoft Defender for Cloud

Cloud security explorer in Microsoft Defender for Cloud

| Microsoft Defender External Attack Surface Management (Defender EASM)

Configure: Agentless scanning for machines in Microsoft Defender for Cloud |

A discovery group in Microsoft Defender External Attack Surface Management (Defender EASM)

Agentless scanning for machines in Microsoft Defender for Cloud

| An inventory filter in Microsoft Defender External Attack Surface Management (Defender EASM)

Answer:

Explanation:

Answer Area

Use: Cloud security explorer in Microsoft Defender for Cloud

Configure: Agentless scanning for machines in Microsoft Defender for Cloud

Question: 247

HOTSPOT

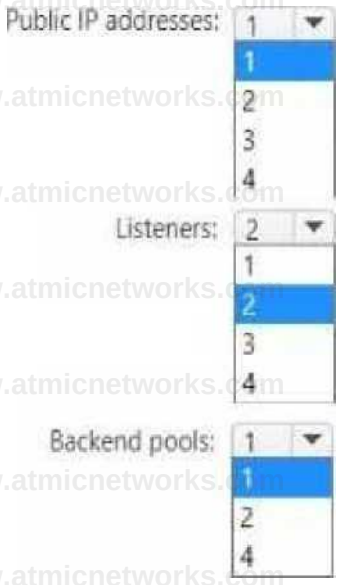
You have an Azure subscription that contains an Azure application gateway named AG1 and two Azure App Service apps named App1 and App2 that have the following configurations:

- Both apps are accessible by using HTTP and HTTPS.
- HTTP host headers are used to route requests to the appropriate apps.
- Both apps are hosted in a single App Service Environment in the West Europe Azure region. You need to publish the apps by using AG1. The solution must ensure that AG1 provides both HTTP and HTTPS access.

What is the minimum number of resources required for AG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Public IP addresses: 1 ¥

Listeners: 2 ’

Backend pools: 1 ’

Topic 4, Labs / Tasks

Question: 248

SIMULATION

Task 1

You plan to deploy a firewall to subnetI-2. The firewall will have an IP address of 10.1.2.4.
You need to ensure that traffic from subnetI-1 to the IP address range of 192.168.10.0/24 is routed through the firewall that will be deployed to subnetI-2. The solution must be achieved without using dynamic routing protocols.

Answer: See the Explanation below for step by step instructions.

Explanation:

To deploy a firewall to subnetI-2, you need to create a network virtual appliance (NVA) in the same virtual network as subnetI-2. An NVA is a virtual machine that performs network functions, such as firewall, routing, or load balancing1.
To create an NVA, you need to create a virtual machine in the Azure portal and select an image that has the firewall software installed. You can choose from the Azure Marketplace or upload your own image2.
To assign the IP address of 10.1.2.4 to the NVA, you need to create a static private IP address for the network interface of the virtual machine. You can do this in the IP configurations settings of the network interface3.
To ensure that traffic from subnetI-1 to the IP address range of 192.168.10.0/24 is routed through the NVA, you need to create a user-defined route (UDR) table and associate it with subnetI-1. A UDR table allows you to override the default routing behavior of Azure and specify custom routes for your subnets4.
To create a UDR table, you need to go to the Route tables service in the Azure portal and select + Create. You can give a name and a resource group for the route table5.
To create a custom route, you need to select Routes in the route table and select + Add. You can enter the following information for the route5: Destination: 192.168.10.0/24
Next hop type: Virtual appliance
Next hop address: 10.1.2.4

To associate the route table with subnetI-1, you need to select Subnets in the route table and select + Associate.
You can select the virtual network and subnet that you want to associate with the route table5.

Question: 249

SIMULATION

Task 2

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

- Has an IP address from the address range of 10.1.255.0/24
- Uses a new Premium firewall policy named FW-pohcy1
- Routes traffic directly to the internet

Answer: See the

Explanation below for step by step instructions.

Explanation:

To create an Azure Firewall instance, you need to go to the Azure portal and select Create a resource. Type firewall in the search box and press Enter. Select Firewall and then select Create1.
To assign an IP address from the address range of 10.1.255.0/24 to the firewall, you need to select a public IP address that belongs to that range. You can either create a new public IP address or use an existing one1.
To use a new Premium firewall policy named FW-policy1, you need to select Premium as the Firewall tier and create a new policy with the name FW-policy12. A Premium firewall policy allows you to configure advanced features such as TLS Inspection, IDPS, URL Filtering, and Web Categories3.
To route traffic directly to the internet, you need to enable SNAT (Source Network Address Translation) for the firewall. SNAT allows the firewall to use its public IP address as the source address for outbound traffic4.

Question: 250

SIMULATION

Task 3

You plan to implement an Azure application gateway in the East US Azure region. The application gateway will have Web Application Firewall (WAF) enabled.
You need to create a policy that can be linked to the planned application gateway. The policy must block connections from IP addresses in the 131.107.150.0/24 range. You do NOT need to provision the application gateway to complete this task.

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for creating a policy that can be linked to the planned application gateway and block connections from IP addresses in the 131.107.150.0/24 range: To create a policy, you need to go to the Azure portal and select Create a resource. Search for WAF, select Web Application Firewall, then select Create1.
On the Create a WAF policy page, Basics tab, enter or select the following information and accept the defaults for the remaining settings:
Policy for: Regional WAF (Application Gateway)
Subscription: Select your subscription name
Resource group: Select your resource group
Policy name: Type a unique name for your WAF policy
On the Custom rules tab, select Add a rule to create a custom rule that blocks connections from IP addresses in the 131.107.150.0/24 range2. Enter or select the following information for the custom rule:
Rule name: Type a unique name for your custom rule
Priority: Type a number that indicates the order of evaluation for this rule
Rule type: Select Match rule

Match variable: Select RemoteAddr
Operator: Select IPMatch
Match values: Type 131.107.150.0/24
Action: Select Block
On the Review + create tab, review your settings and select Create to create your WAF policy1.
To link your policy to the planned application gateway, you need to go to the Application
Gateway service in the Azure portal and select your application gateway3.
On the Web application firewall tab, select your WAF policy from the drop-down list and select Save

Question: 251

SIMULATION

Task 4

You need to ensure that connections to the storage34280945 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name storage34280945.pnvatelinlcblob.core.windows.net.

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that connections to the storage34280945 storage account can be made by using an IP address in the 10.1.1.0/24 range and the name stor-age34280945.pnvatelinlcblob.core.windows.net:
To allow access from a specific IP address range, you need to configure the Azure Storage firewall and virtual network settings for your storage account. You can do this in the Azure portal by selecting your storage account and then selecting Networking under Settings1.
On the Networking page, select Firewalls and virtual networks, and then select Selected networks under Allow access from1. This will block all access to your storage account except from the networks or resources that you specify.
Under Firewall, select Add rule, and then enter 10.1.1.0/24 as the IP address or range. You can also enter an optional rule name and description1. This will allow access from any IP address in the 10.1.1.0/24 range.
Select Save to apply your changes1.
To map a custom domain name to your storage account, you need to create a CNAME record with your domain provider that points to your storage account endpoint2. A CNAME record is a type of DNS record that maps a source domain name to a destination domain name.
Sign in to your domain registrar's website, and then go to the page for managing DNS settings2.
Create a CNAME record with the following information2:
Source domain name: stor-age34280945.pnvatelinlcblob.core.windows.net
Destination domain name: stor-age34280945.pnvatelinlcblob.core.windows.net
Save your changes and wait for the DNS propagation to take effect2.
To register the custom domain name with Azure, you need to go back to the Azure portal and select your storage account. Then select Custom domain under Blob service2.
On the Custom domain page, enter stor-age34280945.pnvatelinlcblob.core.windows.net as the custom domain name and select Save2.

Question: 252

SIMULATION

Task 5

You need to ensure that requests for wwwjelecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net.

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that requests for wwwjelecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net:

To use a custom domain with your Azure Front Door, you need to create a CNAME record with your domain provider that points to the Front Door default frontend host. A CNAME record is a type of DNS record that maps a source domain name to a destination domain name1.

To create a CNAME record, you need to sign in to your domain registrar's website and go to the page for managing DNS settings1.

Create a CNAME record with the following information1:

Source domain name: wwwjelecloud.com

Destination domain name: frontdoor1.azurefd.net

Save your changes and wait for the DNS propagation to take effect1.

To verify the custom domain, you need to go to the Azure portal and select your Front Door profile. Then select Domains under Settings and select Add2.

On the Add a domain page, select Non-Azure validated domain as the Domain type and enter wwwjelecloud.com as the Domain name. Then select Add2.

On the Domains page, select wwwjelecloud.com and select Verify. This will check if the CNAME record is correctly configured2.

Once the domain is verified, you can associate it with your Front Door endpoint. On the Domains page, select wwwjelecloud.com and select Associate endpoint. Then select your Front Door endpoint from the drop-down list and select Associate2.

Question: 253

SIMULATION

Task 6

You need to ensure that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address. The solution must minimize administrative effort when adding hosts to the subnet.

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that all hosts deployed to subnet3-2 connect to the internet by using the same static public IP address:
To use the same static public IP address for multiple hosts, you need to create a NAT gateway and associate it with subnet3-2. A NAT gateway is a resource that performs network address translation (NAT) for outbound traffic from a subnet1. It allows you to use a single public IP address for multiple private IP addresses2.
To create a NAT gateway, you need to go to the Azure portal and select Create a resource. Search for NAT gateway, select NAT gateway, then select Create3.
On the Create a NAT gateway page, enter or select the following information and accept the defaults for the remaining settings:
Subscription: Select your subscription name
Resource group: Select your resource group
Name: Type a unique name for your NAT gateway
Region: Select the same region as your virtual network
Public IP address: Select Create new and type a name for your public IP address. Select Standard as the SKU and Static as the assignment method4.
Select Review + create and then select Create to create your NAT gateway3.
To associate the NAT gateway with subnet3-2, you need to go to the Virtual networks service in the Azure portal and select your virtual network.
On the Virtual network page, select Subnets under Settings, and then select subnet3-2 from the list. On the Edit subnet page, under NAT gateway, select your NAT gateway from the drop-down list. Then select Save.

Question: 254

SIMULATION
Task 7
You need to ensure that hosts on VNET2 can access hosts on both VNET1 and VNET3. The solution must prevent hosts on VNET1 and VNET3 from communicating through VNET2.

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that hosts on VNET2 can access hosts on both VNET1 and VNET3, but hosts on VNET1 and VNET3 cannot communicate through VNET2: To connect different virtual networks in Azure, you need to use virtual network peering. Virtual network peering allows you to create low-latency, high-bandwidth connections between virtual networks without using gateways or the internet1.
To create a virtual network peering, you need to go to the Azure portal and select your virtual network. Then select Peerings under Settings and select + Add2.
On the Add peering page, enter or select the following information:
Name: Type a unique name for the peering from the source virtual network to the destination virtual network.
Virtual network deployment model: Select Resource manager.
Subscription: Select the subscription that contains the destination virtual network.
Virtual network: Select the destination virtual network from the list or enter its resource ID.
Name of the peering from [destination virtual network] to [source virtual network]: Type a unique name for the

peering from the destination virtual network to the source virtual network.

Configure virtual network access settings: Select Enabled to allow resources in both virtual networks to communicate with each other.

Allow forwarded traffic: Select Disabled to prevent traffic that originates from outside either of the peered virtual networks from being forwarded through either of them.

Allow gateway transit: Select Disabled to prevent either of the peered virtual networks from using a gateway in the other virtual network.

Use remote gateways: Select Disabled to prevent either of the peered virtual networks from using a gateway in the other virtual network as a transit point to another network.

Select Add to create the peering2.

Repeat the previous steps to create peerings between VNET2 and VNET1, and between VNET2 and VNET3. This will allow hosts on VNET2 to access hosts on both VNET1 and VNET3.

To prevent hosts on VNET1 and VNET3 from communicating through VNET2, you need to use network security groups (NSGs) to filter traffic between subnets. NSGs are rules that allow or deny inbound or outbound traffic based on source or destination IP address, port, or protocol3.

To create an NSG, you need to go to the Azure portal and select Create a resource. Search for network security group and select Network security group. Then select Create4.

On the Create a network security group page, enter or select the following information: Subscription: Select your subscription name.

Resource group: Select your resource group name.

Name: Type a unique name for your NSG.

Region: Select the same region as your virtual networks.

Select Review + create and then select Create to create your NSG4.

To add rules to your NSG, you need to go to the Network security groups service in the Azure portal and select your NSG. Then select Inbound security rules or Outbound security rules under Settings and select + Add4.

On the Add inbound security rule page or Add outbound security rule page, enter or select the following information:

Source or Destination: Select CIDR block.

Source CIDR blocks or Destination CIDR blocks: Enter the IP address range of the source or destination subnet that you want to filter. For example, 10.0.1.0/24 for VNET1 subnet 1, 10.0.2.0/24 for VNET2 subnet 1, and 10.0.3.0/24 for VNET3 subnet 1.

Protocol: Select Any to apply the rule to any protocol.

Action: Select Deny to block traffic from or to the source or destination subnet.

Priority: Enter a number between 100 and 4096 that indicates the order of evaluation for this rule.

Lower numbers have higher priority than higher numbers.

Name: Type a unique name for your rule.

Select Add to create your rule4.

Repeat the previous steps to create inbound and outbound rules for your NSG that deny traffic between VNET1 and VNET3 subnets. For example, you can create an inbound rule that denies traffic from 10.0.1.0/24 (VNET1 subnet 1) to 10.0.3.0/24 (VNET3 subnet 1), and an outbound rule that denies traffic from 10.0.3.0/24 (VNET3 subnet 1) to 10.0.1.0/24 (VNET1 subnet 1).

To associate your NSG with a subnet, you need to go to the Virtual networks service in the Azure portal and select your virtual network. Then select Subnets under Settings and select the subnet that you want to associate with your NSG5.

On the Edit subnet page, under Network security group, select your NSG from the drop-down list. Then select Save5.

Repeat the previous steps to associate your NSG with the subnets in VNET1 and VNET3 that you want to isolate

from each other.

Question: 255

SIMULATION

Task 8

You need to ensure that the storage34280945 storage account will only accept connections from hosts on VNET1

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that the storage34280945 storage account will only accept connections from hosts on VNET1:

To restrict network access to your storage account, you need to configure the Azure Storage firewall and virtual network settings for your storage account. You can do this in the Azure portal by selecting your storage account and then selecting Networking under Settings1.

On the Networking page, select Firewalls and virtual networks, and then select Selected networks under Allow access from1. This will block all access to your storage account except from the networks or resources that you specify.

Under Virtual networks, select + Add existing virtual network. Then select VNET1 from the list of virtual networks and select the subnet that contains the hosts that you want to allow access to your storage account1. This will enable a service endpoint for Storage in the subnet and configure a virtual network rule for that subnet through the Azure storage firewall2.

Select Add to add the virtual network and subnet to your storage account1.

Select Save to apply your changes1.

Question: 256

SIMULATION

Task 9

You need to ensure that subnet4-3 can accommodate 507 hosts.

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for ensuring that subnet4-3 can accommodate 507 hosts:

To determine the subnet size that can accommodate 507 hosts, you need to use the formula: number of hosts = 2^(32 - n) - 2, where n is the number of bits in the subnet mask1. You need to find the value of

n that satisfies this equation for 507 hosts.

To solve this equation, you can use trial and error or a binary search method. For example, you can start with n = 24, which is the default subnet mask for Class C networks. Then, plug in the value of n into the formula and see if it is too big or too small for 507 hosts.

If you try n = 24, you get number of hosts = 2^(32 - 24) - 2 = 254, which is too small. You need to increase the value of n to get a larger number of hosts.

If you try n = 25, you get number of hosts = 2^(32 - 25) - 2 = 510, which is just enough to accommodate 507 hosts. You can stop here or try a smaller value of n to see if it still works.

If you try n = 26, you get number of hosts = 2^(32 - 26) - 2 = 254, which is too small again. You need to decrease the value of n to get a larger number of hosts.

Therefore, the smallest value of n that can accommodate 507 hosts is n = 25. This means that the subnet mask for subnet4-3 should be /25 or 255.255.255.128 in dot-decimal notation1.

To change the subnet mask for subnet4-3, you need to go to the Azure portal and select your virtual network. Then select Subnets under Settings and select subnet4-3 from the list2.

On the Edit subnet page, under Address range (CIDR block), change the value from /24 to /25. Then select Save2.

Question: 257

SIMULATION

Task 10

You need to configure VNET1 to log all events and metrics. The solution must ensure that you can query the events and metrics directly from the Azure portal by using KQL.

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for configuring VNET1 to log all events and metrics and query them by using KQL:

To enable logging for VNET1, you need to create a diagnostic setting that collects the platform metrics and logs from the virtual network and routes them to one or more destinations. You can choose to send the data to a Log Analytics workspace, a storage account, an event hub, or a partner solution1.

To create a diagnostic setting, you need to go to the Azure portal and select your virtual network. Then select Diagnostic settings under Monitoring and select + Add diagnostic setting1. On the Add diagnostic setting page, enter or select the following information: Diagnostic setting name: Type a unique name for your diagnostic setting.

Destination details: Select the destination where you want to send the dat

a. For example, you can select Send to Log Analytics workspace and choose your workspace from the list.

Log: Select the categories of logs that you want to collect. For VNET1, you can select NetworkSecurityGroupEvent and NetworkSecurityGroupRuleCounter as the log categories2.

Metric: Select AllMetrics to collect all the platform metrics for VNET12.

Select Save to create your diagnostic setting1.

To query the events and metrics from the Azure portal by using KQL, you need to go to the Log

Analytics workspace that you selected as the destination. Then select Logs under General and enter your KQL query in the query editor3.

For example, you can use the following KQL query to get the top 10 network security group events for VNET1 in the last 24 hours:

```
NetworkSecurityGroupEvent
| where TimeGenerated > ago(24h)
| where ResourceId contains "VNET1"
| summarize count() by EventID
| top 10 by count_
```

Copy

Select Run to execute your query and view the results in a table or a chart3.

Question: 258

SIMULATION

Task 11

You are preparing to connect your on-premises network to VNET4 by using a Site-to-Site VPN. The on-premises endpoint of the VPN will be created on a firewall named Firewall 1.

The on-premises network has the following configurations:

- Internal address range: 10.10.0.0/16.
- Firewall 1 internal IP address: 10.10.1.1.
- Firewall1 public IP address: 131.107.50.60.

BGP is NOT used.

You need to create the object that will provide the IP addressing configuration of the on-premises network to the Site-to-Site VPN. You do NOT need to create a virtual network gateway to complete this task.

Answer: See the Explanation below for step by step instructions.

Explanation:

Here are the steps and explanations for creating the object that will provide the IP addressing configuration of the on-premises network to the Site-to-Site VPN:

The object that you need to create is called a local network gateway. A local network gateway represents your on-premises network and VPN device in Azure. It contains the public IP address of your VPN device and the address prefixes of your on-premises network that you want to connect to the Azure virtual network1.

To create a local network gateway, you need to go to the Azure portal and select Create a resource. Search for local network gateway, select Local network gateway, then select Create2.

On the Create local network gateway page, enter or select the following information and accept the defaults for the remaining settings:

Name: Type a unique name for your local network gateway.

IP address: Type the public IP address of your VPN device, which is 131.107.50.60 in this case.

Address space: Type the internal address range of your on-premises network, which is 10.10.0.0/16 in this case.

Subscription: Select your subscription name.
Resource group: Select your resource group name.
Location: Select the same region as your virtual network.
Select Review + create and then select Create to create your local network gateway2.

Question: 259

SIMULATION

Task 1
You need to ensure that virtual machines on VNET1 and VNET2 are included automatically in a DNS zone named contoso.azure. The solution must ensure that the virtual machines on VNET1 and VNET2 can resolve the names of the virtual machines on either virtual network.

Answer: See the Explanation below for step by step instructions.

Explanation:

To achieve the task of ensuring that virtual machines on VNET1 and VNET2 are included automatically in a DNS zone named contoso.azure, and that they can resolve the names of the virtual machines on either virtual network, you can follow these steps:

Step-by-Step Solution
Step 1: Create a Private DNS Zone
Navigate to the Azure Portal.
Search for “Private DNS zones” in the search bar and select it.
Click on “Create”.
Enter the DNS zone name as contoso.azure.
Select the appropriate subscription and resource group.
Click on “Review + create” and then “Create”.
Step 2: Link VNET1 and VNET2 to the DNS Zone
Go to the newly created DNS zone (contoso.azure).
Select “Virtual network links” from the left-hand menu.
Click on “Add”.
Enter a name for the link (e.g., VNET1-link).
Select the subscription and virtual network (VNET1).
Enable auto-registration to ensure that VMs are automatically registered in the DNS zone.
Click on “OK”.
Repeat the process for VNET2.
Step 3: Configure DNS Settings for VNET1 and VNET2
Navigate to VNET1 in the Azure Portal.
Select “DNS servers” under the “Settings” section.
Ensure that the DNS server is set to “Default (Azure-provided)”.
Repeat the process for VNET2.
Step 4: Verify Name Resolution
Deploy a virtual machine in VNET1 and another in VNET2.

Connect to the virtual machines using Remote Desktop Protocol (RDP) or Secure Shell (SSH).
Test name resolution by pinging the VM in VNET2 from the VM in VNET1 using its hostname (e.g., ping <VM-name>.contoso.azure).

Explanation

Private DNS Zone: This allows you to manage and resolve domain names in a private network without exposing them to the public internet.
Virtual Network Links: Linking VNET1 and VNET2 to the DNS zone ensures that VMs in these networks can register their DNS records automatically.
Auto-registration: This feature automatically registers the DNS records of VMs in the linked virtual networks, simplifying management.
DNS Settings: Using Azure-provided DNS ensures that the VMs can resolve each other's names without additional configuration.
By following these steps, you ensure that virtual machines on VNET1 and VNET2 are included automatically in the DNS zone contoso.azure and can resolve each other's names seamlessly.

Question: 260

SIMULATION
Task 2
You need to ensure that you can deploy Azure virtual machines to the France Central Azure region.
The solution must ensure that virtual machines in the France Central region are in a network segment that has an IP address range of 10.5.1.0/24.

Answer: See the Explanation below for step by step instructions.

Explanation:

To deploy Azure virtual machines to the France Central region and ensure they are in a network segment with an IP address range of 10.5.1.0/24, follow these steps: Step-by-Step Solution
Step 1: Create a Virtual Network in France Central
Navigate to the Azure Portal.
Search for "Virtual networks" in the search bar and select it.
Click on "Create".
Enter the following details:
Subscription: Select your subscription.
Resource Group: Select an existing resource group or create a new one.
Name: Enter a name for the virtual network (e.g., VNet-FranceCentral).
Region: Select France Central.
Click on "Next: IP Addresses".
Step 2: Configure the Address Space and Subnet
In the IP Addresses tab, enter the address space as 10.5.1.0/24.
Click on "Add subnet".
Enter the following details:
Subnet name: Enter a name for the subnet (e.g., Subnet-1).
Subnet address range: Enter 10.5.1.0/24.
Click on "Add".

Click on “Review + create” and then “Create”.

Step 3: Deploy Virtual Machines to the Virtual Network

Navigate to the Azure Portal.

Search for “Virtual machines” in the search bar and select it.

Click on “Create” and then “Azure virtual machine”.

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select the same resource group used for the virtual network.

Virtual machine name: Enter a name for the VM.

Region: Select France Central.

Image: Select the desired OS image.

Size: Select the appropriate VM size.

Click on “Next: Disks”, configure the disks as needed, and then click on “Next: Networking”.

In the Networking tab, select the virtual network (VNet-FranceCentral) and subnet (Subnet-1) created earlier.

Complete the remaining configuration steps and click on “Review + create” and then “Create”. Explanation

Virtual Network: A virtual network in Azure allows you to create a logically isolated network that can host your Azure resources.

Address Space: The address space 10.5.1.0/24 ensures that the VMs are in a specific network segment.

Subnet: Subnets allow you to segment the virtual network into smaller, manageable sections. Region: Deploying the virtual network and VMs in the France Central region ensures that the resources are physically located in that region.

By following these steps, you can ensure that your Azure virtual machines in the France Central region are deployed within the specified IP address range of 10.5.1.0/24.

Question: 261

SIMULATION

Task 3

You need to ensure that hosts on VNET1 and VNET2 can communicate. The solution must minimize latency between the virtual networks.

Answer: See the Explanation below for step by step instructions.

Explanation:

To ensure that hosts on VNET1 and VNET2 can communicate with minimal latency, you can use Virtual Network Peering. This method connects the two virtual networks directly through the Microsoft backbone network, ensuring low-latency and high-bandwidth communication.

Step-by-Step Solution

Step 1: Set Up Virtual Network Peering

Navigate to the Azure Portal.

Search for “Virtual networks” and select VNET1.

In the left-hand menu, select “Peerings” under the “Settings” section.

Click on “Add” to create a new peering.

Enter the following details:

Name: Enter a name for the peering (e.g., VNET1-to-VNET2).

Peer virtual network: Select VNET2.
Allow virtual network access: Ensure this is enabled.
Allow forwarded traffic: Enable if needed.
Allow gateway transit: Enable if needed.
Click on “Add”.
Step 2: Configure Peering on VNET2
Navigate to VNET2 in the Azure Portal.
In the left-hand menu, select “Peerings” under the “Settings” section.
Click on “Add” to create a new peering.
Enter the following details:
Name: Enter a name for the peering (e.g., VNET2-to-VNET1).
Peer virtual network: Select VNET1.
Allow virtual network access: Ensure this is enabled.
Allow forwarded traffic: Enable if needed.
Allow gateway transit: Enable if needed.
Click on “Add”.
Explanation
Virtual Network Peering: This feature connects two virtual networks in the same or different regions, allowing resources in both networks to communicate with each other as if they were part of the same network. The traffic between peered virtual networks uses the Microsoft backbone infrastructure, ensuring low latency and high bandwidth12.
Allow Virtual Network Access: This setting ensures that the virtual networks can communicate with each other.
Allow Forwarded Traffic: This setting allows traffic forwarded from a network security appliance in the peered virtual network.
Allow Gateway Transit: This setting allows the peered virtual network to use the gateway in the local virtual network.
By following these steps, you can ensure that hosts on VNET1 and VNET2 can communicate with minimal latency, leveraging the high-speed Microsoft backbone network.

Question: 262

SIMULATION
Task 4
You need to ensure that the owner of VNET3 receives an alert if an administrative operation is performed on the virtual network.

Answer: See the Explanation below for step by step instructions.

Explanation:

To ensure that the owner of VNET3 receives an alert whenever an administrative operation is performed on the virtual network, you can set up an Activity Log Alert in Azure Monitor. Here’s how you can do it: Step-by-Step Solution
Step 1: Create an Activity Log Alert Navigate to the Azure Portal.
Search for “Monitor” and select it.
In the Monitor blade, select “Alerts” from the left-hand menu.

Click on “New alert rule”.
Step 2: Configure the Alert Rule
Select the Scope:
Click on “Select resource”.
Choose “Virtual Network” as the resource type.
Select VNET3 from the list of virtual networks.
Define the Condition:
Click on “Add condition”.
In the “Signal type” dropdown, select “Activity Log”.
Choose “Administrative” as the category.
Select the specific operations you want to monitor
(e.g., Microsoft.Network/virtualNetworks/write for any write operations on the virtual network).
Set the Alert Details:
Enter a name for the alert rule (e.g., VNET3 Admin Operations Alert).
Provide a description if needed.
Configure the Action Group:
Click on “Add action group”.
Enter a name for the action group.
Select the action type (e.g., Email/SMS/Push/Voice).
Enter the details of the recipient (e.g., the email address of the owner of VNET3).
Review and Create:
Review the alert rule settings.
Click on “Create alert rule”.
Explanation
Activity Log Alerts: These alerts notify you when specific operations are performed on your Azure resources. By setting up an alert for administrative operations, you ensure that any changes to VNET3 are promptly reported.
Action Groups: These define the actions to take when an alert is triggered. You can configure notifications via email, SMS, or other methods to ensure the owner of VNET3 is informed immediately.
Administrative Operations: Monitoring these operations helps in tracking changes and maintaining the security and integrity of your virtual network.
By following these steps, you can ensure that the owner of VNET3 receives timely alerts for any administrative operations performed on the virtual network, helping to maintain oversight and security.

Question: 263

SIMULATION
Task 5
You need to archive all the metrics of VNET1 to an existing storage account.

Answer: See the Explanation below for step by step instructions.

Explanation:

To archive all the metrics of VNET1 to an existing storage account, you can use Azure Monitor’s diagnostic settings. Here’s how you can do it: Step-by-Step Solution

Step 1: Navigate to VNET1 in the Azure Portal

Open the Azure Portal.

Search for "Virtual networks" and select VNET1 from the list.

Step 2: Configure Diagnostic Settings

In the VNET1 blade, select "Diagnostic settings" under the "Monitoring" section.

Click on "Add diagnostic setting".

Step 3: Set Up the Diagnostic Setting

Enter a name for the diagnostic setting (e.g., VNET1-Metrics-Archive).

Select the metrics you want to archive. You can choose from various metrics like TotalBytesReceived, TotalBytesSent, etc.

Under "Destination details", select "Archive to a storage account".

Choose the existing storage account where you want to archive the metrics.

Configure the retention period if needed.

Step 4: Save the Configuration

Review your settings to ensure everything is correct.

Click on "Save" to apply the diagnostic setting.

Explanation

Diagnostic Settings: These allow you to collect and route metrics and logs from your Azure resources to various destinations, including storage accounts, Log Analytics workspaces, and Event Hubs.

Metrics: Metrics provide numerical data about the performance and health of your resources.

Archiving these metrics helps in long-term analysis and compliance.

Storage Account: Using an existing storage account ensures that the metrics are stored securely and can be accessed for future analysis.

By following these steps, you can ensure that all the metrics of VNET1 are archived to your existing storage account, enabling you to monitor and analyze the performance and health of your virtual network over time.

Question: 264

SIMULATION

Task 6

You have two servers that are each hosted by a separate service provider in New York and Germany.

The server hosted in New York is accessible by using a host name of ny.contoso.com. The server hosted in Germany is accessible by using a host name of de.contoso.com.

You need to provide a single host name to access both servers. The solution must ensure that traffic originating from Germany is routed to de contoso.com. All other traffic must be routed to ny.contoso.com.

Answer: See the Explanation below for step by step instructions.

Explanation:

To provide a single host name that routes traffic based on the origin, you can use Azure Traffic Manager. This service allows you to route traffic to different endpoints based on various routing methods, including geographic routing.

Step-by-Step Solution

Step 1: Create a Traffic Manager Profile

Navigate to the Azure Portal.
Search for “Traffic Manager profiles” and select it.
Click on “Create”.
Enter the following details:
Name: Enter a name for the Traffic Manager profile (e.g., ContosoTrafficManager).
Routing method: Select Geographic.
Subscription: Select your subscription.
Resource group: Select an existing resource group or create a new one.
Resource group location: Choose a location (this does not affect the routing).
Click on “Create”.
Step 2: Configure Endpoints
Navigate to the newly created Traffic Manager profile.
Select “Endpoints” from the left-hand menu.
Click on “Add” to add a new endpoint.
Enter the following details:
Type: Select External endpoint.
Name: Enter a name for the endpoint (e.g., NewYorkEndpoint).
FQDN: Enter ny.contoso.com.
Geographic region: Select “World” (this will be adjusted later).
Click on “Add” to save the endpoint.
Repeat the process to add the second endpoint:
Type: Select External endpoint.
Name: Enter a name for the endpoint (e.g., GermanyEndpoint).
FQDN: Enter de.contoso.com.
Geographic region: Select Europe.
Step 3: Adjust Geographic Routing
Navigate to the Traffic Manager profile.
Select “Configuration” from the left-hand menu.
Under “Geographic routing”, adjust the regions:
For the GermanyEndpoint, ensure that the geographic region is set to Europe.
For the NewYorkEndpoint, ensure that the geographic region is set to World (excluding Europe).
Step 4: Test the Configuration
Use a DNS query tool to test the routing.
From a location in Germany, query the Traffic Manager profile’s DNS name and ensure it resolves to de.contoso.com.
From a location outside Europe, query the Traffic Manager profile’s DNS name and ensure it resolves to ny.contoso.com.
Explanation
Azure Traffic Manager: This service uses DNS to direct client requests to the most appropriate endpoint based on the routing method you choose. Geographic routing ensures that traffic is directed based on the origin of the request.
Geographic Routing: This method allows you to route traffic based on the geographic location of the DNS query origin, ensuring that users are directed to the nearest or most appropriate endpoint.
By following these steps, you can provide a single host name that routes traffic to de.contoso.com for users in Germany and to ny.contoso.com for users from other locations, ensuring efficient and appropriate traffic management.

Question: 265

SIMULATION

Task 7

You plan to deploy 100 virtual machines to subnet4-1. The virtual machines will NOT be assigned a public IP address. The virtual machines will call the same API. which is hosted by a third party. The virtual machines will make more than 10,000 calls per minute to the API.

You need to minimize the risk of SNAT port exhaustion. The solution must minimize administrative effort.

Answer: See the Explanation below for step by step instructions.

Explanation:

To minimize the risk of SNAT port exhaustion for your 100 virtual machines in subnet4-1, while ensuring minimal administrative effort, you can use an Azure NAT Gateway. This service provides scalable and resilient outbound connectivity for virtual networks, dynamically allocating SNAT ports to avoid exhaustion.

Step-by-Step Solution

Step 1: Create a NAT Gateway

Navigate to the Azure Portal.

Search for “NAT gateways” and select it.

Click on “Create”.

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select an existing resource group or create a new one.

Name: Enter a name for the NAT gateway (e.g., NATGateway-Subnet4-1).

Region: Select the region where your virtual network is located.

Click on “Next: Outbound IP”.

Step 2: Configure Outbound IP Addresses

Choose whether to use existing public IP addresses or create new ones.

If creating new ones, click on “Add new” and configure the new public IP addresses.

Click on “Next: Subnet”.

Step 3: Associate the NAT Gateway with Subnet4-1

Click on “Associate subnet”.

Select the virtual network that contains subnet4-1.

Select subnet4-1 from the list of subnets.

Click on “OK”.

Step 4: Review and Create

Review your settings to ensure everything is correct.

Click on “Review + create” and then “Create”.

Explanation

Azure NAT Gateway: This service provides outbound connectivity for virtual networks, dynamically allocating SNAT ports across all VM instances within a subnet. This dynamic allocation helps prevent SNAT port exhaustion, especially in scenarios with high outbound connection volumes12.

Dynamic SNAT Port Allocation: Unlike static allocation methods, NAT Gateway dynamically allocates SNAT ports based on demand, ensuring efficient use of available ports and reducing the risk of exhaustion2.

By following these steps, you can ensure that your 100 virtual machines in subnet4-1 can make the necessary API calls without running into SNAT port exhaustion, all while minimizing administrative effort.

Question: 266

SIMULATION

Task 8

You plan to deploy an appliance to subnet3-2- The appliance will perform packet inspection and will have an IP address of 10.3.2.100.

You need to ensure that all traffic to the internet from subnet3-1 is forwarded to the appliance for inspection.

Answer: See the Explanation below for step by step instructions.

Explanation:

To ensure that all traffic to the internet from subnet3-1 is forwarded to the appliance in subnet3-2 for packet inspection, you can use User-Defined Routes (UDRs) to direct the traffic. Here's how you can do it:

Step-by-Step Solution

Step 1: Create a Route Table

Navigate to the Azure Portal.

Search for "Route tables" and select it.

Click on "Create".

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select an existing resource group or create a new one.

Name: Enter a name for the route table (e.g., RouteTable-Subnet3-1).

Region: Select the region where your virtual network is located.

Click on "Review + create" and then "Create".

Step 2: Add a Route to the Route Table

Navigate to the newly created route table.

Select "Routes" from the left-hand menu.

Click on "Add" to create a new route.

Enter the following details:

Route name: Enter a name for the route (e.g., RouteToAppliance).

Address prefix: Enter 0.0.0.0/0 to route all internet traffic.

Next hop type: Select Virtual appliance.

Next hop address: Enter the IP address of the appliance (10.3.2.100).

Click on "OK" to add the route.

Step 3: Associate the Route Table with Subnet3-1

Navigate to the route table.

Select "Subnets" from the left-hand menu.

Click on "Associate".

Select the virtual network that contains subnet3-1.

Select subnet3-1 from the list of subnets.

Click on "OK".

Explanation

User-Defined Routes (UDRs): These allow you to control the routing of traffic within your virtual network. By defining a route that directs all internet-bound traffic to the appliance, you ensure that the traffic is inspected before it reaches the internet1.

Virtual Appliance: This is a network appliance that performs specific functions, such as packet inspection, and is treated as a next hop in the routing table2.

Route Table Association: Associating the route table with subnet3-1 ensures that all traffic from this subnet follows the defined routes.

By following these steps, you can ensure that all internet-bound traffic from subnet3-1 is forwarded to the appliance in subnet3-2 for inspection, thereby enhancing your network security.

Question: 267

SIMULATION

Task 9

You plan to use VNET4 for an Azure API Management implementation.

You need to configure a policy that can be used by an Azure application gateway to protect against known web attack vectors. The policy must only allow requests that originate from IP addresses in Canad
a. You do NOT need to create the application gateway to complete this task.

Answer: See the Explanation below for step by step instructions.

Explanation:

To configure a policy in Azure API Management that can be used by an Azure Application Gateway to protect against known web attack vectors and only allow requests from IP addresses in Canada, follow these steps:

Step-by-Step Solution

Step 1: Create or Access Your API Management Instance

Navigate to the Azure Portal.

Search for “API Management services” and select your API Management instance.

Step 2: Configure the Policy

In the API Management instance, go to the “APIs” section.

Select the API you want to apply the policy to.

Go to the “Design” tab.

Select “All operations” if you want to apply the policy to all operations, or select a specific operation. Step 3: Add the Inbound Policy

In the Inbound processing section, click on “+ Add policy”.

Select “IP filter” from the list of policies.

Add the IP address ranges for Canada. You can find the IP ranges for Canada from a reliable source or use a service that provides this information.

Here is an example of the XML configuration for the policy:

<inbound>

```
    <ip-filter action="allow">
      <address-range from="24.0.0.0" to="24.255.255.255" />
      <address-range from="47.0.0.0" to="47.255.255.255" />
      <!-- Add other Canadian IP ranges as needed -->
    </ip-filter>
    <ip-filter action="deny">
      <address-range from="0.0.0.0" to="255.255.255.255" />
    </ip-filter>
</inbound>
```

Save the policy to apply the changes.

Explanation

IP Filter Policy: This policy allows you to filter incoming requests based on their IP addresses. By specifying the IP ranges for Canada, you ensure that only requests originating from these IPs are allowed.

Inbound Processing: Applying the policy in the inbound section ensures that the requests are filtered before they reach your API.

By following these steps, you can configure a policy in Azure API Management that restricts access to your API to only those requests originating from IP addresses in Canada, thereby enhancing security and compliance

Question: 268

SIMULATION

Task 10

You plan to deploy several virtual machines to subnet1-2.

You need to prevent all Azure hosts outside of subnetI-2 from connecting to TCP port 5585 on hosts on subnet1-2. The solution must minimize administrative effort.

Answer: See the Explanation below for step by step instructions.

Explanation:

To prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts within subnet1-2, you can use a Network Security Group (NSG). This solution is straightforward and minimizes administrative effort.

Step-by-Step Solution

Step 1: Create a Network Security Group (NSG)

Navigate to the Azure Portal.

Search for “Network security groups” and select it.

Click on “Create”.

Enter the following details:

Subscription: Select your subscription.

Resource Group: Select an existing resource group or create a new one.

Name: Enter a name for the NSG (e.g., NSG-Subnet1-2).

Region: Select the region where your virtual network is located.

Click on “Review + create” and then “Create”.

Step 2: Create an Inbound Security Rule

Navigate to the newly created NSG.

Select “Inbound security rules” from the left-hand menu.

Click on “Add” to create a new rule.

Enter the following details:

Source: Select Service Tag.

Source Service Tag: Select VirtualNetwork.

Source port ranges: Leave as *.

Destination: Select IP Addresses.

Destination IP addresses/CIDR ranges: Enter the IP range of subnet1-2 (e.g., 10.1.2.0/24).

Destination port ranges: Enter 5585.

Protocol: Select TCP.

Action: Select Deny.

Priority: Enter a priority value (e.g., 100).

Name: Enter a name for the rule (e.g., Deny-TCP-5585).

Click on “Add” to create the rule.

Step 3: Associate the NSG with Subnet1-2

Navigate to the virtual network that contains subnet1-2.

Select “Subnets” from the left-hand menu.

Select subnet1-2 from the list of subnets.

Click on “Network security group”.

Select the NSG you created (NSG-Subnet1-2).

Click on “Save”.

Explanation

Network Security Group (NSG): NSGs are used to filter network traffic to and from Azure resources in an Azure virtual network. They contain security rules that allow or deny inbound and outbound traffic based on source and destination IP addresses, port, and protocol1.

Inbound Security Rule: By creating a rule that denies traffic on TCP port 5585 from any source outside of subnet1-2, you ensure that only hosts within subnet1-2 can connect to this port.

Association with Subnet: Associating the NSG with subnet1-2 ensures that the security rules are applied to all resources within this subnet.

By following these steps, you can effectively prevent all Azure hosts outside of subnet1-2 from connecting to TCP port 5585 on hosts within subnet1-2, while minimizing administrative effort.

Question: 269

SIMULATION

Task 11

You need to ensure that only hosts on VNET1 can access the slcnage42150372 storage account. The solution must ensure that access occurs over the Azure backbone network.

Answer: See the Explanation below for step by step instructions.

Explanation:

To ensure that only hosts on VNET1 can access the slcnage42150372 storage account and that access occurs over the Azure backbone network, you can use Azure Private Endpoints. This method secures the connection by assigning a private IP address from your virtual network to the storage account, ensuring that traffic does not traverse the public internet.

Step-by-Step Solution

Step 1: Create a Private Endpoint for the Storage Account

Navigate to the Azure Portal.

Search for "Storage accounts" and select the slcnage42150372 storage account.

In the storage account blade, select "Networking" under the "Security + networking" section.

Under "Private endpoint connections", click on "Add private endpoint".

Enter the following details:

Name: Enter a name for the private endpoint (e.g., PrivateEndpoint-VNET1).

Region: Select the same region as your virtual network (VNET1).

Click on "Next: Resource".

Step 2: Configure the Resource

Select "Target sub-resource": Choose the storage service you want to connect to (e.g., blob, file, queue, table).

Click on "Next: Virtual network".

Step 3: Select the Virtual Network and Subnet

Select the virtual network: Choose VNET1.

Select the subnet: Choose the appropriate subnet within VNET1.

Click on "Next: Configuration".

Step 4: Configure DNS Integration (Optional)

Configure DNS settings if needed to ensure proper name resolution within your virtual network.

Click on "Next: Tags", add any tags if necessary, and then click on "Review + create".

Review your settings and click on "Create".

Step 5: Restrict Public Network Access

Navigate back to the storage account.

Select "Networking" under the "Security + networking" section.

Under "Firewalls and virtual networks", select "Selected networks".

Ensure that only VNET1 is listed under the virtual networks section.

Click on "Save".

Explanation

Private Endpoints: These provide secure connectivity to Azure services by assigning a private IP address from your VNet to the service, ensuring that traffic stays within the Azure backbone network12.

Firewall and Virtual Networks: Configuring the storage account to allow access only from selected networks (VNET1) ensures that no other network can access the storage account3.

By following these steps, you can ensure that only hosts on VNET1 can access the slcnage42150372 storage account, and that all access occurs over the secure Azure backbone network.

Question: 270

Your on-premises network contains a DNS server named Server 1.

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNetl	Virtual network	*None*
VM1	Virtual machine	Connected to VNet! Connected to storage 1 by using a private endpoint
storage 1	Storage account	*None*

The on-premises network is connected to VNet1 by using a Site-to-Site (S2S) VPN.

You need to ensure that Server1 can resolve the DNS name of storage1. The solution must minimize costs and administrative effort.

What should you use?

A. an Azure Private DNS zone
B. an Azure virtual machine that hosts a DNS service
C. an Azure public DNS zone
D. Azure DNS Private Resolver

Answer: D

Explanation:

Question: 271

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
Vnetl	Virtual network	*None*
Subnet!	subnet	Hosted in Vnet!
Subnet?	subnet	Hosted in Vnetl
GatewaySubnet	subnet	Hosted in Vnet!
VM!	Virtual machine	Connected to Subnet! Basic SKU public IP address
VM2	Virtual machine	Connected to Subnet? Standard SKU public IP address

You plan to deploy an Azure Virtual Network NAT gateway named Gateway 1. The solution must meet the following requirements:

- VM1 will access the internet by using its public IP address.
- VM2 will access the internet by using its public IP address.
- Administrative effort must be minimized.

You need to ensure that you can deploy Gateway1 to Vnet1.

What is the minimal number of subnets that Vnet1 must have?

A. 2
B. 3
C. 4
D. 5

Answer: C

Explanation:

Question: 272

Your company has 40 branch offices that are linked by using a Software-Defined Wide Area Network (SD-WAN). The SD-WAN uses
BGP.
You have an Azure subscription that contains 20 virtual networks configured as a hub and spoke topology. The topology contains a hub virtual network named Vnetl.
The virtual networks connect to the SD-WAN by using a network virtual appliance (NVA) in Vnetl.
You need to ensure that BGP route advertisements will propagate between the virtual networks and the SD-WAN. The solution must minimize administrative effort
What should you implement?

A. An Azure VPN Gateway that has BGP enabled
B. a NAT gateway
C. Azure Traffic Manager
D. Azure Route Server

Answer: D

Explanation:

Question: 273

You have an Azure virtual machine named VM1.
You need to capture all the network traffic of VM1 by using Azure Network Watcher. To which locations can the capture be written?

A. a file path on VM1 only
B. General purpose v2 standard only
C. a Block blob premium account only
D. General purpose v2 standard and a file path on VM1 only
E. General purpose v2 standard and a Block blob premium account only
F. blob storage, a file path on VM1, and a Block blob premium account

Answer: D

Explanation:

Question: 274

You have an Azure subscription that contains a resource group named RG1 and a virtual network named VNet1 You need to deploy Azure Firewall to RG1. The solution must minimize administrative effort What should you do first?

A. Create a secured virtual hub named AzureFirewallHub.
B. Create a new resource group named AzureFirewallResourceGroup.
C. Create a new virtual network named AzureFirewallNetwork.
D. On VNet1, create a virtual subnet named AzureFirewallSubnet.

Answer: D

Explanation:

Question: 275

You have an Azure subscription that contains a virtual machine named VM1 and a network security group (NSG) named NSG1. NSG1 has the default rules configured VM1 runs Windows Server and contains a single NIC named NIC1 NIC! is associated with NSG1.
You need to prevent access to the Azure Instance Metadata Service (IMDS) REST API on VM1 The solution must minimize administrative effort.
What should you add to NSG1?

A. an outbound rule that blocks traffic to an IP address
B. an outbound rule that blocks traffic to a service tag
C. an inbound and outbound rule that blocks traffic to an application security group.
D. an inbound rule that blocks traffic to an IP address

Answer: B

Explanation:

Question: 276

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
NSG1	Network security group (NSG)
VMI	Virtual machine
VM2	Virtual machine

NSG1 is associated to the NIC of VM1 and contains the rules shown in the following table.

Name	Priority	Direction	Protocol	Action
Rulel	100	Inbound	RDP	Allow
Rule2	101	Inbound	SSH	Allow

You collect NSG flow logs for five minutes for the following activities:

- Two RDP sessions from VM1 to VM2, each initiated from a different TCP port
- Three SSH sessions from VM2 to VM1, each initiated from a different TCP port

You analyze the logs by using Traffic Analytics in Azure Network Watcher. How many aggregated flow entries will Traffic Analytics identify?

A. 1
B. 2
C. 5
D. 10

Answer: B

Explanation:

Question: 277

You have an Azure subscription that contains an ExpressRoute Standard gateway named GW1.
You need to upgrade GW1 to support ExpressRoute FastPath. The solution must minimize downtime. Which SKU should you use?

A. ErGw3AZ
B. ErGw2AZ
C. High performance
D. Ultra performance

Answer: D

Explanation:

Question: 278

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:

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

Which gateway SKU should you specify?

A. VpnGwIAZ
B. VpnGw2AZ
C. VpnGw4AZ

D. VpnGwSAZ

Answer: C

Explanation:

Question: 279

HOTSPOT

You have an on-premises network and an Azure virtual network named VNet1.

You need to implement Azure Extended Network. The solution must minimize costs.

Which type of virtual machine should you deploy to VNet1, and which tool should you use to configure Azure Extended Network? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Virtual machine
- Windows Server 2019 Datacenter with Containers
- **Windows Server 2022 Datacenter Azure Edition**
- Windows Server 2022 Datacenter Server Core

Tool
- The Azure portal
- The Routing and Remote Access service
- Server Manager
- **Windows Admin Center**

Answer:

Explanation:

Answer Area

Virtual machine: Windows Server 2022 Datacenter. Azure Edition

Tool Windows Admin Center

Question: 280

HOTSPOT

Your on-premises network uses an IP address range of 10.1.0.0 to 10.1.255.255.

You plan to deploy a new Azure virtual network solution that will include the following elements:

- A virtual network named VNet1
- A Site-to-Site (S2S) VPN connection between VNet1 and the on-premises network
- GatewaySubnet in VNet1, which will be used as a route-based virtual network gateway

You need to recommend which subnet masks to assign to VNet1 and GatewaySubnet. The solution must meet the following requirements:

- Maximize the number of available IP addresses on VNet1.
- Minimize the number of available IP addresses on GatewaySubnet

Which address spaces should you assign to VNet1 and GatewaySubnet? To answer, select the

appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

VNetl 10.0.0.0/16
10.0.0.0/8
10.0.0.0/16
10.0.0.0/24
10.000/27

GatewaySubnet [
10.0.0.0/27
10.00.0/16
10.0.0.0/24
10.0.0.0/27
10,0.0.0/29

Answer:

Explanation:
Answer Area

VNetl: 10.0.0.0/16

GatewaySubnet: 10.0.0.0/27

Question: 281

HOTSPOT
You have an Azure subscription that contains 200 virtual machines
You need to use Azure Network Watcher to identify which virtual machines generate the most network traffic. The solution must minimize administrative effort.
Which prerequisites should you deploy for Network Watcher, and which Network Watcher feature should you use to identify the virtual machines? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area

Prerequisites: | A Log Analytics workspace and Azure Blob Storage Azure
Monitor Agent and Azure Blob Storage Azure Monitor Agent
and Azure Files
A Log Analytics workspace and Azure Blob Storage
A Log Analytics workspace and Azure Files

Feature Network Performance Monitor
Connection monitor
IP flow verify
Network Performance Monitor
Traffic Analytics
Usage + quotas

Answer:

Explanation:
Answer Area

Prerequisites A Log Analytics workspace and Azure Blob Storage

Question: 282

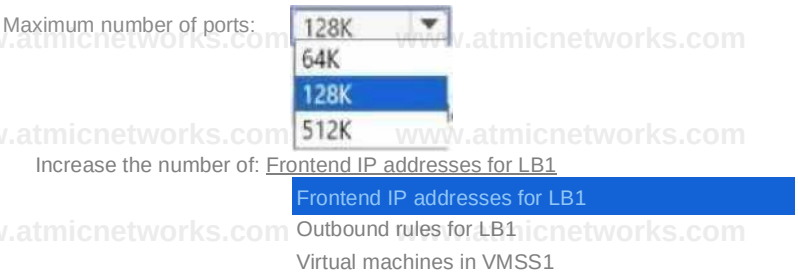
HOTSPOT

You have an Azure subscription that contains a virtual machine scale set named VMSS1 and a public standard Azure load balancer named LB1. VMSS1 contains eight virtual machines that have private IP addresses only VMSS1 is configured as a backend pool of LB1. LB1 has two frontend IP addresses and one outbound rule that provides internet connectivity to VMSS1.

What is the maximum number of ports available to the virtual machines in VMSS1. and what should you change to increase the maximum number of SNAT ports available to VMSS1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

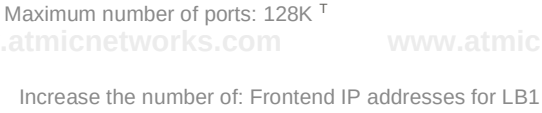
Answer Area



Answer:

Explanation:

Answer Area



Question: 283

You have an Azure virtual network named VNet1 that contains the subnets shown in the following table.

Name	Is a gateway subnet	Description
Subnet!	No	Has connected virtual machines
SubnetZ	No	Has no connected resources
GatewaySubnet	Yes	*None*

You need to deploy an Azure application gateway named AppGW1 to VNetI To where can you deploy AppGW1?

A. GatewaySubnet only
B. Subnet2 only
C. Subnet1 or Subnet2 only
D. Subnet2 or GatewaySubnet only
E. Subnet1, Subnet2, and GatewaySubnet

Answer: B

Explanation:

Question: 284

You have an Azure subscription that contains an Azure App Service web app named WebApp1 and an Azure Front Door profile named FDProfile1 FDProfile1 forwards requests addressed to https://www.contoso.com to WebApp1.
You need to ensure that only requests addressed to https://www.contoso.com/users/are forwarded to WebApp1.
What should you modify in FDProfile1?

A. the origin group
B. the endpoint
C. the routes
D. the domain

Answer: C

Explanation:

Question: 285

HOTSPOT

You have an Azure subscription that contains six Azure App Service apps. The apps have an identical configuration and are deployed across multiple Azure regions.

You plan to deploy Azure Front Door to load balance traffic across the apps.

You need to ensure that the round robin load-balancing algorithm will send traffic only to a limited number App Service apps based on their proximity to a user. The solution must minimize administrative effort.

What should you modify, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Modify: The onqin croup

The origin group
The route
The rule set

Configure: The latency sensitivity

An action
The forwarding protocol
The latency sensitivity

Answer:

Explanation:

Answer Area

Modify: The onqm group

Configure: The latency sensitivity

Question: 286

Your company has offices in London, Tokyo, and New York.

The company has a web app named App1 that has the Azure Traffic Manager profile shown in the following table.

Parameter	Value	Azure region
DNS Name	appl.trafficmanager.net	*Not applicable*
Endpoint	appl-asia.azurewebsites.net	East Asia
Endpoint	appl-na.azurewebsites.net	East US
Endpoint	appl-na.azurewebsites.net	UK South
Routing method	Geographic	*Not applicable*

In Asia, you plan to deploy an additional endpoint that will host an updated version of App1. You need to route 10 percent of the traffic from the Tokyo office to the new endpoint during testi What should you configure in Traffic Manager?

A. one profile and five endpoints
B. two profiles and four endpoints
C. three profiles and four endpoints
D. two profiles and five endpoints

Answer: B

Explanation:

Question: 287

You have an Azure subscription that contains an Azure Front Door Premium profile named AFD1 and an Azure Web Application Firewall (WAF) policy named WAF1. AFD1 is associated with WAF1.

You need to configure a rate limit for incoming requests to AFD1.

Solution: You add a rule to the rule set of AFD1.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Question: 288

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
VNet1	Virtual network	*Not applicable*
FW1	Azure Firewall	Deployed to VNet1
SQLDB1	Azure SQL Database	Configured to only accept connections in Proxy mode Deployed to VNet1

You need to configure FW1 to filter traffic that originates from VNet1 and targets the FQDN of SQLDB1 Which type of rule should you use?

A. infrastructure

B. application

C. DNAT

D. network

Answer: B

Explanation:

Question: 289

HOTSPOT

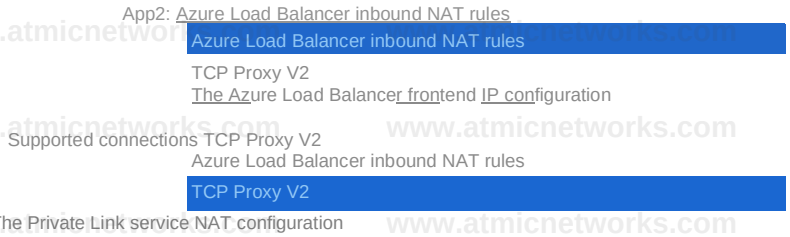
You have an Azure subscription. The subscription contains two virtual machine scale sets that host two apps named App1 and App2, an Azure Private Link service named PLS1. and an Azure load balancer named LB1. PLS1 uses LB1 and has TCP Proxy V2 disabled PLS1 provides access to App1 only.

You need to perform the following actions:

- Provide access to App1 and App2.
- Increase the number of supported private endpoint connections.

What should you modify to provide access to App2, and what should you modify to increase the number of supported connections? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

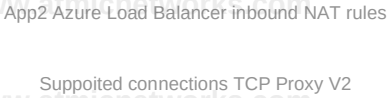
Answer Area



Answer:

Explanation:

Answer Area



Question: 290

HOTSPOT

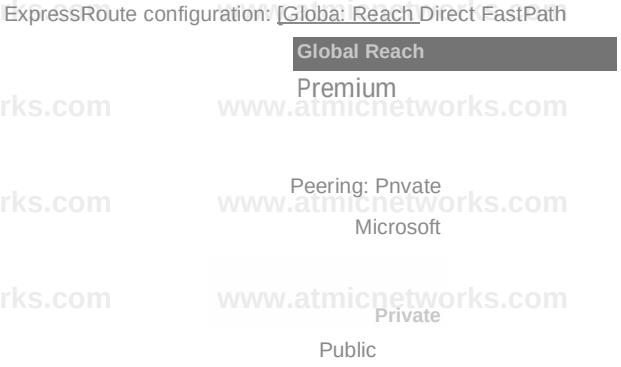
You have on-premises datacenters in New York and Seattle.

You have an Azure subscription that contains the ExpressRoute circuits shown in the following table.

Name	Azure region	Datacenter
ERC1	East US	New Vork
ERC2	West US2	Seattle

You need to ensure that all the data sent between the datacenters is routed via the ExoressRoute circuits. The solution must minimize costs.

Answer Area



Answer:

Answer Area

ExpressRoute configuration: Global Reach *

Peering: Pnvate *

Question: 291

Your company has an office in New York.

The company has an Azure subscription that contains the virtual networks shown in the following table.

Name	Location
Vnet1	East LS
Vnet2	North Europe
Vnet3	West US
Vnet4	West Europe

You need to connect the virtual networks to the office by using ExpressRoute. The solution must meet the following requirements:

- The connection must have up to 1 Gbps of bandwidth.
- The office must have access to all the virtual networks.
- Costs must be minimized.

How many ExpressRoute circuits should be provisioned, and which ExpressRoute 5KU should you enable?

A. one ExpressRoute Standard circuit

B. one ExpressRoute Premium circuit

C. two ExpressRoute Premium circuits

D. four ExpressRoute Standard circuits

Answer: B

Explanation:

Question: 292

You have the Azure virtual networks shown in the following table.

Name	Subnet	Subnet address space	Peered with
Vnetl	Subnet) *1	10.1.1.0/24	Vnet3
Vnet2	Subnet2-1	10.2.1.0/24	Vnet3
Vnet3	AzureFirewallSubnet	10.3.1.0/24	Vnetl, Vnet2

You deploy Azure Firewall to Vnet3.

You need to ensure that the traffic from Subnet1-1 to Subnet2-1 passes through the firewall. What should you configure?

A. peering links between Vnet1 and Vnet2

B. a route table associated to Subnet1 -1 and Subnet2-1
C. an Azure private DNS zone
D. a route table associated to AzureFitewallSubnet

Answer: B

Explanation:

Question: 293

You plan to implement an Azure virtual network that will contain 10 virtual subnets. The subnets will use IPv6 addresses. Each subnet will host up to 200 load-balanced virtual machines.

You need to recommend which subnet mask size to use for the virtual subnets.

What should you recommend?

A. /64
B. /120
C. /48
D. /24

Answer: D

Explanation:

Question: 294

You have 10 on-premises networks that are connected by using a 3rd party Software Defined Wide Area Network (SD-WAN) solution. You have an Azure subscription that contains five virtual networks. You plan to connect the Azure virtual networks and the on-premises networks by using an Azure Virtual WAN with a single virtual WAN hub.

You need to ensure that the Azure Virtual WAN can act as a node in the 3rd party SD-WAN solution. What should you include in the solution?

A. An Azure Virtual WAN ExpressRoute gateway
B. A Network Virtual Appliance (NVA)

C. A Site to site gateway (VPN gateway)
D. A Point to site gateway (User VPN gateway)

Answer: B

Explanation: