Free Questions for AZ-700 by dumpshq

Shared by Meyers on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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

Question 2

Question Type: MultipleChoice

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.

Options:

A- See the Explanationbelow for step by step in structions

Answer:

A

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 selectCreate a resource. Search forlocal network gateway, selectLocal network gateway, then selectCreate2.

On theCreate local network gatewaypage, 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.

SelectReview + createand then selectCreateto create your local network gateway2.

Question 3

Question Type: MultipleChoice

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.

Options:

A- See the Explanationbelow for step by step in structions

Answer:

A

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 4

Question Type: **MultipleChoice**

Task 9

You need to ensure that subnet4-3 can accommodate 507 hosts.

Options:

A- See the Explanationbelow for step by step in structions

Answer:

A

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, wherenis the number of bits in the subnet mask1. You need to find the value ofnthat 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 withn = 24, which is the default subnet mask for Class C networks. Then, plug in the value ofninto the formula and see if it is too big or too small for 507 hosts.

If you tryn = 24, you getnumber of hosts = 2^(32 - 24) - 2 = 254, which is too small. You need to increase the value ofnto get a larger number of hosts.

If you tryn = 25, you getnumber of hosts = 2^(32 - 25) - 2 = 510, which is just enough to accommodate 507 hosts. You can stop here or try a smaller value ofnto see if it still works.

If you tryn = 26, you getnumber of hosts = 2^(32 - 26) - 2 = 254, which is too small again. You need to decrease the value ofnto get a larger number of hosts.

Therefore, the smallest value ofnthat can accommodate 507 hosts isn = 25. This means that the subnet mask for subnet4-3 should be/25or255.255.255.128in 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/24to/25. Then select Save2.

Question 5

Question Type: **MultipleChoice**

Task 8

You need to ensure that the storage34280945 storage account will only accept connections from hosts on VNET1

Options:

A- See the Explanationbelow for step by step in structions

Answer:

A

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 selectingNetworkingunderSettings1.

On theNetworkingpage, selectFirewalls and virtual networks, and then selectSelected networksunderAllow access from1. This will block all access to your storage account except from the networks or resources that you specify.

UnderVirtual 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.

SelectAddto add the virtual network and subnet to your storage account1.

SelectSaveto apply your changes1.

Question 6

Question Type: MultipleChoice

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.

Options:

A- See the Explanationbelow for step by step in structions

Answer:

A

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 7

Question Type: MultipleChoice

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.

Options:

A- See the Explanationbelow for step by step in structions

Answer:

A

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 selectCreate a resource. Search forNAT gateway, selectNAT gateway, then selectCreate3.

On theCreate a NAT gatewaypage, 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: SelectCreate newand type a name for your public IP address. SelectStandardas the SKU andStaticas the assignment method4.

SelectReview + createand then selectCreateto create your NAT gateway3.

To associate the NAT gateway with subnet3-2, you need to go to theVirtual networksservice in the Azure portal and select your virtual network.

On theVirtual networkpage, selectSubnetsunderSettings, and then select subnet3-2 from the list.

On theEdit subnetpage, underNAT gateway, select your NAT gateway from the drop-down list. Then selectSave.

Question 8

Question Type: MultipleChoice

Task 5

You need to ensure that requests for wwwjelecloud.com from any of your Azure virtual networks resolve to frontdoor1.azurefd.net.

Options:

A- See the Explanationbelow for step by step in structions

Answer:

A

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.