AZ-700 Q&As

Designing and Implementing Microsoft Azure Networking Solutions

Pass Microsoft AZ-700 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/az-700.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

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. RouteDiagnosticLog

C. GatewayDiagnosticLog

D. TunnelDiagnosticLog

Correct Answer: A

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.

Reference:

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

QUESTION 2

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

Correct Answer: A

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

QUESTION 3

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. Azure DDoS Protection for virtual networks

C. service endpoint policies

D. service endpoints

Correct Answer: A

During the creation of the load balancer, you\\'ll configure:

Frontend IP address Backend pool Inbound load-balancing rules

When you create an internal load balancer, a virtual network is configured as the network for the load balancer.

A private IP address in the virtual network is configured as the frontend for the load balancer. The frontend IP address can be Static or Dynamic.

Incorrect:

* service endpoints

A service endpoint is created in a virtual subnet, but there is no IP address defined for the Service endpoint.

Service endpoints are a way for Azure DevOps to connect to external systems or services. They\\'re a bundle of properties securely stored by Azure DevOps, which includes but isn\\'t limited to the following properties:

Service name Description Server URL Certificates or tokens User names and passwords

* service endpoint policies Service Endpoint Policy object, example.

"serviceEndpointPolicyDefinitions": [

{

"description": null,

"name": "MySEP-Definition",

"resourceGroup": "MySEPDeployment",

"service": "Microsoft.Storage",

"serviceResources": [

"/subscriptions/subscriptionID/resourceGroups/MySEPDeployment/providers/Microsoft.Storage/storageAccounts/mystgacc"

],

"type": "Microsoft.Network/serviceEndpointPolicies/serviceEndpointPolicyDefinitions"

}]

Reference: https://learn.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-internal-portal https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview

---

QUESTION 4

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. blob storage only

B. blob storage, a file path on VM1, and a premium storage account

C. a file path on VM1 only

D. blob storage and a file path on VM1 only

E. blob storage and a premium storage account only

F. a premium storage account only

Correct Answer: D

Once your packet capture session has completed, the capture file is uploaded to blob storage or to a local file on the virtual machine. The storage location of the packet capture is defined during creation of the packet capture.

Reference: https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-manage-portal

---

QUESTION 5

HOTSPOT

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

Name	Address space	Associated network security group (NSG)
Subnet1	10.10.0.0/24	NSG1
Subnet2	10.10.1.0/24	NSG2

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.

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

Hot 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.	○	○

Correct Answer:

Box 1: Yes

VM3 is Subnet2. NSG2 applies. The default rule will allow communication.

Box 2: No

VM1 and VM2 is in Subnet1. NSG1 applies. Only traffic on ports 80 and 443 will be allowed. Connection on port 9090 will be denied.

Note: Priority: A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a

result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

Box 3: No

VM1 is in Subnet1. NSG1 applies. Only traffic on ports 80 and 443 will be allowed. Connection on port 9090 will be denied.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview