AZ-700$^{\text{Q\&As}}$

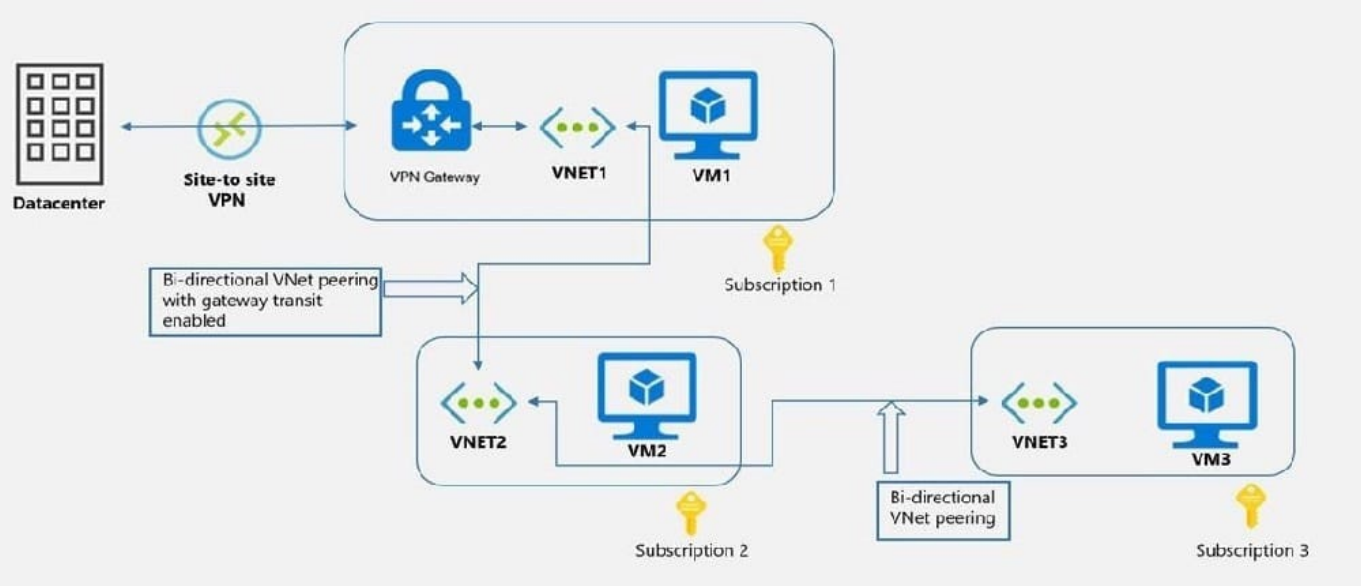
Designing and Implementing Microsoft Azure Networking Solutions

Pass Microsoft AZ-700 Exam with 100% Guarantee

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

QUESTION 1

You have an Azure environment as shown below.



You need to find to which environments/virtual machines that VM1 can communicate?

A. VM2 Only

B. VM2 and VM3 Only

C. The on-premise datacenter and VM2 only

D. The on-premise datacenter, VM2 and VM3 only

Correct Answer: C

VM1 is in VNET1. VNET1 has a Site-to-Site VPN connection with on-premise data center. So, VM1 can communicate with on-premise datacenter.

VM1 is in VNET1. VNET1 is peered with VNET2. So, VM1 can communicate with VM2.

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

QUESTION 2

You have an Azure subscription named Subscription1.

You have two virtual networks in Subscription1 named HubVNet and SpokeVNet.

You have an Azure Firewall with a public IP address, configured as a Standard SKU in HubVNet.

You have a Windows Server 2016 with private IP address in SpokeVNet.

You need to connect to Windows Server using the public IP address of Azure firewall.

What should you configure?

A. ExpressRoute Gateway

B. Virtual Network Peering

C. Route Table

D. Virtual Network Gateway

E. NAT Rule for the Firewall

Correct Answer: BCE

For traffic to flow between the Hub and Spoke VNets, you will need a peer connection between the virtual networks.

You will need a route table to route ingress traffic to the firewall virtual appliance.

You can configure a NAT rule on the firewall to translate and filter inbound Internet traffic to your subnets.

QUESTION 3

You have an Azure virtual network named Hub1.

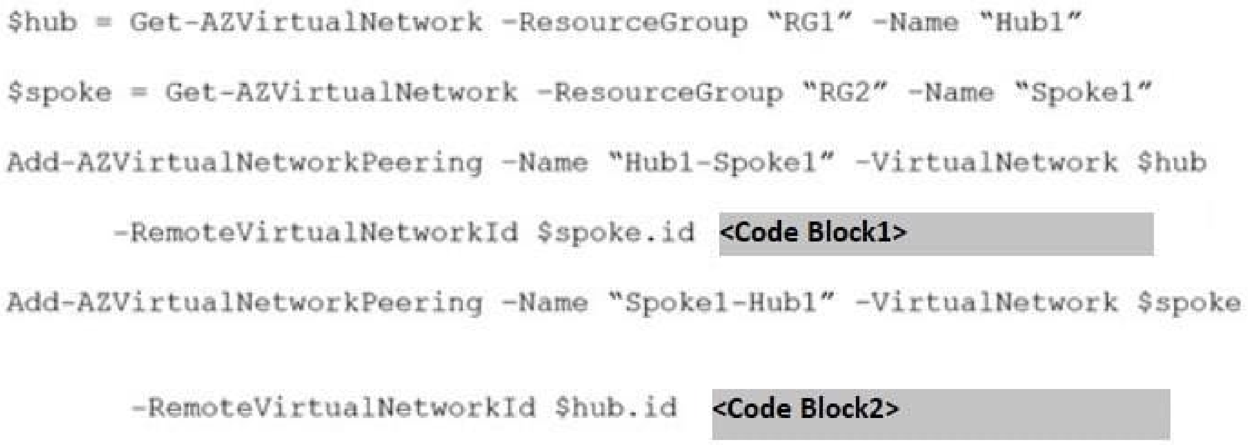
Hub1 connects to an on-premises network by using a Site-to-Site VPN connection.

You created an Azure Virtual network named Spoke1.

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?



```
$hub = Get-AZVirtualNetwork -ResourceGroup “RG1” -Name “Hub1”

$spoke = Get-AZVirtualNetwork -ResourceGroup “RG2” -Name “Spoke1”

Add-AZVirtualNetworkPeering -Name “Hub1-Spoke1” -VirtualNetwork $hub

      -RemoteVirtualNetworkId $spoke.id <Code Block1>

Add-AZVirtualNetworkPeering -Name “Spoke1-Hub1” -VirtualNetwork $spoke


       -RemoteVirtualNetworkId $hub.id <Code Block2>
```

A. Code Block1: -AllowForwardedTraffic

B. Code Block1: -AllowGatewayTransit

C. Code Block1: -UseRemoteGateways

D. Code Block2: -AllowForwardedTraffic

E. Code Block2: -AllowGatewayTransit

F. Code Block2: -UseRemoteGateways

Correct Answer: BF

Virtual network peering is a non-transitive relationship between two virtual networks. You can configure spokes to use the hub gateway to communicate with remote networks. To allow gateway traffic to flow from spoke to hub and connect to

remote networks, you must:

Configure the peering connection in the hub to allow gateway transit.

Configure the peering connection in each spoke to use remote gateways.

Configure all peering connections to allow forwarded traffic.

Below is the sample code.

```
# Peer hub to spoke

Add-AzVirtualNetworkPeering -Name HubtoSpoke -VirtualNetwork $VNetHub -RemoteVirtualNetworkId $VNetSpoke.Id
-AllowGatewayTransit

# Peer spoke to hub

Add-AzVirtualNetworkPeering -Name SpoketoHub -VirtualNetwork $VNetSpoke -RemoteVirtualNetworkId $VNetHub.Id
-AllowForwardedTraffic UseRemoteGateways
```

https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-ps#peer-the-hub-and-spoke-virtual-networks
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli#virtual-networkpeering

Wrong Answers:

Code Block1: -AllowForwardedTraffic and Code Block2: -AllowForwardedTraffic

Allow forwarded traffic is used if you require connectivity between spokes. You can create routes to forward traffic from the spoke to the firewall or network virtual appliance, which can then route to the second spoke.

QUESTION 4

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

Correct Answer: A

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 5

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

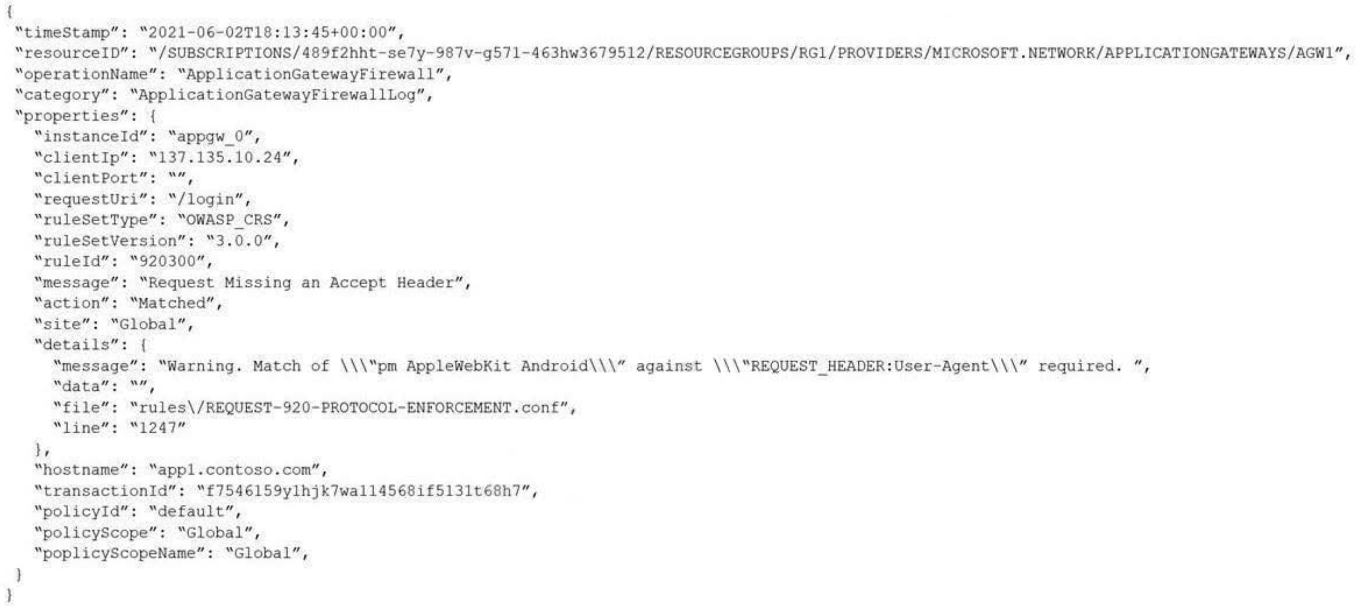
others might not have a correct solution.

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/489f2hht-se7y-987v-g571-463hw3679512/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_HEADER:User-Agent\\\" required. ",
     "data": "",
     "file": "rules\/REQUEST-920-PROTOCOL-ENFORCEMENT.conf",
     "line": "1247"
   },
   "hostname": "app1.contoso.com",
   "transactionId": "f7546159y1hjk7wa114568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```

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

Correct Answer: B

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

AZ-700 PDF Dumps AZ-700 Study Guide AZ-700 Braindumps