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

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.geekcert.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 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 Site1 can connect to storage1 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 service endpoint

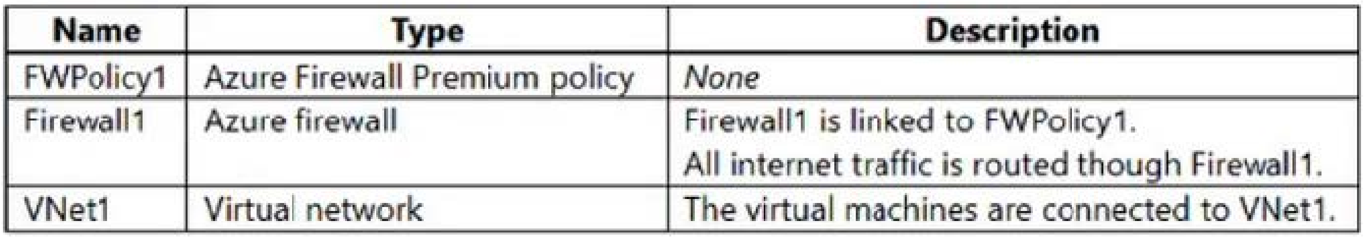
D. a private endpoint

Correct Answer: D

**QUESTION 2**

HOTSPOT

You have an Azure subscription that contains 10 virtual machines. The virtual machines are assigned private IP addresses. The subscription contains the resources shown in the following table.



| Name | Type | Description |
|---|---|---|
| FWPolicy1 | Azure Firewall Premium policy | *None* |
| Firewall1 | Azure firewall | Firewall1 is linked to FWPolicy1.<br>All internet traffic is routed though Firewall1. |
| VNet1 | Virtual network | The virtual machines are connected to VNet1. |

You need to configure FWPolicy1 to meet the following requirements:

1.

Allow incoming connections to the virtual machines from the internet on port 4567.

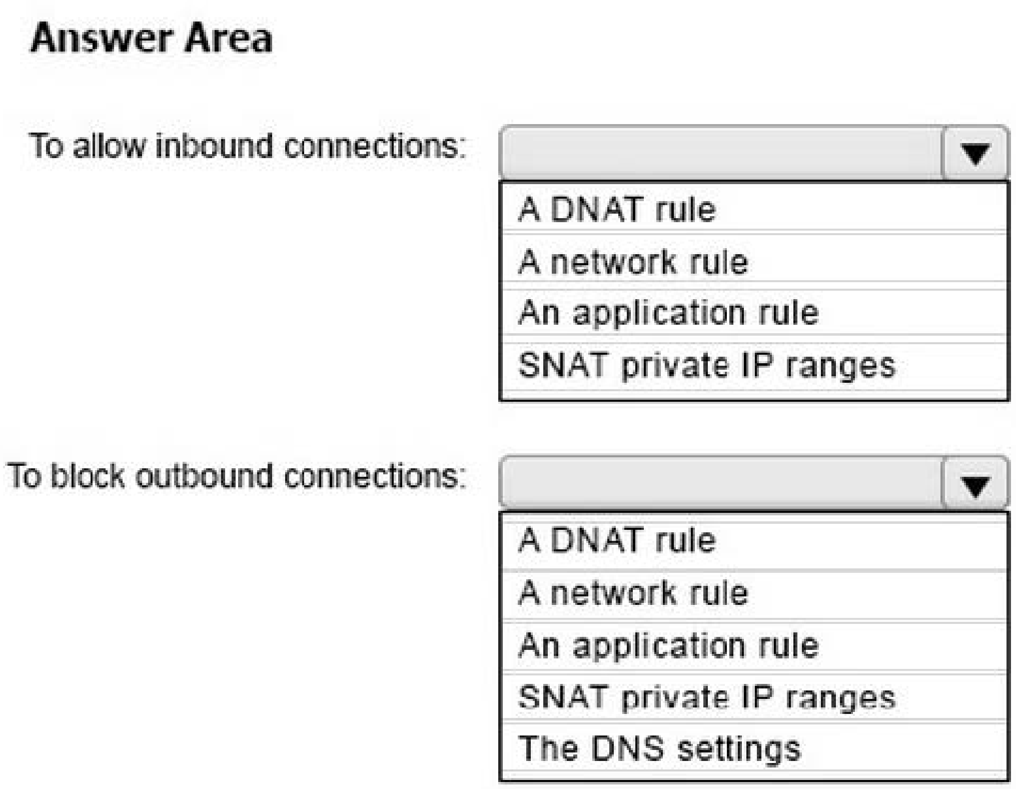
2.

Block outbound connections from the virtual machines to an FQDN of *.fabrikam.com.

What should you configure in FWPolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

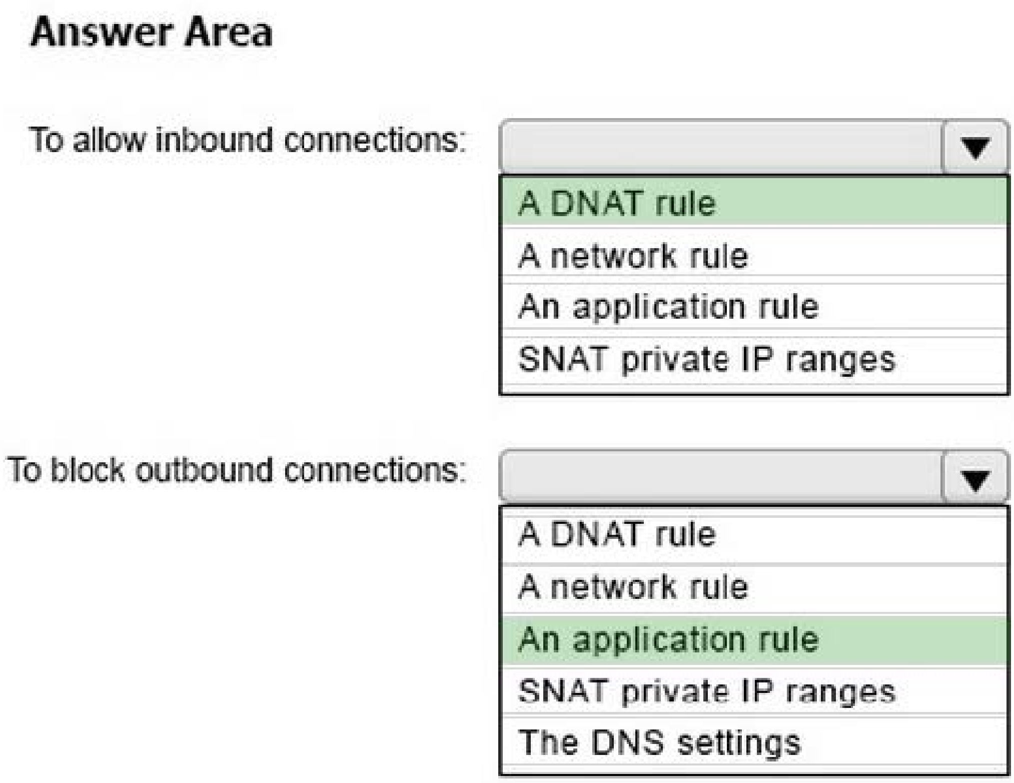
To allow inbound connections:

- A DNAT rule
- A network rule
- An application rule
- SNAT private IP ranges

To block outbound connections:

- A DNAT rule
- A network rule
- An application rule
- SNAT private IP ranges
- The DNS settings

Correct Answer:



Answer Area

To allow inbound connections:

- [✓ A DNAT rule]
- A network rule
- An application rule
- SNAT private IP ranges

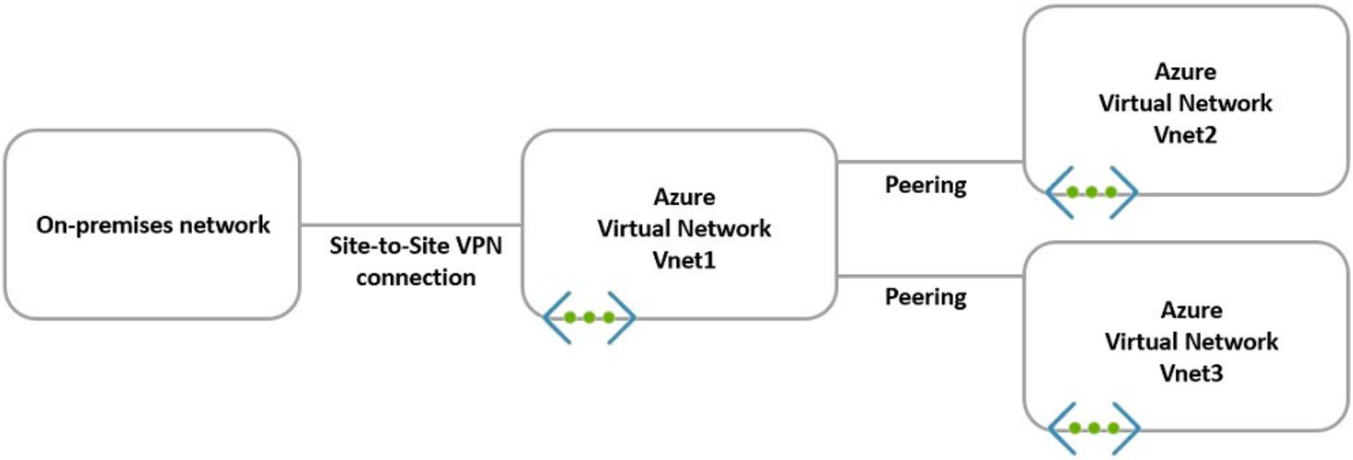
To block outbound connections:

- A DNAT rule
- A network rule
- [✓ An application rule]
- SNAT private IP ranges
- The DNS settings

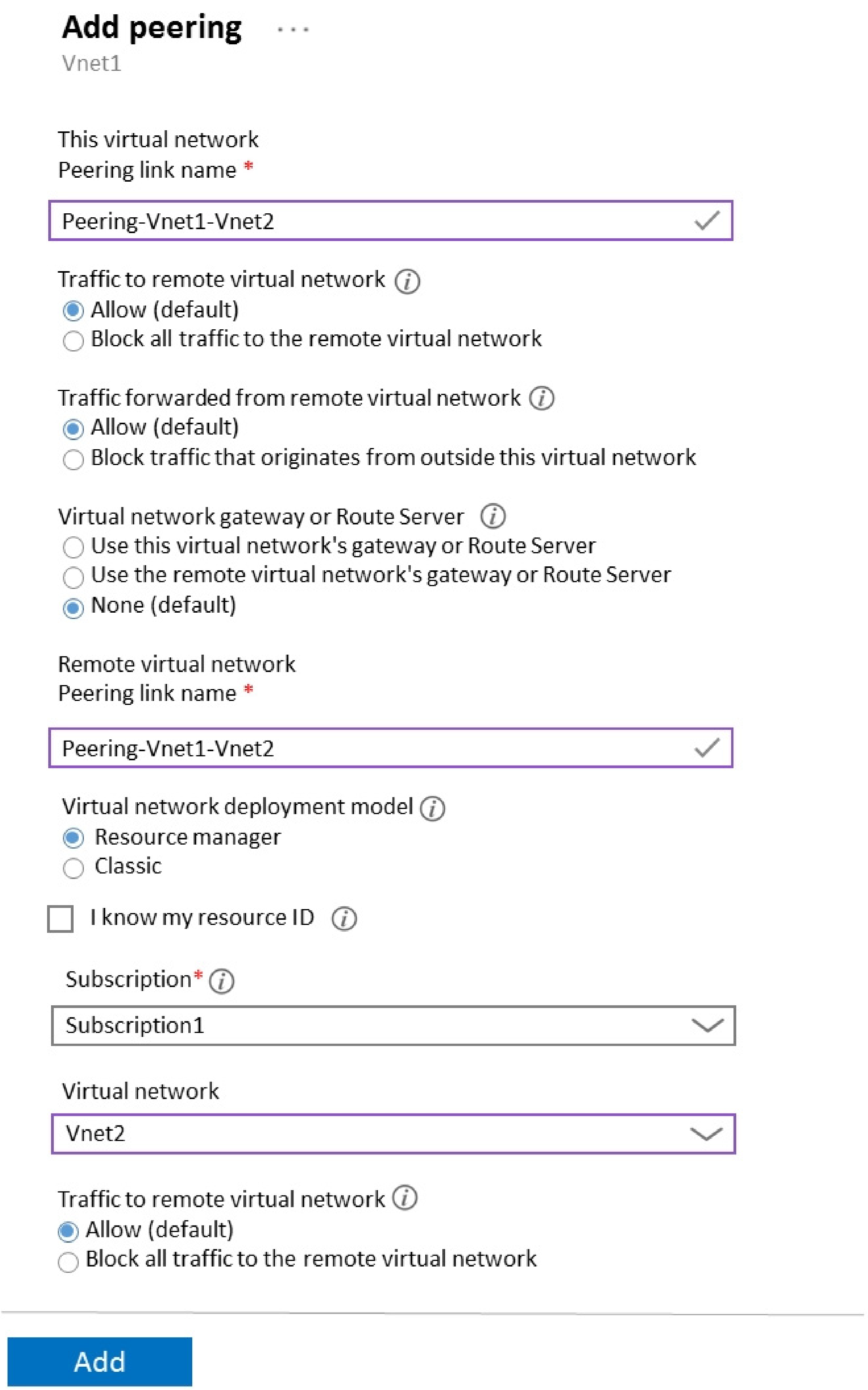
**QUESTION 3**

HOTSPOT

You have the hybrid network shown in the Network Diagram exhibit.


On-premises network
Site-to-Site VPN connection
Azure Virtual Network Vnet1
Peering
Peering
Azure Virtual Network Vnet2
Azure Virtual Network Vnet3

You have a peering connection between Vnet1 and Vnet2 as shown in the Peering-Vnet1-Vnet2 exhibit.



Add peering ...

Vnet1

This virtual network

Peering link name *

Peering-Vnet1-Vnet2 ✓

Traffic to remote virtual network ⓘ

● Allow (default)

○ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

● Allow (default)

○ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

○ Use this virtual network's gateway or Route Server

○ Use the remote virtual network's gateway or Route Server

● None (default)

Remote virtual network

Peering link name *

Peering-Vnet1-Vnet2 ✓

Virtual network deployment model ⓘ

● Resource manager

○ Classic

□ I know my resource ID ⓘ

Subscription * ⓘ

Subscription1

Virtual network

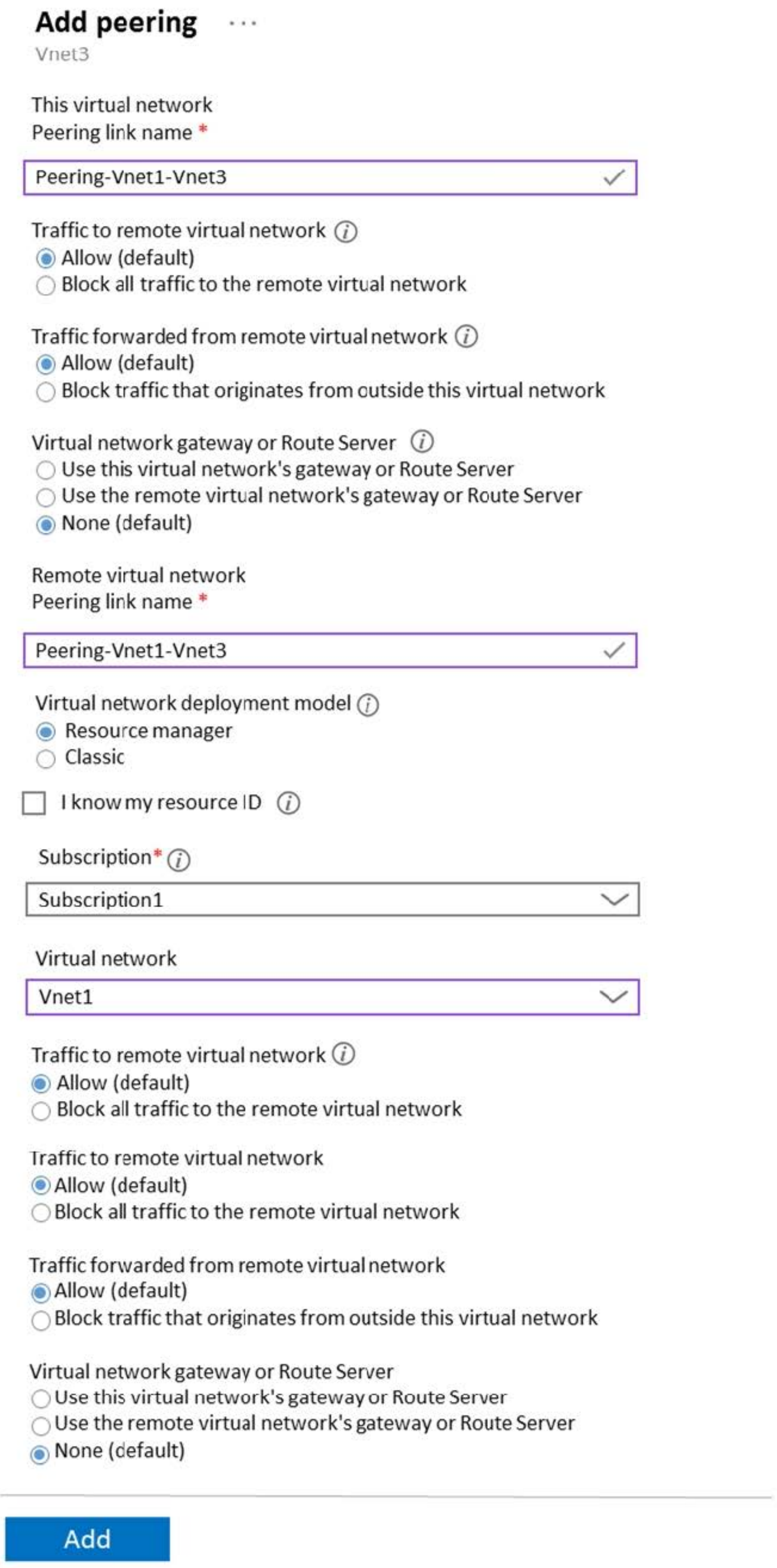
Vnet2

Traffic to remote virtual network ⓘ

● Allow (default)

○ Block all traffic to the remote virtual network

You have a peering connection between Vnet1 and Vnet3 as shown in the Peering-Vnet1-Vnet3 exhibit.



Add peering ···

Vnet3

This virtual network
Peering link name *

Peering-Vnet1-Vnet3 ✓

Traffic to remote virtual network ⓘ
● Allow (default)
○ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
● Allow (default)
○ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ
○ Use this virtual network's gateway or Route Server
○ Use the remote virtual network's gateway or Route Server
● None (default)

Remote virtual network
Peering link name *

Peering-Vnet1-Vnet3 ✓

Virtual network deployment model ⓘ
● Resource manager
○ Classic

□ I know my resource ID ⓘ

Subscription * ⓘ

Subscription1

Virtual network

Vnet1

Traffic to remote virtual network ⓘ
● Allow (default)
○ Block all traffic to the remote virtual network

Traffic to remote virtual network
● Allow (default)
○ Block all traffic to the remote virtual network

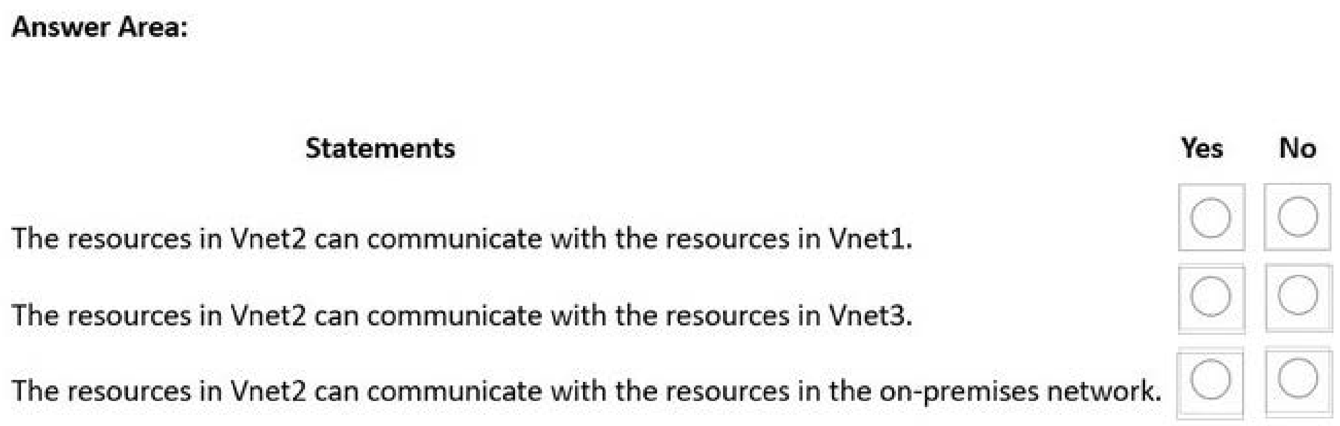
Traffic forwarded from remote virtual network
● Allow (default)
○ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server
○ Use this virtual network's gateway or Route Server
○ Use the remote virtual network's gateway or Route Server
● None (default)

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

NOTE: Each correct selection is worth one point.

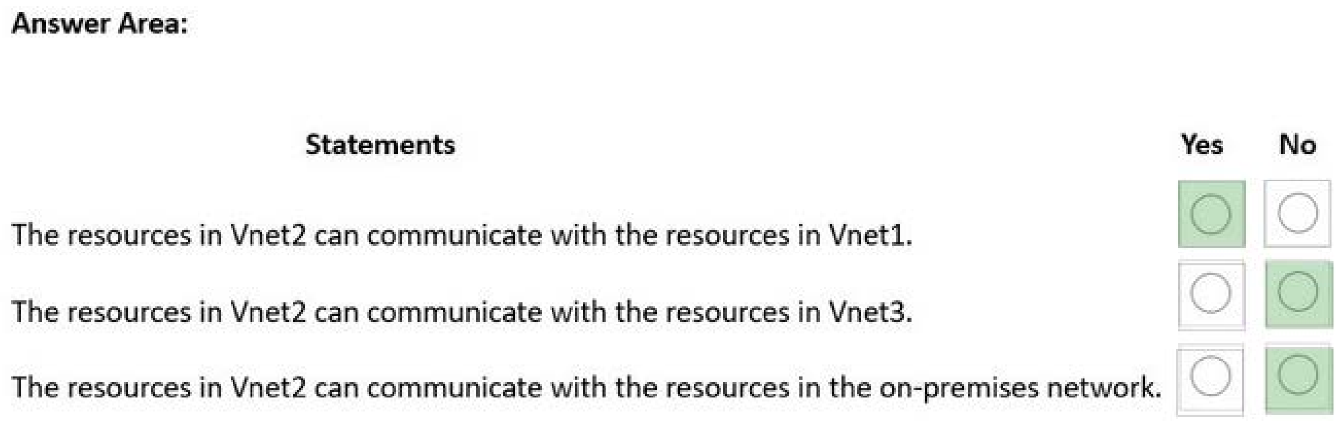
Hot Area:



**Answer Area:**

| Statements | Yes | No |
|---|---|---|
| The resources in Vnet2 can communicate with the resources in Vnet1. | ○ | ○ |
| The resources in Vnet2 can communicate with the resources in Vnet3. | ○ | ○ |
| The resources in Vnet2 can communicate with the resources in the on-premises network. | ○ | ○ |

Correct Answer:



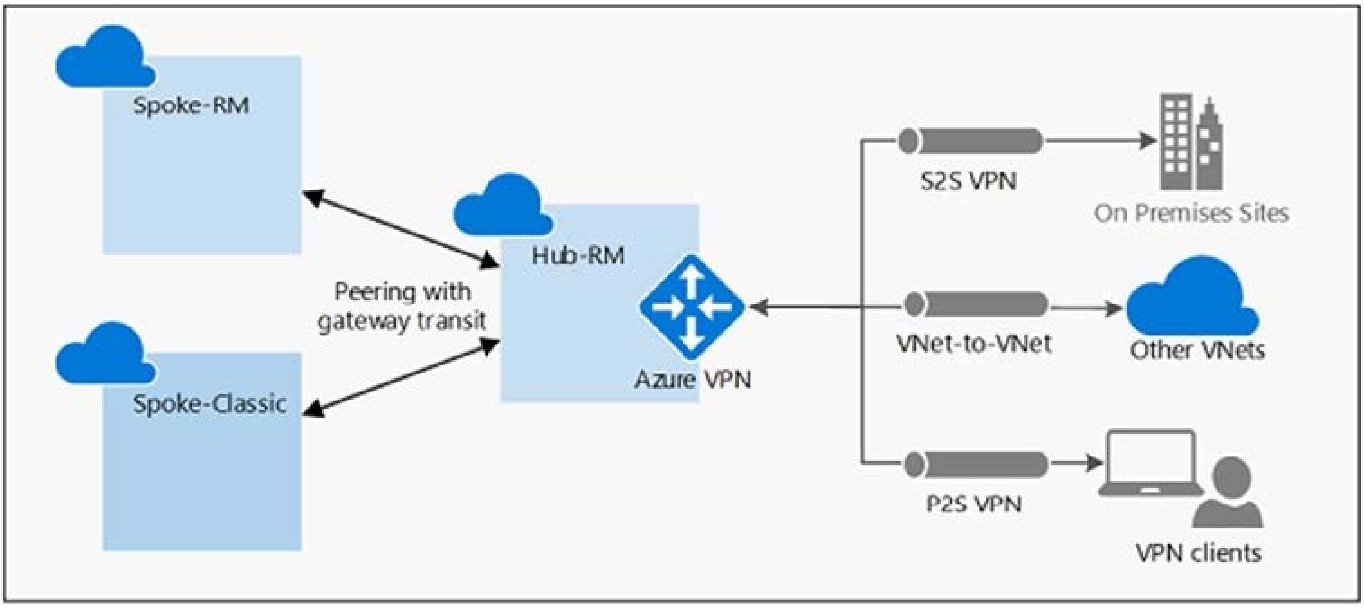
**Answer Area:**

| Statements | Yes | No |
|---|---|---|
| The resources in Vnet2 can communicate with the resources in Vnet1. | ● | ○ |
| The resources in Vnet2 can communicate with the resources in Vnet3. | ○ | ● |
| The resources in Vnet2 can communicate with the resources in the on-premises network. | ○ | ● |

Box 1: Yes

Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes.

Box 2: No No Virtual Gateway is used. Gateway transit is a peering property that lets one virtual network use the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity. The following diagram shows how gateway transit works with virtual network peering.



In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual

networks.

Box 3: No

No Virtual Gateway is used.

Reference:

https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

**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 reset the gateway of Vnet1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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**

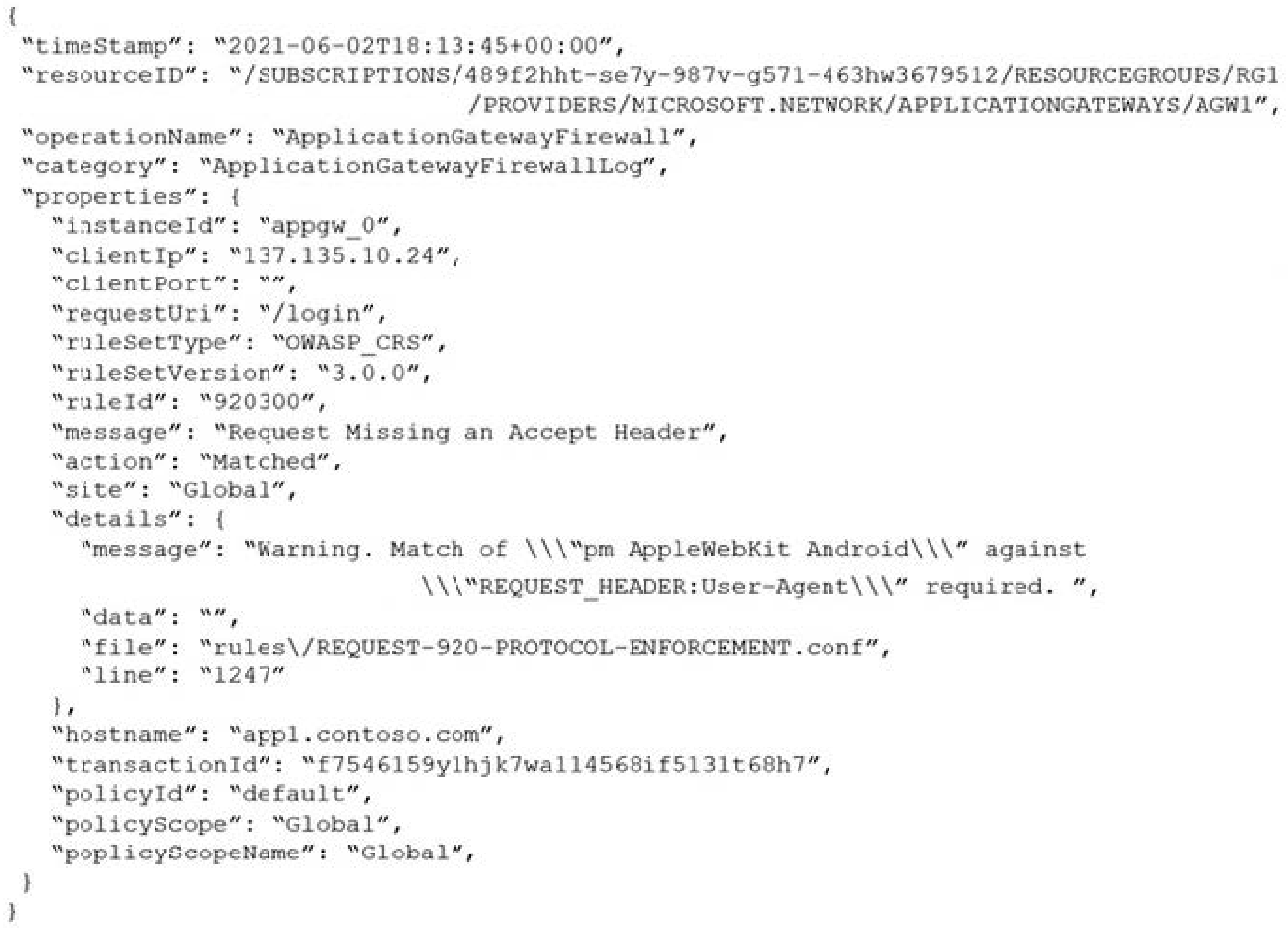
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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": "appl.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 disable the WAF rule that has a ruleld of 920300.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Latest AZ-700 Dumps    AZ-700 PDF Dumps    AZ-700 Study Guide