Microsoft AZ-700 Exam Actual Questions (P. 8)

The questions for AZ-700 were last updated on April 23, 2024.

Viewing page **8** out of 10 pages.
Viewing questions 190-216 out of 267 questions

Custom View Settings

Question #22

Topic 4

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. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).
B. On FW1, create an outbound service tag rule for Azure Cloud.
C. Deploy a NAT gateway.
D. Deploy an application security group that allows outbound traffic to 1688.

Reveal Solution

Discussion 5

Question #23

Topic 4

You have an Azure subscription that contains a virtual network named 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. a network rule
B. URL filtering
C. a DNAT rule
D. an application rule

Reveal Solution

Discussion 4

Question #24 *Topic 4*

HOTSPOT

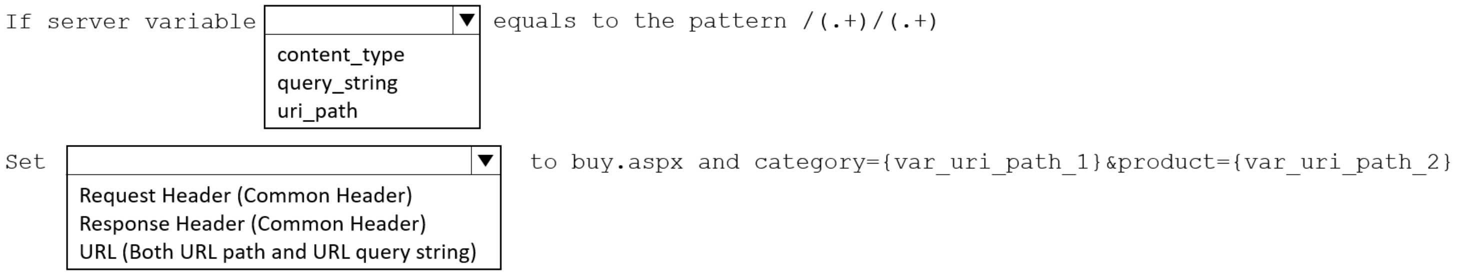
-

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 https://www.contoso.com/buy.aspx?category=fashion&product=shirts.

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

NOTE: Each correct selection is worth one point.



If server variable [▼] equals to the pattern /(.+)/(.+)

- content_type
- query_string
- uri_path

Set [▼] to buy.aspx and category={var_uri_path_1}&product={var_uri_path_2}

- Request Header (Common Header)
- Response Header (Common Header)
- URL (Both URL path and URL query string)

Reveal Solution   Discussion 2

Question #25 *Topic 4*

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. On FW1, create an outbound network rule that allows traffic to the Azure Key Management Service (KMS).

B. On FW1, create an outbound service tag rule for Azure Cloud.

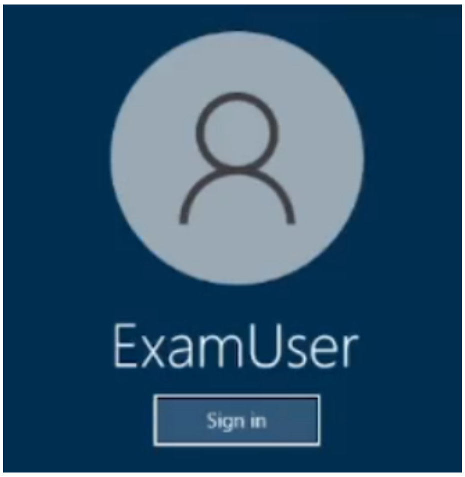
C. Deploy a NAT gateway.

D. On FW1, configure a DNAT rule for port 1688.

Reveal Solution   Discussion 7

Question #26 *Topic 4*

SIMULATION
-



Username and password
-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx
-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the
portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678
-

You need to create an Azure Firewall instance named FW1 that meets the following requirements:

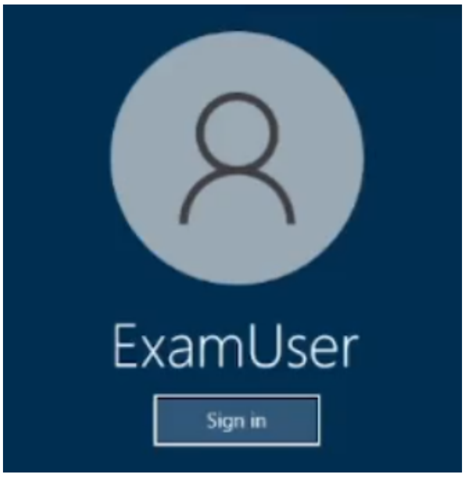
- Has an IP address from the address range of 10.1.255.0/24
- Uses a new Premium firewall policy named FW-policy1
- Routes traffic directly to the internet

To complete this task, sign in to the Azure portal.

Reveal Solution Discussion 9

Question #27 *Topic 4*

SIMULATION
-



ExamUser

Sign in

Username and password
-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx
-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the
portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678
-

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.

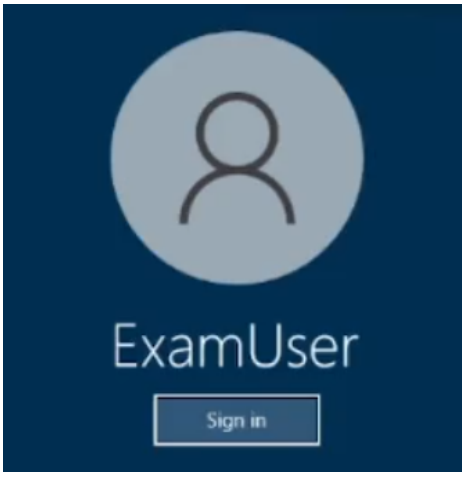
To complete this task, sign in to the Azure portal.

Reveal Solution   Discussion 4

Question #28 *Topic 4*

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

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.

To complete this task, sign in to the Azure portal.

Reveal Solution Discussion 3

Question #29 *Topic 4*

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 NSG1 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 131.1071.15.
• Minimize changes to NSG1 when a new subnet is created.

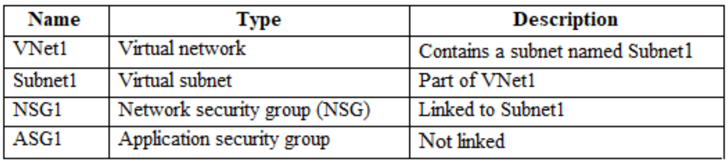
What should you use as the destination in the inbound security rule?

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

Reveal Solution Discussion 4

Question #30 *Topic 4*

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



Name	Type	Description
VNet1	Virtual network	Contains a subnet named Subnet1
Subnet1	Virtual subnet	Part of VNet1
NSG1	Network security group (NSG)	Linked to Subnet1
ASG1	Application security group	Not linked

Subnet1 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.

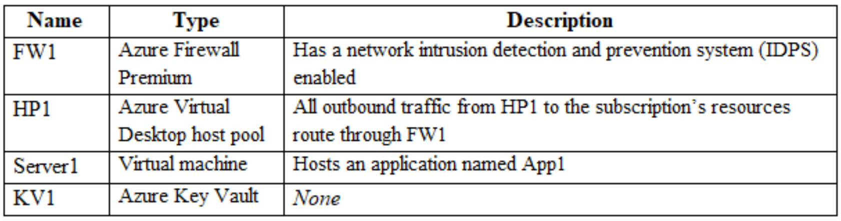
What should you do?

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.

Reveal Solution Discussion 2

Question #31 *Topic 4*

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
Server1	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.contoso.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.

Reveal Solution Discussion 3

Question #32 *Topic 4*

HOTSPOT
-

Case Study
-

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. When you are ready to answer a question, click the Question button to return to the question.

Overview
-

Contoso, Ltd. is a consulting company that has a main office in San Francisco and a branch office in Dallas.

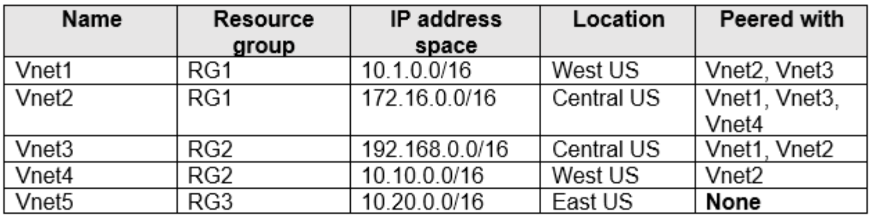
Contoso recently purchased an Azure subscription and is performing its first pilot project in Azure.

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.

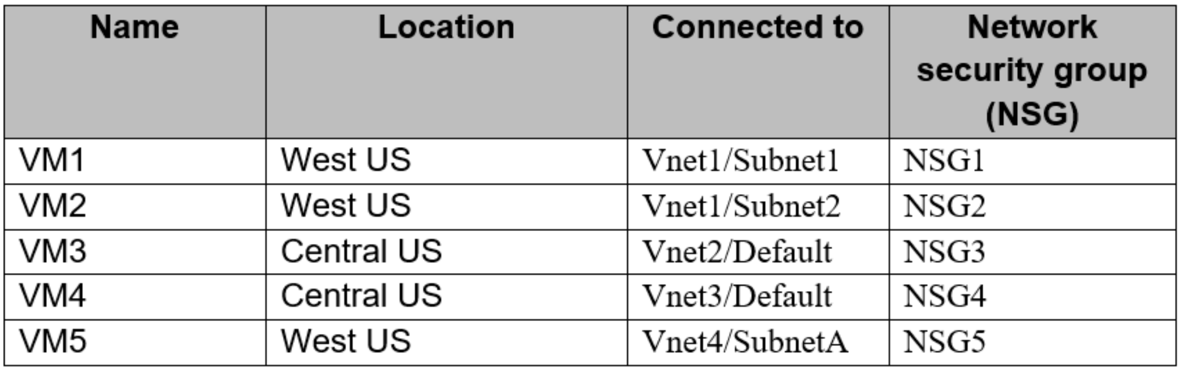


Name	Resource group	IP address space	Location	Peered with
Vnet1	RG1	10.1.0.0/16	West US	Vnet2, Vnet3
Vnet2	RG1	172.16.0.0/16	Central US	Vnet1, Vnet3, Vnet4
Vnet3	RG2	192.168.0.0/16	Central US	Vnet1, Vnet2
Vnet4	RG2	10.10.0.0/16	West US	Vnet2
Vnet5	RG3	10.20.0.0/16	East US	**None**

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.

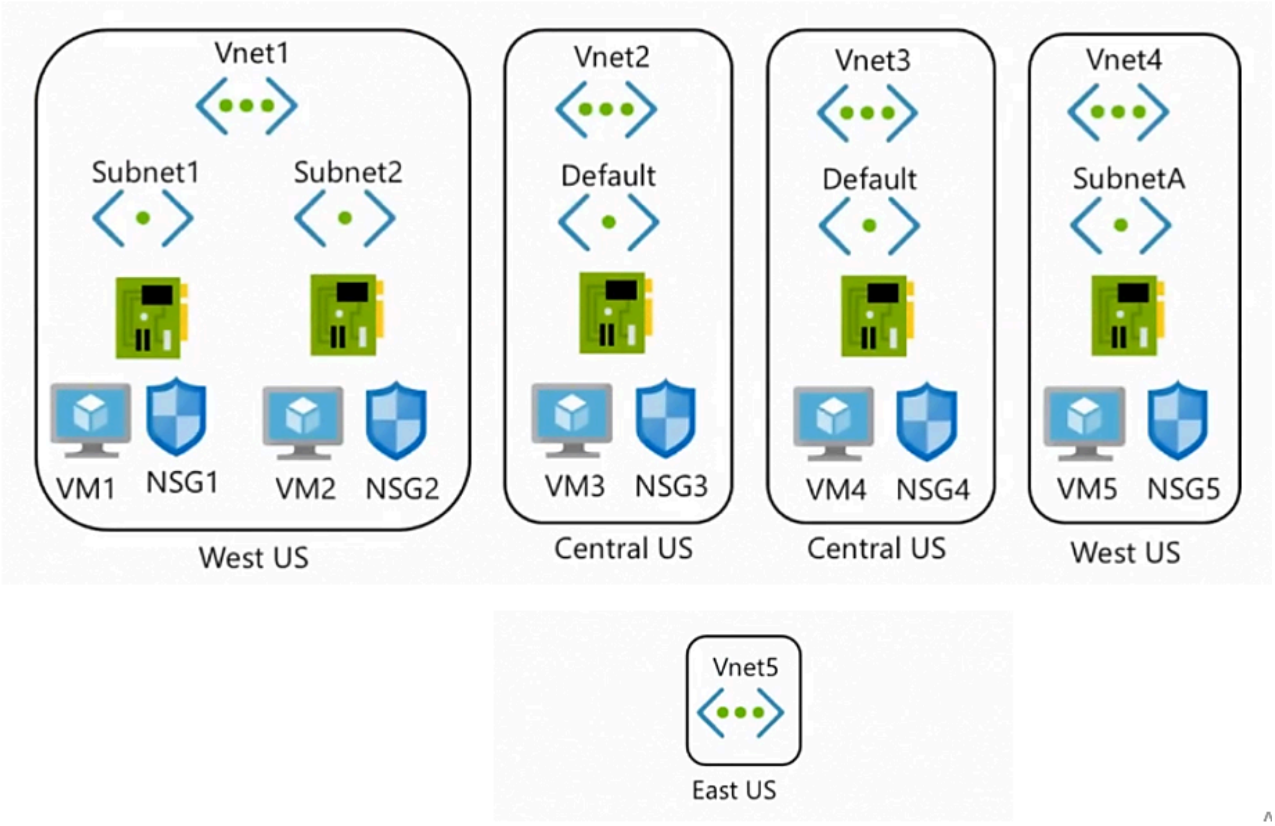


Name	Location	Connected to	Network security group (NSG)
VM1	West US	Vnet1/Subnet1	NSG1
VM2	West US	Vnet1/Subnet2	NSG2
VM3	Central US	Vnet2/Default	NSG3
VM4	Central US	Vnet3/Default	NSG4
VM5	West US	Vnet4/SubnetA	NSG5

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 Network Infrastructure Diagram



Azure Private DNS Zones
-

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

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

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

Requirements
-

Virtual Network Requirements
-

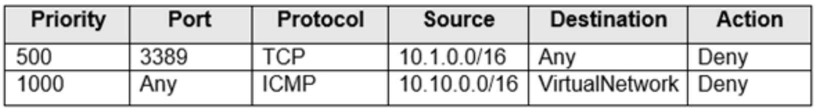
Contoso has the following virtual network requirements:

• Create a virtual network named Vnet6 in West US that will contain the following resources and configurations:
o Two container groups that connect to Vnet6
o Three virtual machines that connect to Vnet6
o Allow VPN connections to be established to Vnet6
o 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
-

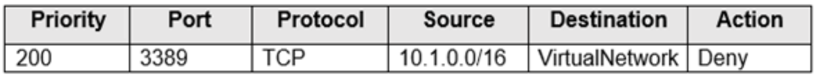
Contoso has the following network security requirements:

- 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.



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

- 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.

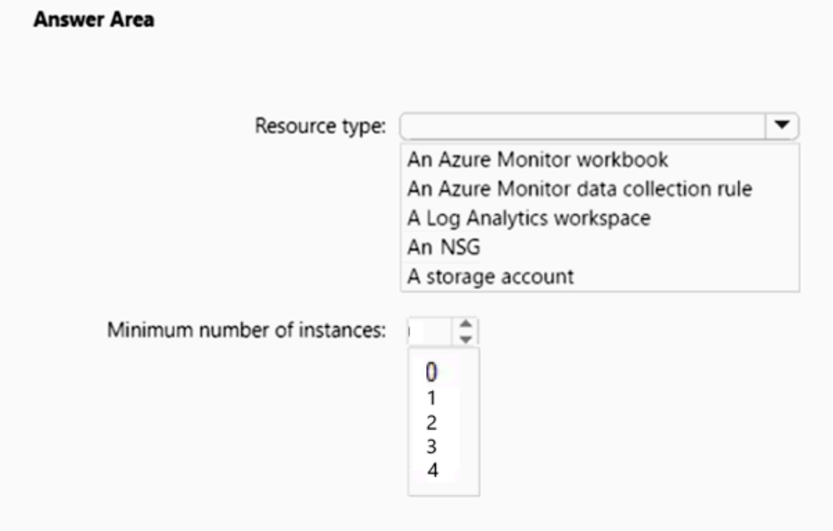


Priority	Port	Protocol	Source	Destination	Action
200	3389	TCP	10.1.0.0/16	VirtualNetwork	Deny

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 Area

Resource type:
- An Azure Monitor workbook
- An Azure Monitor data collection rule
- A Log Analytics workspace
- An NSG
- A storage account

Minimum number of instances:
- 0
- 1
- 2
- 3
- 4

Reveal Solution

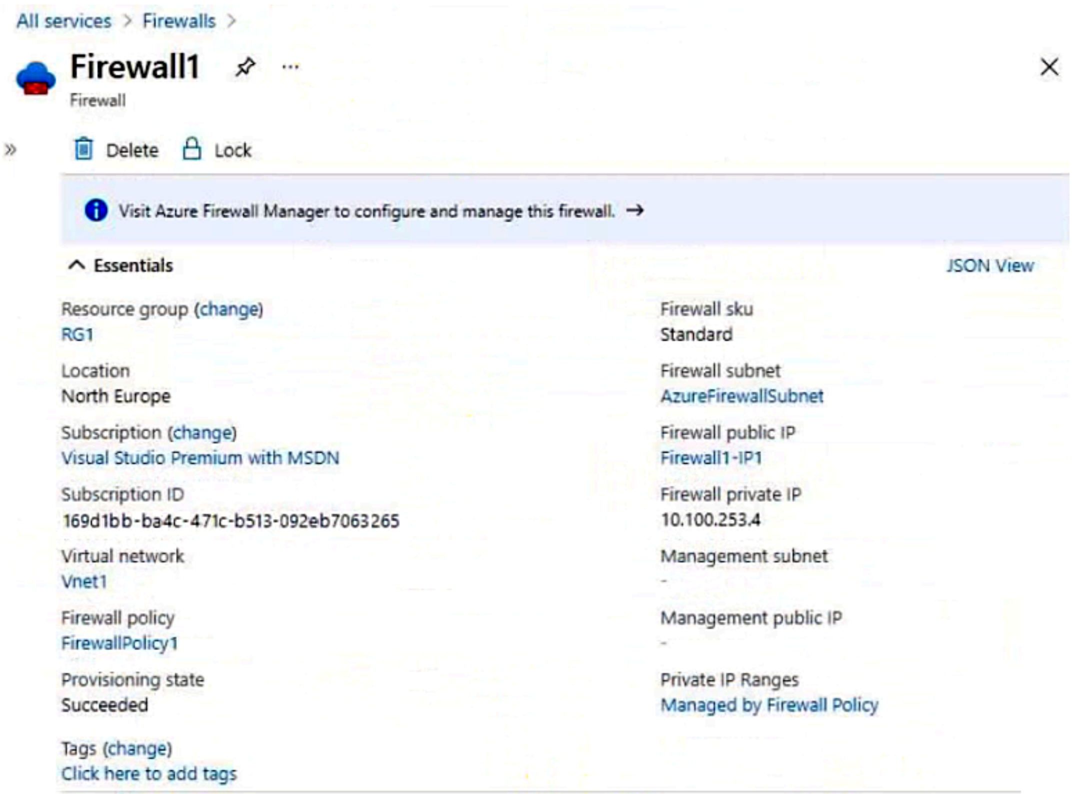
Discussion 4

Question #33 Topic 4

HOTSPOT

-

You have the Azure firewall shown in the following exhibit.



All services > Firewalls >

Firewall1

Firewall

Delete Lock

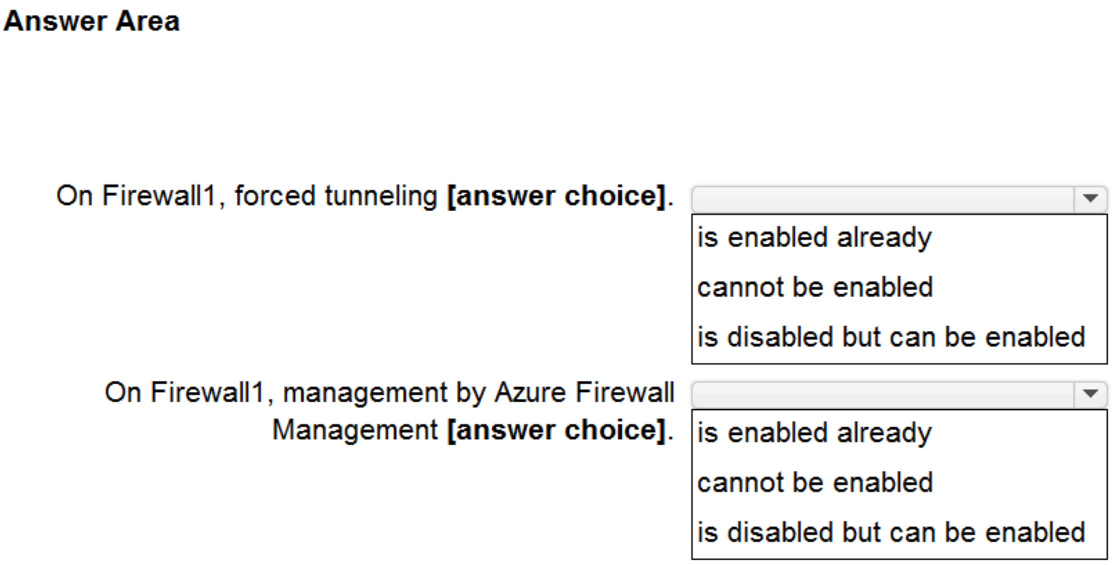
Visit Azure Firewall Manager to configure and manage this firewall. →

Essentials JSON View

Resource group (change) RG1	Firewall sku Standard
Location North Europe	Firewall subnet AzureFirewallSubnet
Subscription (change) Visual Studio Premium with MSDN	Firewall public IP Firewall1-IP1
Subscription ID 169d1bb-ba4c-471c-b513-092eb7063265	Firewall private IP 10.100.253.4
Virtual network Vnet1	Management subnet -
Firewall policy FirewallPolicy1	Management public IP -
Provisioning state Succeeded	Private IP Ranges Managed by Firewall Policy
Tags (change) Click here to add tags	

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

On Firewall1, forced tunneling **[answer choice]**.
- is enabled already
- cannot be enabled
- is disabled but can be enabled

On Firewall1, management by Azure Firewall Management **[answer choice]**.
- is enabled already
- cannot be enabled
- is disabled but can be enabled

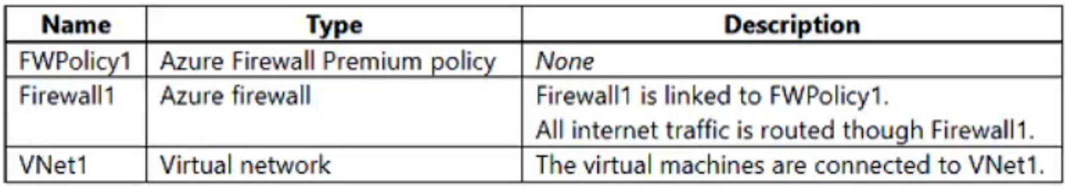
Reveal Solution Discussion 7

Question #34 Topic 4

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.



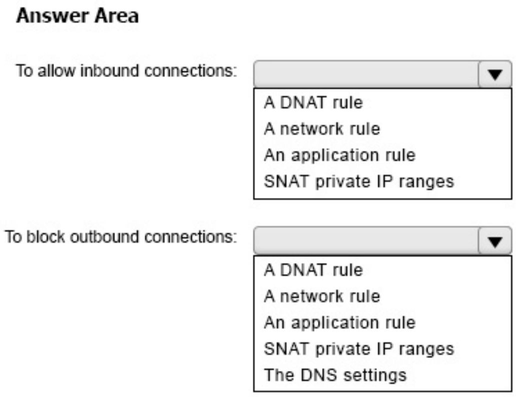
Name	Type	Description
FWPolicy1	Azure Firewall Premium policy	*None*
Firewall1	Azure firewall	Firewall1 is linked to FWPolicy1. All internet traffic is routed though Firewall1.
VNet1	Virtual network	The virtual machines are connected to VNet1.

You need to configure FWPolicy1 to meet the following requirements:

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



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

Reveal Solution Discussion 9

Question #35 Topic 4

DRAG DROP

-

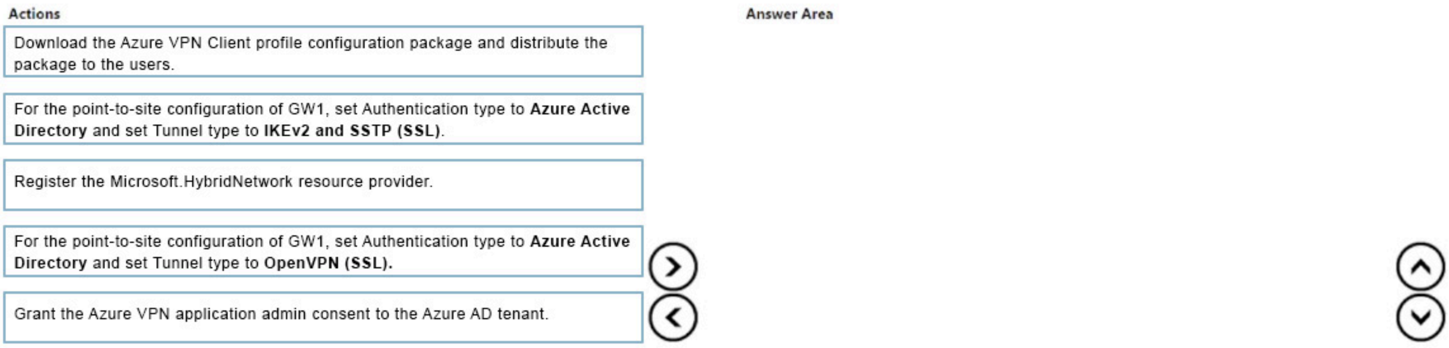
You have an Azure subscription that contains an Azure VPN gateway named GW1. GW1 provides Point-to-Site (P2S) VPN connectivity.

Users connect to GW1 from a Windows 11 device by using an SSTP connection.

You need to ensure that the P2S VPN connections support Azure AD 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 any of the correct orders you select.



Actions

- Download the Azure VPN Client profile configuration package and distribute the package to the users.
- For the point-to-site configuration of GW1, set Authentication type to **Azure Active Directory** and set Tunnel type to **IKEv2 and SSTP (SSL)**.
- Register the Microsoft.HybridNetwork resource provider.
- For the point-to-site configuration of GW1, set Authentication type to **Azure Active Directory** and set Tunnel type to **OpenVPN (SSL)**.
- Grant the Azure VPN application admin consent to the Azure AD tenant.

Answer Area

Reveal Solution Discussion 4

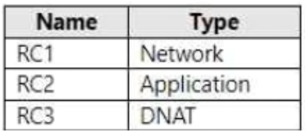
Question #36 *Topic 4*

DRAG DROP

-

You have an Azure subscription that contains an Azure Firewall Premium policy named FWP1.

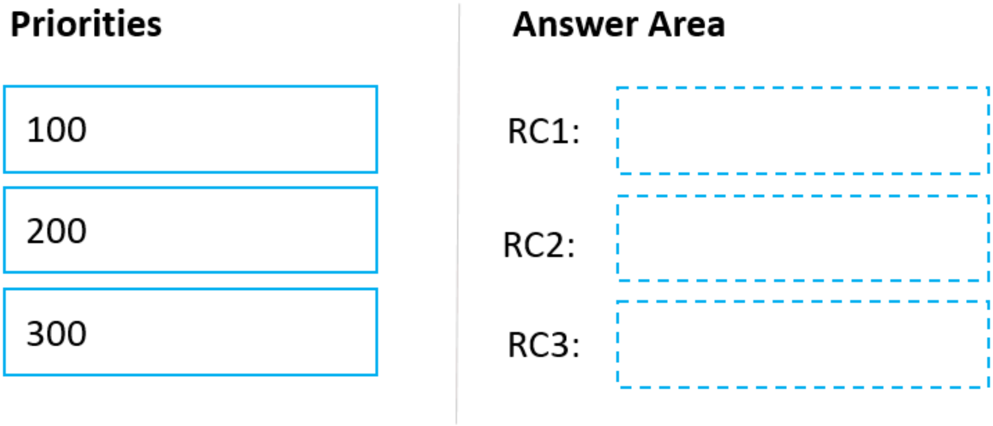
To FWP1, you plan to add the rule collections shown in the following table.



Name	Type
RC1	Network
RC2	Application
RC3	DNAT

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:

Reveal Solution | Discussion 3

Question #37 *Topic 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 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

Reveal Solution | Discussion 2

Question #38 *Topic 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 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

Reveal Solution Discussion 1

Question #39 *Topic 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 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 custom rule for WAF1.

Does this meet the goal?

A. Yes

B. No

Reveal Solution Discussion 2

Question #40 *Topic 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 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

Reveal Solution Discussion 1

Question #41 *Topic 4*

HOTSPOT
-

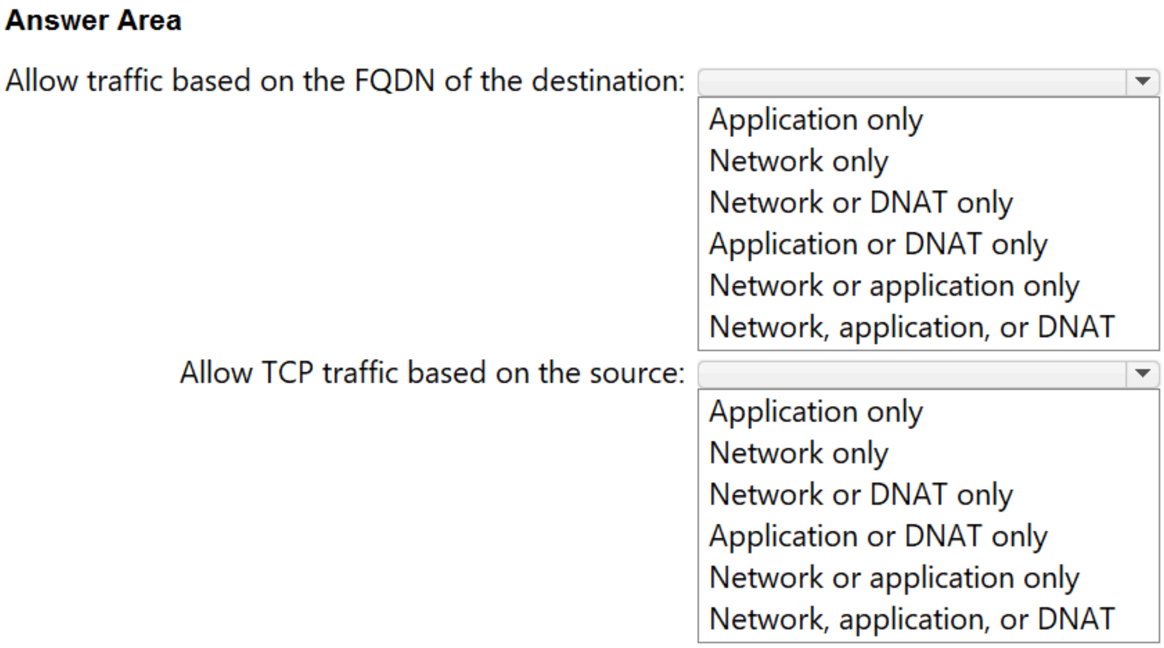
You have an Azure subscription that contains an Azure Firewall policy named FWPolicy1.

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

Allow traffic based on the FQDN of the destination:

- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Allow TCP traffic based on the source:

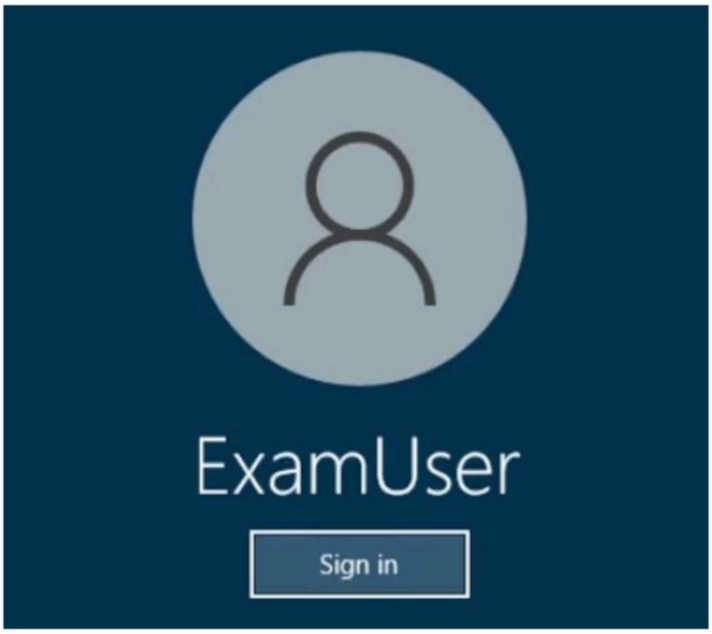
- Application only
- Network only
- Network or DNAT only
- Application or DNAT only
- Network or application only
- Network, application, or DNAT

Reveal Solution

Discussion 2

Question #42 *Topic 4*

SIMULATION
-



Username and password
-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx
-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678
-

You need to block all outbound internet traffic for HTTP and HTTPS that originates from subnet1-1. All other traffic must be allowed.

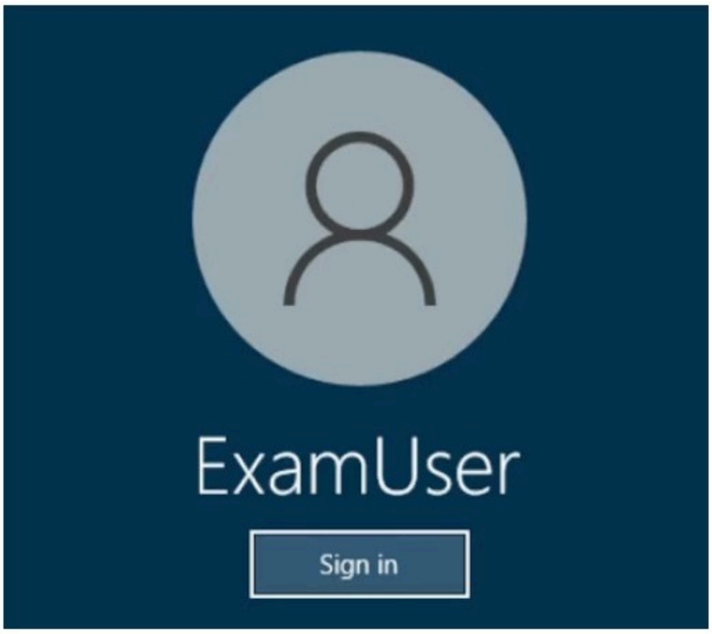
To complete this task, sign in to the Azure portal.

Reveal Solution Discussion 2

Question #43 *Topic 4*

SIMULATION

-



Username and password

-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx

-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the
portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

-

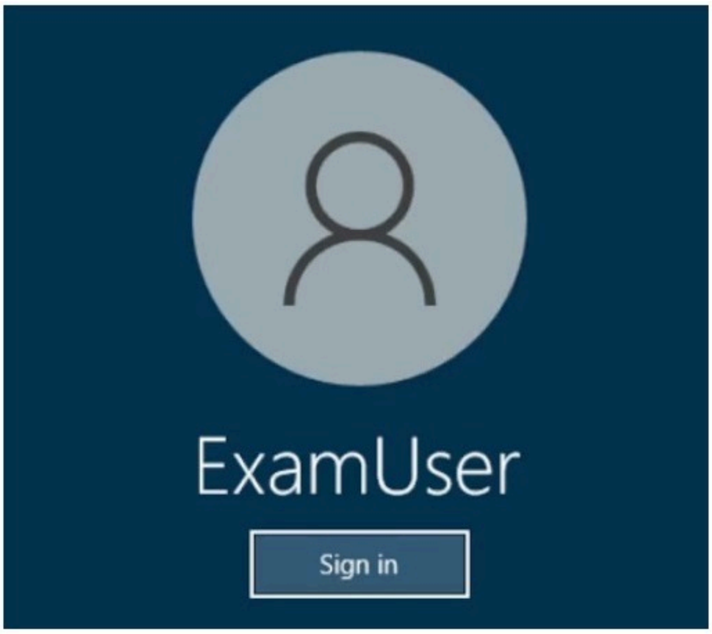
You need to restrict access to the storage35433841 storage account to ensure that only subnet1-2 can access the account.

To complete this task, sign in to the Azure portal.

Reveal Solution Discussion

Question #44 *Topic 4*

SIMULATION
-



Username and password
-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx
-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678
-

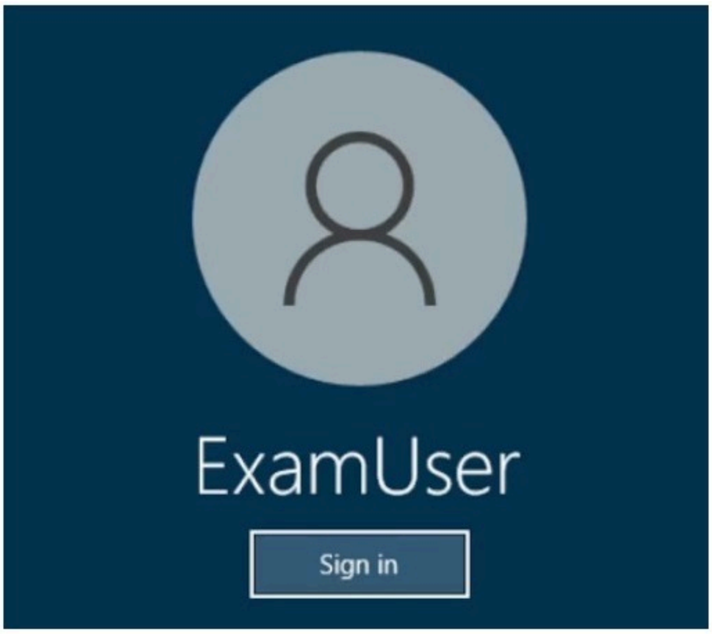
You need to ensure that subnet3-2 can only access resources on subnet3-1.

To complete this task, sign in to the Azure portal.

Reveal Solution Discussion

Question #45 *Topic 4*

SIMULATION
-



Username and password
-

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User-12345678@cloudslice.onmicrosoft.com

Azure Password: xxxxxxxxxx
-

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678
-

You are planning security for Azure Front Door.

You need to create a rule that can be applied to Front Door hosts. The rule must prevent hosts in Japan from making more than 50 requests per minute. You do NOT need to associate the rule to a Front Door instance to complete this task.

To complete this task, sign in to the Azure portal.

Reveal Solution Discussion

Question #46 *Topic 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 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

Reveal Solution Discussion 1

Question #47 *Topic 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 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 Firewall.

Does this meet the requirement?

A. Yes
B. No

Reveal Solution Discussion 2

Question #48 *Topic 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 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 NAT Gateway.

Does this meet the requirement?

A. Yes
B. No

Reveal Solution Discussion 1

Previous Questions

Next Questions