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

Viewing page **7** out of 10 pages.
Viewing questions 163-189 out of 267 questions

Custom View Settings

Question #53 *Topic 3*

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 service tag rule for AzureCloud.

B. Deploy an Azure Standard Load Balancer that has an outbound NAT rule.

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

D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

Hide Solution Discussion 4

Correct Answer: *C*

Community vote distribution
C (100%)

Question #54 *Topic 3*

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 machine operating systems were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

A. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

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

C. Deploy a NAT gateway.

D. Deploy an application security group that allows outbound traffic to 1688.

Hide Solution | Discussion 2

Correct Answer: *B*

Question #55 *Topic 3*

DRAG DROP
-

You have an Azure subscription.

You plan to deploy Azure Front Door with Azure Web Application Firewall (WAF).

You plan to implement custom rules and managed rules that meet the following requirements:

• Block malicious bots.
• Throttle client IP addresses that exceed 100 connections per minute.

You need to identify which Front Door SKU to configure, and which type of rule to configure for each requirement. The solution must minimize administrative effort and costs.

What should you identify? To answer, drag the appropriate options to the correct targets. Each option 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.

Options

- A custom rule
- A managed rule
- Classic
- Premium
- Standard

Answer Area

SKU:	Option
Block malicious bots:	Option
Throttle client IP addresses:	Option

Hide Solution | Discussion 4

Correct Answer:

Answer Area

SKU:	Premium
Block malicious bots:	A managed rule
Throttle client IP addresses:	A custom rule

Question #56 *Topic 3*

HOTSPOT
-

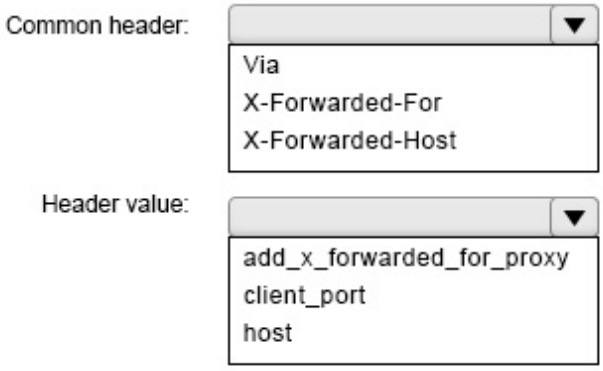
You have an Azure application gateway.

You need to create a rewrite rule that will remove the origin port from the HTTP header of incoming requests that are being forwarded to the backend pool.

How should you configure each setting? To answer, select the appropriate options in the answer area.

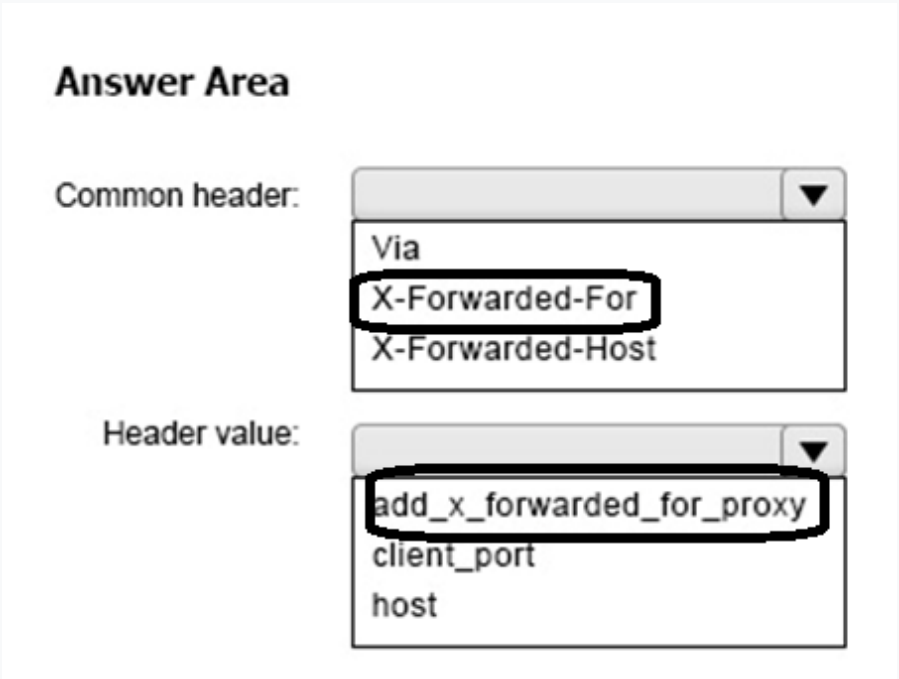
NOTE: Each correct selection is worth one point.

Answer Area



Hide Solution | Discussion 1

Correct Answer:



Question #57 *Topic 3*

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 machine operating systems were activated.

You need to ensure that the virtual machines can be activated.

What should you do?

A. On FW1, create an outbound service tag rule for AzureCloud.

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

C. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

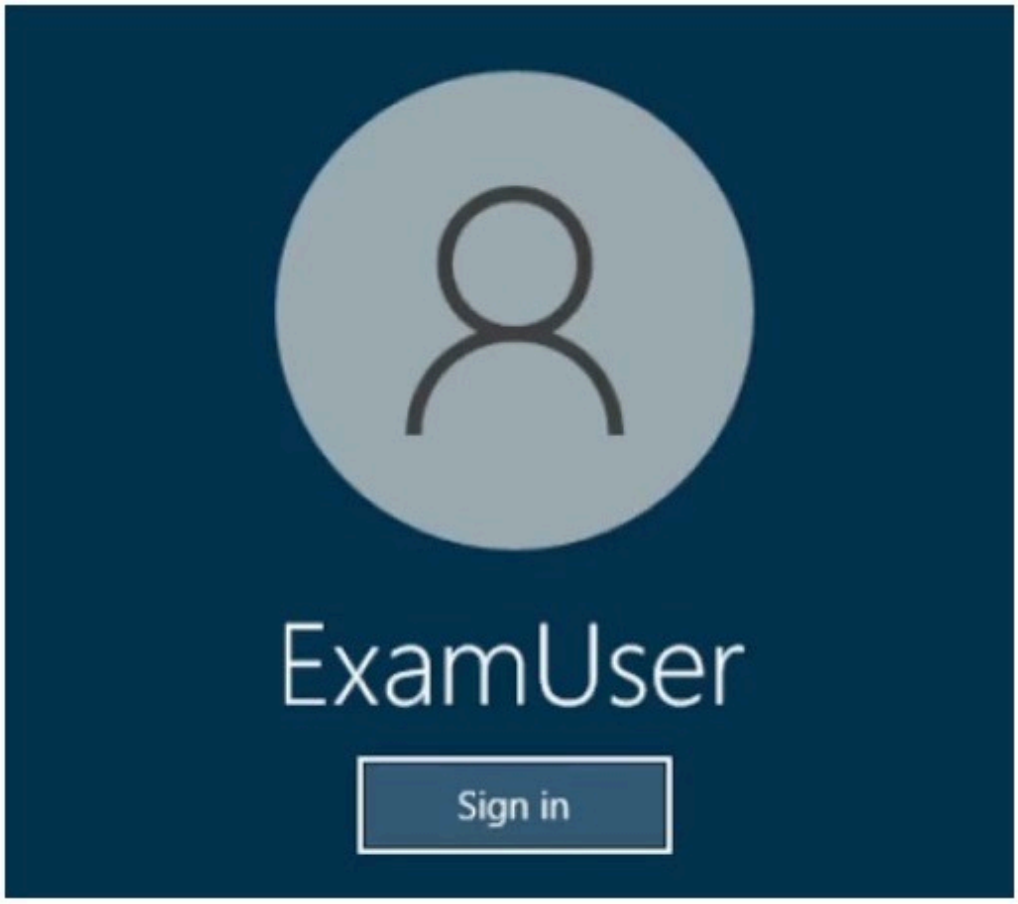
D. Deploy an application security group that allows outbound traffic to 1688.

Hide Solution | Discussion 1

Correct Answer: *B*

Question #58 *Topic 3*

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 traffic to host.fabrikam.com is directed to the Traffic Manager profile.

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

Hide Solution | Discussion 1

Correct Answer:

Manage an Azure Traffic Manager profile
Traffic Manager profiles use traffic-routing methods to control the distribution of traffic to your cloud services or website endpoints.

Add Traffic Manager endpoint

Step 1: In the portal's search bar, search for the Traffic Manager. Select the profile in the results that are displayed.

Step 2: In Traffic Manager profile, in the Settings section, select Endpoints > Add.

Step 3: Enter or select the following information. Accept the defaults for the other settings, and then select OK.

Setting Value
Type: Enter the Azure endpoint.
Name: Enter myEndpoint.
Target resource type: Select Host name.
Target resource: host.fabrikam.com
Weight Enter 100.

Step 4: When the addition of the endpoints is complete, it is displayed in the Traffic Manager profile along with its monitoring status as Online.

Reference:
https://learn.microsoft.com/en-us/azure/traffic-manager/tutorial-traffic-manager-weighted-endpoint-routing

Topic 4 - Question Set 4

Question #1 *Topic 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 **Most Voted**

E. blob storage and a premium storage account only

F. a premium storage account only

Hide Solution | Discussion 11

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

Community vote distribution
D (88%) 13%

Question #2 *Topic 4*

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

Name	IP address space
AzureFirewallSubnet	192.168.1.0/24
Subnet2	192.168.2.0/24

You deploy an Azure firewall to AzureFirewallSubnet. You route all traffic from Subnet2 through the firewall.
You need to ensure that all the hosts on Subnet2 can access an external site located at https://*.contoso.com.
What should you do?

A. In a firewall policy, create a DNAT rule.

B. Create a network security group (NSG) and associate the NSG to Subnet2.

C. In a firewall policy, create a network rule.

D. In a firewall policy, create an application rule. **Most Voted**

Hide Solution | Discussion 18

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

Community vote distribution
D (100%)

Question #3 *Topic 4*

You have an Azure Web Application Firewall (WAF) policy in prevention mode that is associated to an Azure Front Door instance.
You need to configure the policy to meet the following requirements:
- Log all connections from Australia.
- Deny all connections from New Zealand.
- Deny all further connections from a network of 131.107.100.0/24 if there are more than 100 connections during one minute.

What is the minimum number of objects you should create?

A. three custom rules that each has one condition **Most Voted**

B. one custom rule that has three conditions

C. one custom rule that has one condition

D. one rule that has two conditions and another rule that has one condition

Hide Solution | Discussion 21

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

Community vote distribution
A(100%)

Question #4 *Topic 4*

You have an Azure subscription that contains multiple virtual machines in the West US Azure region.
You need to use Traffic Analytics.
Which two resources should you create? Each correct answer presents part of the solution.
(Choose two.)
NOTE: Each correct answer selection is worth one point.

A. an Azure Monitor workbook
B. a Log Analytics workspace **Most Voted**
C. a storage account **Most Voted**
D. an Azure Sentinel workspace
E. an Azure Monitor data collection rule

Hide Solution | Discussion 4

Correct Answer: *BC*
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

Community vote distribution
BC (100%)

Question #5 *Topic 4*

HOTSPOT -
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Connected to
VM1	Vnet1/Subnet1
VM2	Vnet1/Subnet2

Subnet1 and Subnet2 are associated to a network security group (NSG) named NSG1 that has the following outbound rule:
- Priority: 100
- Port: Any
- Protocol: Any
- Source: Any
- Destination: Storage
- Action: Deny

You create a private endpoint that has the following settings:
- Name: Private1
- Resource type: Microsoft.Storage/storageAccounts
- Resource: storage1
- Target sub-resource: blob
- Virtual network: Vnet1
- Subnet: Subnet1

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
From VM2, you can create a container in storage1	○	○
From VM1, you can upload data to a blob storage container in storage1	○	○
From VM2, you can upload data to a blob storage container in storage1	○	○

Hide Solution Discussion 66

Correct Answer:

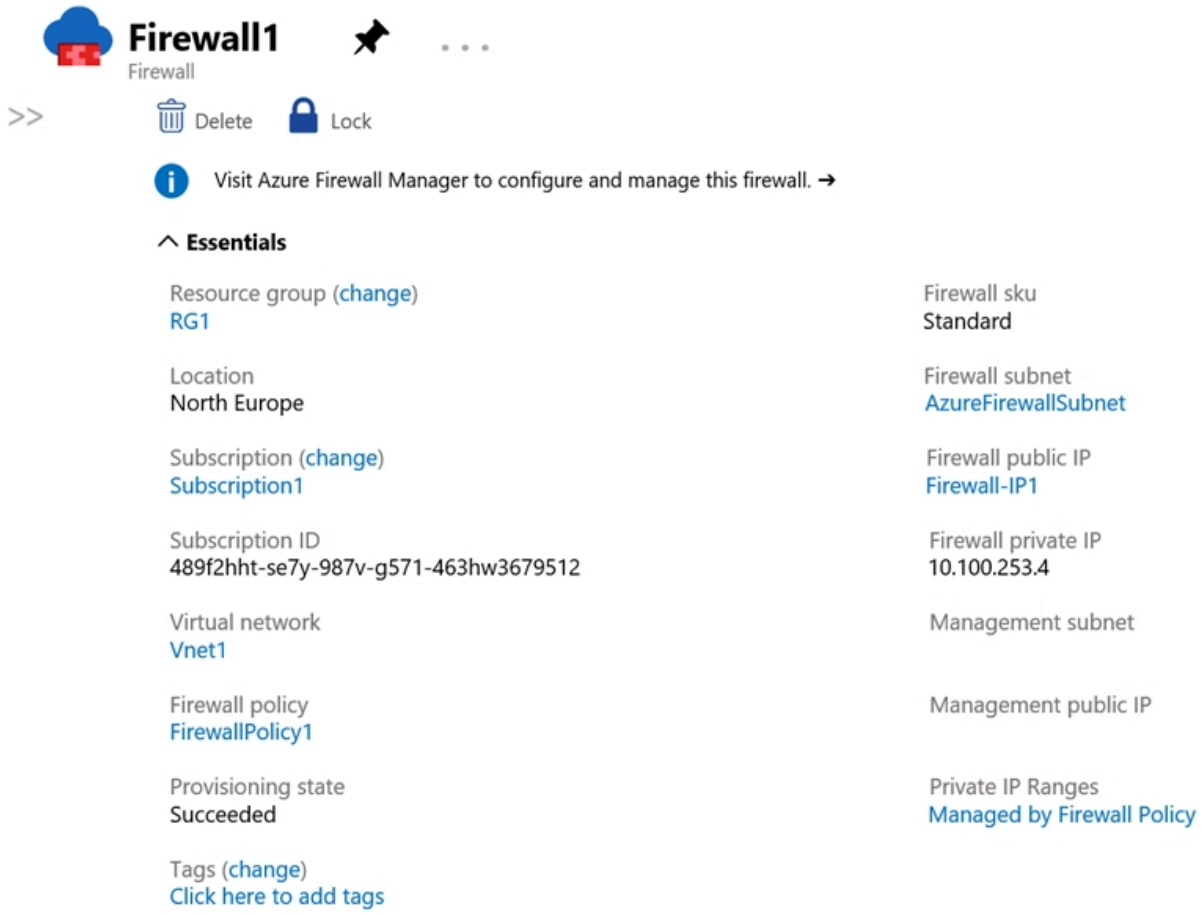
Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1	○	◉
From VM1, you can upload data to a blob storage container in storage1	◉	○
From VM2, you can upload data to a blob storage container in storage1	○	◉

Reference:
https://docs.microsoft.com/en-us/azure/private-link/disable-private-endpoint-network-policy

Question #6 *Topic 4*

HOTSPOT -
You have an Azure firewall shown in the following exhibit.



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.
Hot Area:

Answer Area

On Firewall1, forced tunneling **[answer choice]**

- is enabled already
- cannot be enabled
- is disabled but can be enabled

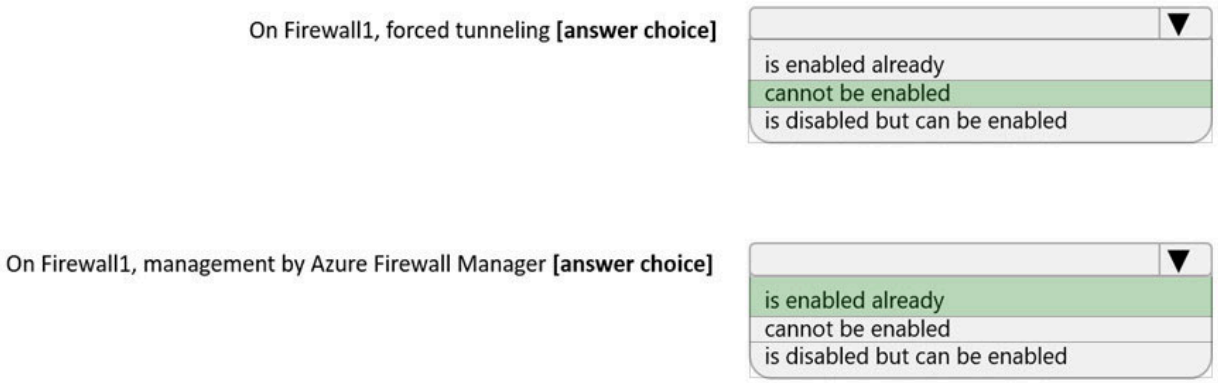
On Firewall1, management by Azure Firewall Manager **[answer choice]**

- is enabled already
- cannot be enabled
- is disabled but can be enabled

Hide Solution | Discussion 11

Correct Answer:

Answer Area



Box 1:
If forced tunneling was enabled, the Firewall Subnet would be named AzureFirewallManagementSubnet. Forced tunneling can only be enabled during the creation of the firewall. It cannot be enabled after the firewall has been deployed.
Box 2:
The ‚€Visit Azure Firewall Manager to configure and manage this firewall‚€ link in the exhibit shows that the firewall is managed by Azure Firewall Manager.

Question #7 *Topic 4*

You have a hybrid environment that uses ExpressRoute to connect an on-premises network and Azure.
You need to log the uptime and the latency of the connection periodically by using an Azure virtual machine and an on-premises virtual machine.
What should you use?

A. Azure Monitor
B. IP flow verify
C. Connection Monitor **Most Voted**
D. Azure Internet Analyzer

Hide Solution | Discussion 14

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor

Community vote distribution
C (100%)

Question #8 *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 service tag rule for AzureCloud.

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

C. Deploy a NAT gateway.

D. To Subnet1, associate a network security group (NSG) that allows outbound access to port 1688.

Hide Solution | Discussion 19

Correct Answer: *B*
Reference:
https://ryanmangansitblog.com/2020/05/11/firewall-considerations-windows-virtual-desktop-wvd/

Community vote distribution
B (100%)

Question #9 *Topic 4*

HOTSPOT -
You have an Azure application gateway named AppGW1 that provides access to the following hosts:

- www.adatum.com
- www.contoso.com
- www.fabrikam.com

AppGW1 has the listeners shown in the following table.

Name	Frontend IP address	Type	Host name
Listen1	Public	Multi site	www.contoso.com
Listen2	Public	Multi site	www.fabrikam.com
Listen3	Public	Multi site	www.adatum.com

You create Azure Web Application Firewall (WAF) policies for AppGW1 as shown in the following table.

Name	Policy mode	Custom rule		
		Priority	Condition	Association
Policy1	Prevention	50	If IP address does contain 131.107.10.15 then deny traffic.	Application gateway: AppGW1
Policy2	Detection	10	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen1
Policy3	Prevention	70	If IP address does contain 131.107.10.15 then allow traffic.	HTTP listener: Listen2

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
From 131.107.10.15, you can access www.contoso.com	◯	◯
From 131.107.10.15, you can access www.fabrikam.com	◯	◯
From 131.107.10.15, you can access www.adatum.com	◯	◯

Hide Solution Discussion 49

Correct Answer:

Answer Area

Statements	Yes	No
From 131.107.10.15, you can access www.contoso.com	◯	◯
From 131.107.10.15, you can access www.fabrikam.com	◯	◯
From 131.107.10.15, you can access www.adatum.com	◯	◯

Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/per-site-policies

Question #10 *Topic 4*

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 **Most Voted**

B. a service endpoint policy

C. a subnet delegation

D. an application security group

Hide Solution | Discussion 22

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-portal

Community vote distribution
A(87%) 13%

Question #11 *Topic 4*

Your company has offices in Montreal, Seattle, and Paris. The outbound traffic from each office originates from a specific public IP address.
You create an Azure Front Door instance named FD1 that has Azure Web Application Firewall (WAF) enabled. You configure a WAF policy named Policy1 that has a rule named Rule1. Rule1 applies a rate limit of 100 requests for traffic that originates from the office in Montreal.
You need to apply a rate limit of 100 requests for traffic that originates from each office.
What should you do?

A. Modify the rate limit threshold of Rule1.

B. Create two additional associations.

C. Modify the conditions of Rule1. **Most Voted**

D. Modify the rule type of Rule1.

Hide Solution | Discussion 23

Correct Answer: *C*

Community vote distribution

C (88%) 12%

Question #12 *Topic 4*

You have an Azure virtual network named Vnet1.
You need to ensure that the virtual machines in Vnet1 can access only the Azure SQL resources in the East US Azure region. The virtual machines must be prevented from accessing any Azure Storage resources.
Which two outbound network security group (NSG) rules should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a deny rule that has a source of VirtualNetwork and a destination of Sql

B. an allow rule that has the IP address range of Vnet1 as the source and destination of Sql.EastUS **Most Voted**

C. a deny rule that has a source of VirtualNetwork and a destination of 168.63.129.0/24

D. a deny rule that has the IP address range of Vnet1 as the source and destination of Storage **Most Voted**

Hide Solution | Discussion 13

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

Community vote distribution
BD (95%) 5%

Question #13 *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 the following resources:

- A virtual network named Vnet1
- A subnet named Subnet1 in Vnet1
- A virtual machine named VM1 that connects to Subnet1
- Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You configure the firewall on storage1 to only accept connections from Vnet1.

Does this meet the goal?

A. Yes

B. No **Most Voted**

Hide Solution | Discussion 8

Correct Answer: *B*

Community vote distribution

B (100%)

Question #14 *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 the following resources:

- A virtual network named Vnet1
- A subnet named Subnet1 in Vnet1
- A virtual machine named VM1 that connects to Subnet1
- Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.

Solution: You create a network security group (NSG) and associate the NSG to Subnet1.

Does this meet the goal?

A. Yes **Most Voted**

B. No **Most Voted**

Hide Solution | Discussion 22

Correct Answer: *B*

Community vote distribution

B (84%) A (16%)

Question #15 *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 the following resources:
- A virtual network named Vnet1

A subnet named Subnet1 in Vnet1 -

- A virtual machine named VM1 that connects to Subnet1
- Three storage accounts named storage1, storage2, and storage3

You need to ensure that VM1 can access storage1. VM1 must be prevented from accessing any other storage accounts.
Solution: You create a network security group (NSG). You configure a service tag for Microsoft.Storage and link the tag to Subnet1.
Does this meet the goal?

A. Yes

B. No **Most Voted**

Hide Solution | Discussion 5

Correct Answer: *B*

Community vote distribution

B (100%)

Question #16 *Topic 4*

You need to use Traffic Analytics to monitor the usage of applications deployed to Azure virtual machines.
Which Azure Network Watcher feature should you implement first?

A. NSG flow logs **Most Voted**

B. IP flow verify

C. Connection monitor

D. Packet capture

Hide Solution | Discussion 6

Correct Answer: *A*
Network Watcher: A regional service that enables you to monitor and diagnose conditions at a network scenario level in Azure. You can turn NSG flow logs on and off with Network Watcher.
Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG.
Why use NSG Flow Logs?
It is vital to monitor, manage, and know your own network for uncompromised security, compliance, and performance.
Common use cases include Network Monitoring: Identify unknown or undesired traffic. Monitor traffic levels and bandwidth consumption. Filter flow logs by IP and port to understand application behavior.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview

Community vote distribution
A(100%)

Question #17 *Topic 4*

HOTSPOT -
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Virtual network	Subnet	Workload
SQL1	VNet1	Subnet1	Microsoft SQL Server 2019
Web1	VNet1	Subnet1	IIS
Web2	VNet1	Subnet2	IIS
SQL2	VNet2	Subnet1	Microsoft SQL Server 2019
Web3	VNet2	Subnet1	IIS
SQL3	VNet2	Subnet2	Microsoft SQL Server 2019

VNet1 and VNet2 are NOT connected to each other.
You need to block traffic from SQL Server 2019 to IIS by using application security groups. The solution must minimize administrative effort.
How should you configure the application security groups? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area:

Minimum number of application security groups:

1
2
3
6

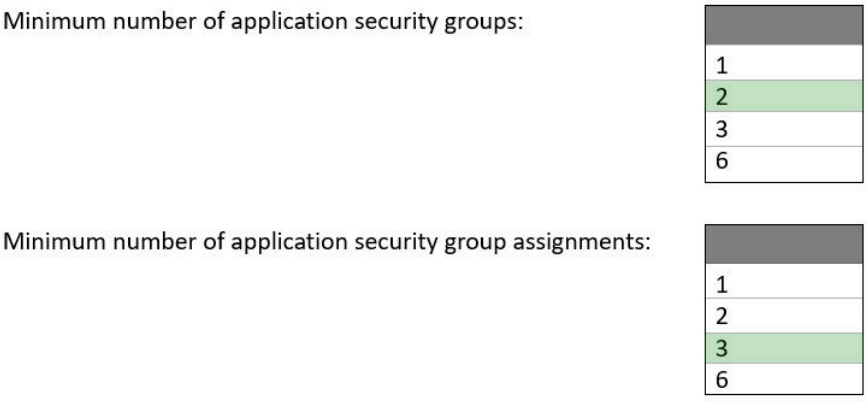
Minimum number of application security group assignments:

1
2
3
6

Hide Solution Discussion 30

Correct Answer:

Answer Area:



Box 1: 2 -
All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.
We need one application security group for each of the two virtual networks.

Box 2: 3 -
One network assignment in VNet1. Two network assignments in VNET2.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups

Question #18 *Topic 4*

HOTSPOT -
You have an Azure virtual network that contains the subnets 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

NSG2 has only the default rules configured.
You have the Azure virtual machines shown in the following table.

Name	Subnet
VM1	Subnet1
VM2	Subnet1
VM3	Subnet2

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
VM3 can connect to port 8080 on VM1.	○	○
VM1 and VM2 can connect on port 9090.	○	○
VM1 can connect to VM3 on port 9090.	○	○

Hide Solution | Discussion 44

Correct Answer:

Answer 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.	○	○

Box 1: Yes -
VM3 is Subnet2. NSG2 applies. The default rule will allow communication.

Box 2: No -
VM1 & 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

Question #19 *Topic 4*

You have the Azure virtual networks shown in the following table.

Name	Resource group	Location
Vnet1	RG1	East US
Vnet2	RG1	UK West
Vnet3	RG1	East US
Vnet4	RG1	UK West

You have the Azure resources shown in the following table.

Name	Type	Virtual network	Resource group	Location
VM1	Virtual machine	Vnet1	RG1	East US
VM2	Virtual machine	Vnet2	RG2	UK West
VM3	Virtual machine	Vnet3	RG3	East US
App1	App Service	Vnet1	RG4	East US
St1	Storage account	**Not applicable**	RG5	UK West

You need to check latency between the resources by using connection monitors in Azure Network Watcher.
What is the minimum number of connection monitors that you must create?

A. 1

B. 2 **Most Voted**

C. 3

D. 4

E. 5

Hide Solution | Discussion 26

Correct Answer: *C*
In the Region UK West region we have one single virtual machine VM2.
There is not anything to monitor here.
In the Region East US region we have two virtual machines VM1 & VM3, and App1.
We can monitor the connections: VM1-VM3, VM1-App1, VM3-App1.
Note: Connection Monitor includes the following entities:
Connection monitor resource: A region-specific Azure resource. All the following entities are properties of a connection monitor resource.
Endpoint: A source or destination that participates in connectivity checks. Examples of endpoints include Azure VMs, on-premises agents, URLs, and IP addresses.
Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/connection-monitor-overview

Community vote distribution
B (63%) C (26%) 9%

Question #20 *Topic 4*

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

RG1 contains an Azure Network Watcher instance named NW1.

You need to ensure that Admin1 can place a lock on NW1. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

A. User Access Administrator **Most Voted**

B. Resource Policy Contributor

C. Network Contributor

D. Monitoring Contributor

Hide Solution | Discussion 14

Correct Answer: *A*

Community vote distribution

A(71%) C (29%)

Question #21 *Topic 4*

You have a network security group named NSG1.

You need to enable network security group (NS) flow logs for NSG1. The solution must support retention policies.

What should you create first?

A. A standard general-purpose v2 Azure Storage account **Most Voted**

B. An Azure Log Analytics workspace

C. A standard general-purpose v1 Azure Storage account

D. A premium Block blobs Azure Storage account

Hide Solution | Discussion 17

Correct Answer: *A*

Community vote distribution

A(78%) B (22%)