Correct Answer:

Values		Answer Area		
		Item	**Value**	
Web Application Firewall (WAF)				
Azure Application Gateway		Azure service	Azure Application Gateway	
Azure Load Balancer		Feature	Web Application Firewall (WAF)	
Azure Traffic Manager				
SSL offloading				
URL-based content routing				

QUESTION 115
You use a virtual network to extend an on-premises IT environment into the cloud. The virtual network has two virtual machines (VMs) that store sensitive data.

The data must only be available using internal communication channels. Internet access to those VMs is not permitted.

You need to ensure that the VMs cannot access the Internet.

Which two options should you recommend? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. network interface (NIC)
B. Source Network Address Translation (SNAT)
C. Azure ExpressRoute
D. Network Security Groups (NSG)

Correct Answer: CD

QUESTION 116
HOTSPOT
A company plans to implement an HTTP-based API to support a web app. The web app allows customers to check the status of their orders.
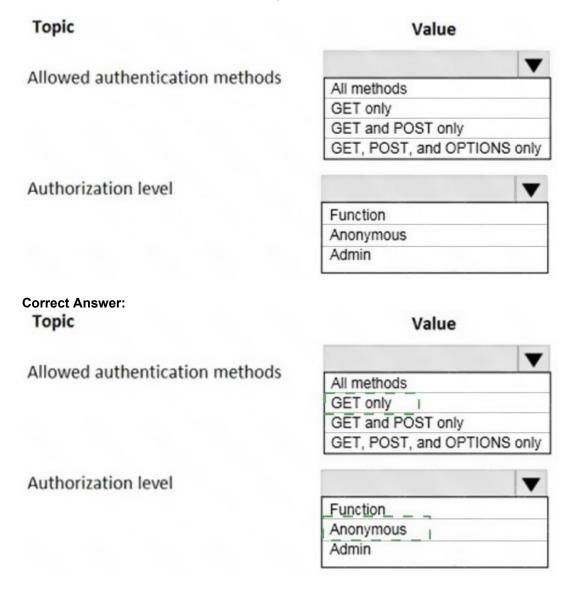
The API must meet the following requirements:

▪ Implement Azure Functions
▪ Provide public read-only operations
▪ Do not allow write operations

You need to recommend configuration options.

What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

Topic	Value
Allowed authentication methods	▼
	All methods
	GET only
	GET and POST only
	GET, POST, and OPTIONS only
Authorization level	▼
	Function
	Anonymous
	Admin

Correct Answer:

Topic	Value
Allowed authentication methods	▼
	All methods
	GET only
	GET and POST only
	GET, POST, and OPTIONS only
Authorization level	▼
	Function
	Anonymous
	Admin

QUESTION 117
Note: This question is part of 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.

A company has custom ASP.NET and Java applications that run old versions of Windows and Linux. The company plans to place applications in containers.

You need to design a solution that includes networking, service discovery, and load balancing for

the applications. The solution must support storage orchestration.

Solution: Deploy a Kubernetes cluster that has the desired number of instances of the applications.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Explanation:
Instead you should deploy each application to an Azure Container instance.

Note:
Docker Containers are the global standard and are natively supported in Azure, offering enterprises an interesting and flexible way to migrate legacy apps for both future proofing and cost benefits.

References:
https://docs.microsoft.com/en-us/dotnet/standard/modernize-with-azure-and-containers/modernize-existing-apps-to-cloud-optimized/deploy-existing-net-apps-as-windows-containers

QUESTION 118
You manage on-premises networks and Azure virtual networks.

You need a secure private connection between the on-premises networks and the Azure virtual networks. The connection must offer a redundant pair of cross connections to provide high availability.

What should you recommend?

A. ExpressRoute
B. Azure Load Balancer
C. virtual network peering
D. VPN Gateway

Correct Answer: A

QUESTION 119
Note: This question is part of 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.

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Explanation:
The Network Watcher Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.

Note:
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.

References:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

QUESTION 120
Note: This question is part of 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 are migrating an on-premises application to Azure. One component of the application is a legacy Windows native executable that performs image processing.

The image processing application must run every hour. During times that the image processing application is not running, it should not be consuming any Azure compute resources.

You need to ensure that the image processing application runs correctly every hour.

Solution: Create an Azure WebJob that runs the image processing application every hour.

Does the solution meet the goal?

A. Yes

B.   No

Correct Answer: B

QUESTION 121
You have an Azure subscription.

You need to recommend a solution to provide developers with the ability to provision Azure virtual machines.

The solution must meet the following requirements:

▪ Only allow the creation of the virtual machines in specific regions.
▪ Only allow the creation of specific sizes of virtual machines.

What should include in the recommendation?

A.   conditional access policies
B.   Azure Policy
C.   Azure Resource Manager templates
D.   role-based access control (RBAC)

Correct Answer: B

QUESTION 122
You manage a solution in Azure.

You must collect usage data including MAC addresses from all devices on the network.

You need to recommend a monitoring solution.

What should you recommend?

A.   Activity Log Analytics
B.   Azure Network Security Group Analytics
C.   Network Performance Monitor
D.   Azure Application Gateway Analytics
E.   Azure Wire Data

Correct Answer: B
Explanation:
A network security group (NSG) includes rules that allow or deny traffic to a virtual network subnet, network interface, or both. When you enable diagnostic logging for an NSG, you can log the following categories of information:

Event: Entries are logged for which NSG rules are applied to VMs, based on MAC address. The status for these rules is collected every 60 seconds.

Rule counter: Contains entries for how many times each NSG rule is applied to deny or allow traffic.

References:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log