Vendor: Microsoft

Exam Code: AZ-700

Exam Name: Designing and Implementing Microsoft Azure Networking Solutions

Version: DEMO

QUESTION 1
QUESTION 1
Case Study 1 - Litware. Inc

Overview
Litware. Inc. is a financial company that has a main datacenter in Boston and 20 branch offices across the United States. Users have Android, iOS, and Windows 10 devices.

Existing Environment:
Hybrid Environment
The on-prernises network contains an Active Directory forest named litwareinc.com that syncs to an Azure Active Directory (Azure AD) tenant named litwareinc.com by usinq Azure AD Connect. All the offices connect to a virtual network named Vnetl by using a Site-to-Site VPN connection.

Azure Environment
Litware has an Azure subscription named Sub1 that is linked to the litwareinc.com Azure AD tenant. Sub1 contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
Vnet1	Virtual network	Uses an IP address space of 192.168.0.0/20
GatewaySubnet	Virtual network subnet	Located in Vnet1 and uses an IP address space of 192.168.15.128/29
VPNGW1	VPN gateway	Deployed to Vnet1
Vnet2	Virtual network	Uses an IP address space of 192.168.16.0/20
SubnetA	Virtual network subnet	Located in Vnet2 and uses an IP address space of 192.168.16.0/24
Vnet3	Virtual network	Uses an IP address space of 192.168.32.0/20
cloud.litwareinc.com	Private DNS zone	**None**
VMScaleSet1	Virtual machine scale set	Contains four virtual machines deployed to SubnetA
VMScaleSet2	Virtual machine scale set	Contains two virtual machines deployed to SubnetA
storage1	Storage account	Has the public endpoint blocked
storage2	Storage account	Has the public endpoint blocked

A diagram of the resource in the East US Azure region is shown in the Network Diagram exhibit.

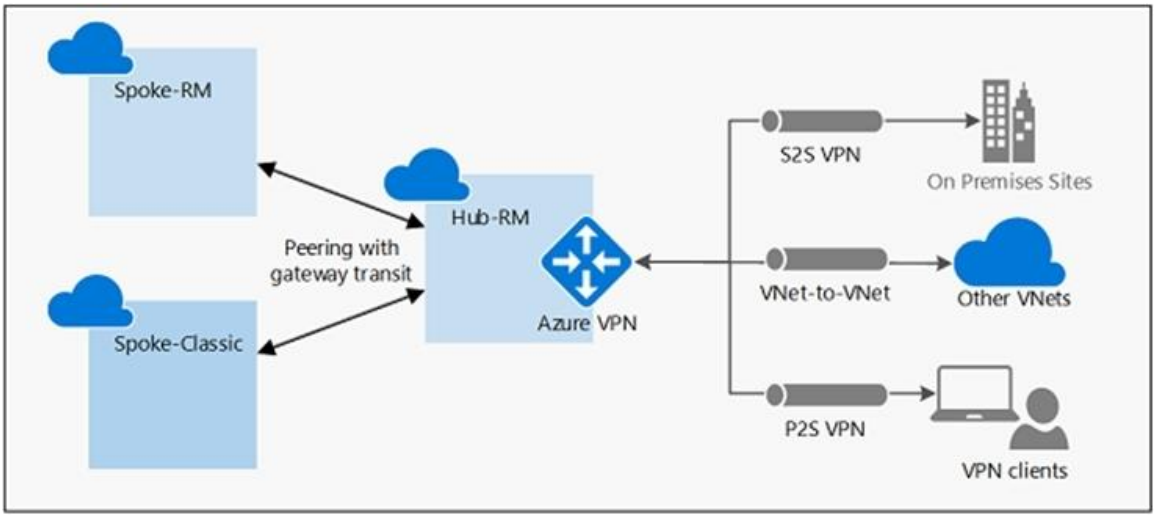
There is bidirectional peering between Vnet1 and Vnet2. There is bidirectional peering between Vnet1 and Vnet3. Currently, Vnet2 and Vnet3 cannot communicate directly.

You need to connect Vnet2 and Vnet3. The solution must meet the virtual networking requirements and the business requirements.
Which two actions should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. On the peerings from Vnet2 and Vnet3, select Use remote gateways.
B. On the peering from Vnet1, select Allow forwarded traffic.

C. On the peering from Vnet1, select Use remote gateways.
D. On the peering from Vnet1, select Allow gateway transit.
E. On the peerings from Vnet2 and Vnet3, select Allow gateway transit.

Answer: AD
Explanation:
Virtual network peering seamlessly connects two Azure virtual networks, merging the two virtual networks into one for connectivity purposes. 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,
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-peering-gateway-transit

QUESTION 2
Case Study 2 - Contoso, Ltd

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.

What should you implement to meet the virtual network requirements for the virtual machines that connect to Vnet4 and Vnet5?

A. a private endpoint
B. a virtual network peering
C. a private link service
D. a routing table
E. a service endpoint

Answer: B
Explanation:
There is no virtual network peering between VM4's VNet (VNet3) and VM5's VNet (VNet4). To enable the VMs to communicate over the Microsoft backbone network a VNet peering is required between VNet3 and VNet4.

QUESTION 3
You have an Azure subscription that contains the virtual networks shown in the following table.

Name	In resource group	Location
Vnet1	RG1	West US
Vnet2	RG1	Central US
Vnet3	RG2	Central US
Vnet4	RG2	West US
Vnet5	RG3	East US

You plan to deploy an Azure firewall named AF1 to RG1 in the West US Azure region.
To which virtual networks can you deploy AF1?

A. Vnet1 only
B. Vnet1 and Vnet2 only
C. Vnet1, Vnet2, and Vnet4 only
D. Vnet1 and Vnet4 only
E. Vnet1, Vnet2. Vnet3, and Vnet4

Answer: A
Explanation:
Azure Firewall operates in a single VNET.
Azure Firewall is a regional service.
Yes. Vnet1: Same VNET and same region.
No. Vnet2: Same Resource Group but different VNET and different region. Must be in the same region.
No. Vnet3: Different VNET, different region. Must be in the same region.
No. Vnet4: Different VNET, same region.
Reference:
https://docs.microsoft.com/en-us/azure/architecture/networking/guide/well-architected-framework-azure-firewall

QUESTION 4
You fail to establish a Site-to-Site VPN connection between your company's main office and an Azure virtual network.
You need to troubleshoot what prevents you from establishing the IPsec tunnel.
Which diagnostic log should you review?

A. IKEDiagnosticLog
B. GatewayDiagnosticLog
C. TunnelDiagnosticLog
D. RouteDiagnosticLog

Answer: A
Explanation:
IKEDiagnosticLog = The IKEDiagnosticLog table offers verbose debug logging for IKE/IPsec. This is very useful to review when troubleshooting disconnections, or failure to connect VPN scenarios.
GatewayDiagnosticLog = Configuration changes are audited in the GatewayDiagnosticLog table.
TunnelDiagnosticLog = The TunnelDiagnosticLog table is very useful to inspect the historical connectivity statuses of the tunnel.

RouteDiagnosticLog = The RouteDiagnosticLog table traces the activity for statically modified routes or routes received via BGP.
P2SDiagnosticLog = The last available table for VPN diagnostics is P2SDiagnosticLog. This table traces the activity for Point to Site.
https://docs.microsoft.com/en-us/azure/vpn-gateway/troubleshoot-vpn-with-azure-diagnostics

QUESTION 5
Your company has an on-premises network and three Azure subscriptions named Subscription1, Subscription2, and Subscription3.
The departments at the company use the Azure subscriptions as shown in the following table.

Department	Subscription
IT	Subscription1
Research	Subscription1
Development	Subscription2
Testing	Subscription2
Distribution	Subscription3

All the resources in the subscriptions are in either the West US Azure region or the West US 2 Azure region.
You plan to connect all the subscriptions to the on-premises network by using ExpressRoute.
What is the minimum number of ExpressRoute circuits required?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: A
Explanation:
Managing Authorization
The circuit owner can share a circuit with up to 10 Azure subscriptions. The circuit owner can view who has been authorized to the circuit. The owner can revoke the authorization at any time.
https://azure.microsoft.com/en-us/blog/enable-multiple-subscription-expressroute/#:~:text=The%20circuit%20owner%20can%20share,the%20authorization%20at%20any%20time.

QUESTION 6
You have the Azure resources shown in the following table.

Name	Type	Location	Description
storage1	Storage account	East US	Read-access geo-redundant storage (RA-GRS)
Vnet1	Virtual network	East US	Contains one subnet

You configure storage1 to provide access to the subnet in Vnet1 by using a service endpoint.
You need to ensure that you can use the service endpoint to connect to the read-only endpoint of storage1 in the paired Azure region.
What should you do first?

A. Configure the firewall settings for storage1.
B. Fail over storage1 to the paired Azure region.
C. Create a virtual network in the paired Azure region.
D. Create another service endpoint.

Answer: C
Explanation:
When planning for disaster recovery during a regional outage, you should create the VNets in the paired region in advance. Enable service endpoints for Azure Storage, with network rules granting access from these alternative virtual networks. Then apply these rules to your geo-redundant storage accounts.
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

QUESTION 7
You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The subscription contains the following resources:

```
- An Azure App Service app named App1
- An Azure DNS zone named contoso.com
- An Azure private DNS zone named private.contoso.com
- A virtual network named Vnet1
```

You create a private endpoint for App1. The record for the endpoint is registered automatically in Azure DNS.
You need to provide a developer with the name that is registered in Azure DNS for the private endpoint.
What should you provide?

A. app1.privatelink.azurewebsites.net
B. app1.contoso.com
C. app1.contoso.onmicrosoft.com
D. app1.private.contoso.com

Answer: A
Explanation:
When you use Private Endpoint for Web App, the requested URL must match the name of your Web App. By default mywebappname.azurewebsites.net.
By default, without Private Endpoint, the public name of your web app is a canonical name to the cluster. For example, the name resolution will be:

DNS
Name Type Value
mywebapp.azurewebsites.net CNAME clustername.azurewebsites.windows.net
clustername.azurewebsites.windows.net CNAME cloudservicename.cloudapp.net
cloudservicename.cloudapp.net A 40.122.110.154
When you deploy a Private Endpoint, we update the DNS entry to point to the canonical name mywebapp.privatelink.azurewebsites.net. For example, the name resolution will be:

DNS
Name Type Value Remark
mywebapp.azurewebsites.net CNAME mywebapp.privatelink.azurewebsites.net
mywebapp.privatelink.azurewebsites.net CNAME clustername.azurewebsites.windows.net
clustername.azurewebsites.windows.net CNAME cloudservicename.cloudapp.net
cloudservicename.cloudapp.net A 40.122.110.154

https://docs.microsoft.com/en-us/azure/app-service/networking/private-endpoint

QUESTION 8
You have an Azure subscription that contains the public IP addresses shown in the following table.

Name	IP version	SKU	IP address assignment
IP1	IPv4	Basic	Static
IP2	IPv4	Basic	Dynamic
IP3	IPv4	Standard	Static
IP4	IPv6	Basic	Dynamic
IP5	IPv6	Standard	Static

You plan to deploy a NAT gateway named NAT1.
Which public IP addresses can be used as the public IP address for NAT1?

A. IP3 and IP5 only
B. IP5 only
C. IP1, IP3, and IP5 only
D. IP3 only
E. IP2 and IP4 only

Answer: D
Explanation:
Only static IPv4 addresses in the Standard SKU are supported. IPv6 doesn't support NAT.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-overview

QUESTION 9
You have an Azure Front Door instance named FD1 that is protected by using Azure Web Application Firewall (WAF).
FD1 uses a frontend host named app1.contoso.com to provide access to Azure web apps hosted in the East US Azure region and the West US Azure region.
You need to configure FD1 to block requests to app1.contoso.com from all countries other than the United States.

What should you include in the WAF policy?

A. a frontend host association
B. a managed rule set
C. a custom rule that uses a rate limit rule
D. a custom rule that uses a match rule

Answer: D
Explanation:
Custom rules allow you to create tailored rules to suit the exact needs of your applications and security policies. Now, you can restrict access to your web applications by country/region. As with all custom rules, this logic can be compounded with other rules to suit the needs of your application.
To create a geo-filtering custom rule in the Azure portal, simply select Geo location as the Match Type, and then select the country/region or countries/regions you want to allow/block from your application.

QUESTION 10
Your company has offices in New York and Amsterdam. The company has an Azure subscription. Both offices connect to Azure by using a Site-to-Site VPN connection.
The office in Amsterdam uses resources in the North Europe Azure region. The office in New York uses resources in the East US Azure region.
You need to implement ExpressRoute circuits to connect each office to the nearest Azure region. Once the ExpressRoute circuits are connected, the on-premises computers in the Amsterdam office must be able to connect to the on-premises servers in the New York office by using the ExpressRoute circuits.
Which ExpressRoute option should you use?

A. ExpressRoute Local
B. ExpressRoute FastPath
C. ExpressRoute Direct
D. ExpressRoute Global Reach

Answer: D
Explanation:
With ExpressRoute Global Reach, you can link ExpressRoute circuits together to make a private network between your on-premises networks. In the above example, with the addition of ExpressRoute Global Reach, your San Francisco office (10.0.1.0/24) can directly exchange data with your London office (10.0.2.0/24) through the existing ExpressRoute circuits and via Microsoft's global network.
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach

QUESTION 11
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": "f7546159ylhjk7wal14568if5131t68h7",
   "policyId": "default",
   "policyScope": "Global",
   "poplicyScopeName": "Global",
 }
}
```


You need to ensure that the URL is accessible through the application gateway.

Solution: You configure a custom cookie and an exclusion rule.

Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
The log shows that WAF rule with ruleId 920300 was trigged. Instead we should disable the WAF rule that has a ruleId 920300.
Reference:
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-troubleshoot

QUESTION 12
Hotspot Question

You have an Azure private DNS zone named contoso.com that is linked to the virtual networks shown in the following table.

Name	IP address
Vnet1	10.1.0.0/16
Vnet2	10.2.0.0/16

The links have auto registration enabled.

You create the virtual machines shown in the following table.

Name	IP address
VM1	10.1.10.10
VM2	10.2.10.10
VM3	10.2.10.11

You manually add the following entry to the contoso.com zone:

```
- Name: VM1
- IP address: 10.1.10.9
```

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	◯	◯
Deleting VM1 will delete all VM1 records automatically	◯	◯
Changing the IP address of VM3 will update the DNS record of VM3 automatically	◯	◯

Answer:

Answer Area

Statements	Yes	No
VM2 will resolve vm1.contoso.com to 10.1.10.10	◯	◯
Deleting VM1 will delete all VM1 records automatically	◯	◯
Changing the IP address of VM3 will update the DNS record of VM3 automatically	◯	◯

Explanation:
Box 1: No
The manual DNS record will overwrite the auto-registered DNS record so VM1 will resolve to 10.1.10.9.

Box 2: No
The DNS record for VM1 is now a manually created record rather than an auto-registered record. Only auto-registered DNS records are deleted when a VM is deleted.

Box 3: No
This answer depends on how the IP address is changed. To change the IP address of a VM manually, you would need to select `Static' as the IP address assignment. In this case, the DNS record will not be updated because only DHCP assigned IP addresses are auto-registered.

Reference:
https://docs.microsoft.com/en-us/azure/dns/dns-faq-private

QUESTION 13
You have an Azure virtual network named Vnet1 that hosts an Azure firewall named FW1 and 150 virtual machines. Vnet1 is linked to a private DNS zone named contoso.com. All the virtual machines have their name registered in the contoso.com zone.

Vnet1 connects to an on-premises datacenter by using ExpressRoute.

You need to ensure that on-premises DNS servers can resolve the names in the contoso.com zone.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Modify the DNS server settings of Vnet1.
B. For FW1, configure custom DNS server.
C. For FW1, enable DNS proxy.
D. On the on-premises DNS servers, configure forwarders that point to the frontend IP address of FW1.
E. On the on-premises DNS servers, configure forwarders that point to the Azure provided DNS service at 168.63.129.16.

Answer: CD
Explanation:
Azure Firewall DNS proxy is an option to meet this DNS forwarding requirement, applicable with a hub-and-spoke model. To do this, configure your on-premises DNS server to conditionally forward requests to Azure Firewall for the required zone name. Ensure that your private DNS zone is linked to the Virtual Network within which the Azure Firewall resides. Configure Azure Firewall to use the default Azure DNS for lookups, and enable DNS proxy in Azure Firewall DNS settings.
https://azure.microsoft.com/en-us/blog/new-enhanced-dns-features-in-azure-firewall-now-generally-available/

QUESTION 14
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.
D. Modify the rule type of Rule1.

Answer: C
Explanation:
Rate limits are applied for each client IP address. If you have multiple clients accessing your Front Door from different IP addresses, they will have their own rate limits applied.
https://azure.microsoft.com/en-us/resources/templates/front-door-rate-limiting/

QUESTION 15
You have a hub-and-spoke topology. The topology includes multiple on-premises locations that connect to a hub virtual network in Azure via ExpressRoute circuits.
You have an Azure Application Gateway named GW1 that provides a single point of ingress from the internet.
You plan to migrate the hub-and-spoke topology to Azure Virtual WAN.
You need to identify which changes must be applied to the existing topology. The solution must ensure that you maintain a single point of ingress from the internet.
Which three changes should you include in the solution? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add user-defined routes.
B. Add virtual network peerings.
C. Replace the user-defined routes used by the current topology.
D. Create virtual network connections.
E. Remove the existing virtual network peerings.
F. Redeploy GW1.

Answer: CDE
Explanation:
Transition connectivity to virtual WAN hub:
Step 1. (E) Delete the existing peering connections from Spoke virtual networks to the old customer-managed hub. Access to applications in spoke virtual networks is unavailable until steps 1-3 are complete.
Step 2. (D) Connect the spoke virtual networks to the Virtual WAN hub via VNet connections.
Step 3. (C) Remove any user-defined routes (UDR) previously used within spoke virtual networks for spoke-to-spoke communications. This path is now enabled by dynamic routing available within the Virtual WAN hub.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**