2022 AZ-104: Configure and manage virtual networks for Azure administra tors

Study online at https://quizlet.com/_ar1njp

1. **What is a Azure Virtual Network (VNET)?:** A representation of your own network in the cloud. It is a logical isolation of the azure cloud dedicated to your subscription. It can be used to provision and manage VPNs, and link VNETs in azure to your on-prem networks for hybrid or cross-premises solutions. The CIDR blocks need to be unique
2. **What are the 5 IPs Azure reserves within each subnet?:** .0 for network address, .1 for default gateway, .2 and .3 for azure to map the azure dns ips to the VNet space, .255 network broadcast address
3. **What's the default limit on virtual networks per subscription per region?:** 50 before contacting azure support, you can then be limited to 500
4. **What are the two types of Azure IP addresses?:** Public and Private IP addresses
5. **If you allocate an ip address as dynamic in a network where 10.0.0.4-10.0.0.9 are already assigned resources, what ip will you be assigned?:** 10.0.0.10 Azure assigns the next available unassigned or unreserved ip address
6. **What is a Network Security Group (NSG)?:** A list of security rules that can be applied to a virtual network restricting inbound or outbound network traffic. Can be applied to a subnet or a network interface. Can be used multiple times.
7. **What are the default inbound security rules?:** Deny all inbound traffic except from the virtual network and azure load balancers.
8. **What are the default outbound security rules?:** Deny all outbound traffic except to the internet and the virtual network.
9. **How would you allow traffic on port 80 through your NSG?:** You need to dictate a subnet level Allow for port 80, all traffic is denied by default.
10. **What order are the NSGs evaluated?:** For inbound, the Subnet NSG is evaluated first and for outbound the NIC level is evaluated first.
11. **How do you see what security rules are being applied?:** Use the Effective security rules link.
12. **What info do you need to create an NSG rule?:** The service you are trying to manage, or a port that you are attempting to manage (this is filled in automatically if you select a service) finally a priority that the rule is applied. The value is between 100-4096.
13. **What is Azure Firewall?:** A Managed, cloud-based network security service that protects your azure virtual network resources. Its a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.
14. **What topology is recomended when deploying a firewall?:** A Hub-spoke network topology. The hub is the virtual network in azure that acts as a central point of connectivity. The spoke are the virtual networks that peer with the hub and can be

used to isolate networks. You can use ExpressRoute or a VPN gateway to connect from an on prem datacenter.

15. **What happens to traffic by default with Azure Firewall?:** By default, it blocks all traffic, you need to configure NAT rules, Network Rules, or Application rules to pass traffic.

16. **What are Network Address Translation (NAT) rules?:** It translates and filters inbound traffic to your subnets, each rule translates your firewalls public IP and port to a private IP and Port. This must be accompanied by a matching network rule to allow traffic.

17. **What are Network rules?:** Any non-http/s traffic that flows through the firewall needs this. You configure this rule for the source to the destination.

18. **What are Application rules?:** Define FQDNs that can be accessed from a subnet, like windows update network.

19. **What order are rules processed for packets?:** Network rules, then application rules.

20. **What is the format of the initial domain name created by your azure subscription?:** The name is Domainname.onmicrosoft.com. This is used until the custom domain name is verified.

21. **Can you delete the initial domain name?:** You cant. You can add a routable custom domain name you control. so you can change assign your domain name Contosogold.onmicrosoft.com to contosogold.com

22. **What needs to happen before your custom domain name is verified?:** You must verify ownership, by adding a DNS record, it can be MX or TXT. Once added Azure will query the dns domain for the presence of the record, it can take several minutes or several hours. Once it verifies the presence of the DNS record, it will add the domain name to the subscription.

23. **What is Azure DNS?:** A reliable, secure DNS service to manage and resolve domain names in a VNET without needing a custom DNS solution.

24. **What is a DNS zone?:** It hosts the DNS records for the domain, to start hosting your domain you need to create a DNS zone for that domain name, each DNS record for your domain is then created inside this DNS zone.

25. **What does it mean to Delegate DNS domains?:** When a dns server delegates authority over a part of its namespace to one or more other DNS servers.

26. **What do you need to delegate your domain in Azure DNS?:** You need to know the name servers names for your zone. Each time a DNS zone is created, Azure DNS allocates name servers from a pool and once they are assigned, azure DNS automatically creates authoritative NS records in your zone

27. **What's the easiest way to locate your name servers?:** In the azure portal, look for your DNS zone you created and it should list it there.
28. **Can you delegate a sub domain in azure?:** Yes! setting it up follows the same process as typical delegation, and the only difference is that NS (name server) records must be created in the parent zone rather than the domain registrar.
29. **What is a DNS record set?:** A collection of records in a zone that have the same name and are the same type.
30. **What does an A record require for you to use the Add record set page?:** A TTL and an ip address.
31. **What is TTL?:** How long a record is cached by clients before being re-queried.
32. **Can you view or retrieve DNS records for a private zone?:** No, but they are registered still and will resolve sucessfully.
33. **What is VNET Peering?:** It enables you to seamlessly connect two Azure virtual networks and makes them appear as one for connectivity purposes. This can be accomplished through regional VNet peering and Global VNet peering.
34. **What do you need to configure VNET Peering?:** You need to configure a VPN gateway as a transit point, and the peered virtual network uses the remote gateway to gain access to other resources.
35. **Is VNET peering is transitive?:** No, vnet 1 and 2 can have a connection along with vnet 2 and 3, but vnet 1 and 3 do not have a peering connection. You need to set up all peers yourself.
36. **How do you get around peering no being set up between all your networks?:** You create user defined routes. This lets you implement a multi level hub and spoke architecture and overcome the limit on the number of VNet peerings per virtual network.
37. **What status does VNET peering need to have to pass traffic?:** Status complete, not just initiated.
38. **What is a VPN gateway?:** A specific type of virtual network gateway that is used to send encrypted traffic between an azure virtual network and an on-premises location over the public internet.
39. **What is a Site to site connection?:** Connects on-premises datacenters to Azure virtual networks
40. **What is a VNet to Vnet connection?:** Connects azure virtual networks
41. **What is a Point to site (User VPN) connection?:** Connects individual devices to Azure virtual networks
42. **What are virtual network gateways comprised of?:** Two or more VMs that are deployed to a specific subnet you create called the gateway subnet. They contain

routing tables and run specific gateway services, and are created when you create the virtual network gateway. They cant be directly configured

43. **What are the steps to create a VNet to VNet connection?:** Create Vnets and subnets
Specify the DNS server (optional if you need name resolution)
Create the gateway subnet
Create the VPN gateway
Create the Local network gateway
Create the VPN connection

44. **What are some restrictions to the Gateway subnet?:** You should never deploy other resources to the gateway subnet. The gateway subnet must be named GatewaySubnet

45. **What configurations are available when creating the VPN gateway:** Gateway type (VPN or ExpressRoute)
VPN type (route based or policy based, the type is ased on the make and model of your VPN device and the kind of VPN connection you intend to create)
SKU
Generation
Virtual network

46. **What are the two types of VPN you can use for your VPN gateway: -** Route-based VPNs and Policy-based VPNs

47. **What is a Route-based VPN?:** Uses routes in the IP forwarding or routing table to direct packets to their corresponding tunnel interfaces

48. **What is a Policy-based VPN?:** Encrypts and directs packets through IPsec tunnels based on IPsec policies configured with the combinations of address prefixes between your on-premises network and the azure VNet. The policy is defined as an access list in the VPN device configuration

49. **What are the limitations of Policy based vpns?:** Can only be used on the basic gateway SKU
Only one tunnel
Can only use it for Site to Site connections and only for certain configurations

50. **What increases as you change gens and SKUs of gateways?:** Point to site IKEv2 connections and aggregate throughput benchmarks

51. **What info is used to create a local network gateway?:** The public IP address of the local gateway and the address ranges that define the local network's address space

52. **What do you need to configure your VPN device?:** A shared key that you specify when creating the connection.
The public IP address of your VPN gateway.
53. **What info do you configure when creating the connection between VPN gateways?:** Name, connection type, and Shared key
54. **What does azure do for VPN gateway high availability:** By default it creates two instances in an active-standby configuration that fails over automatically, for planned maintenance the connectivity should be restored within 15 seconds, for unplanned issues it can take up to 1 and a half minutes
55. **What is a active/active configuration?:** both instances of the gateway establish S2S (site to site) VPN tunnels to your on-premises VPN device. when in active active your traffic is routed through both tunnels simultaneously and planned or unplanned maintenance disconnects the tunnel and automatically switches from the affected instance to the active instance.
56. **What is Azure Expressroute?:** It lets you extend your on-premises networks into the Microsoft cloud over a private connection offering more reliability, faster speeds, and lower latencies. This keeps your connection off of the public internet
57. **What are the ways you can connect to ExpressRoute?:** Establishing connections to Azure at an ExpressRoute location such as an exchange provider facility. Or directly connect to azure from your WAN using a multiprotocol label switching (MPLS) VPN provided by a network service provider.
58. **What are ExpressRoute speeds?:** up to 100 Gbps
59. **How much Microsoft cloud services do you have access to with ExpressRoute?:** All regions within the geopolitical region are accessible, with ExpressRoute premium you can extend that connectivity past geopolitical boundaries with the exception of national clouds.
60. **How do your network gateways need to be configured to use Site-to-Site VPN as a secure failover path for ExpressRoute?:** You need to configure two virtual network gateways for the same virtual network (VNET), one using the gateway type VPN, and the other using the gateway type ExpressRoute
61. **What are the three ways to create a connection between your on-premises network and the Microsoft cloud?:** Co-located at a cloud exchange, point to point ethernet connections, Any-to-Any (IPVPN) networks
62. **What does it mean to be co-located at a cloud exchange?:** You order virtual cross connections to the microsoft cloud through the colocation provider's Ethernet exchange. They offer either layer 2 cross connections or managed layer 3 cross-connections between your infrastructure in the colocation facility and the Microsoft cloud

63. **What does it mean to have a point-to-point ethernet connection?:** You connect your on-prem datacenters/offices to the microsoft cloud through point-to-point ethernet links with either layer 2 or managed layer 3
64. **What does it mean to have a Any-to-any (IPVPN) network?:** You integrate your WAN with the Microsoft cloud. IPVPN providers, typically Multiprotocol Label Switching (MPLS) VPN, offer any to any connectivity between your branch offices and datacenters.
65. **What is the typical use case for a virtual network, point to site connection?-:** Dev, Test, and lab environments
66. **What is the typical use case for a virtual network, site to site connection?-:** Dev, test, and lab envrionments. Small scale production workloads and virtual machines
67. **What is the typical use case for a ExpressRoute connection?:** Enterprise-class and mission-critical workloads. Big data solutions
68. **What is Azure Virtual WAN?:** A networking service that provides optimized and automated branch connectivity to, and through, azure. It brings together man azure cloud connectivity services such as site-to-site VPN, User VPN, and ExpressRoute into a single operational interface.
69. **What are the two types of virtual wans?:** Basic for site-to-site VPN only, and Standard
70. **What are System routes?:** information to direct traffic between items in azure, the internet, and your on-prem networks. This info is recorded in a route table that contains a set of rules, called routes, that specifies how packets should be routed in a virtual network.
71. **What is an alternative to Azure automatically handling traffic routing?:** Using user defined routes (UDRs) you can control network traffic by defining routes that specify the next hop of the traffic flow. Each subnet can only be associated with a single route table.
72. **What info do you need to create a routing table?:** Name
Subscription
Resource Group
Location
You can chose to use Virtual network gateway route propagation, which automatically adds routes to the route table for all subnets. This is enabled by default.
73. **What information do you need to create a custom route?:** Route name
Address prefix
Next hop type
IP of hop

74. **What's the final step in implementing your custom route?:** Associate a subnet with the new routing table
75. **What does a service endpoint do?:** Provides the identity of your virtual network to the azure service. This eliminates the need for a public IP address
76. **Why use service endpoint?:** Improved Security for your Azure service resources

Optimal routing for Azure service traffic from your virtual network

Endpoints always take service traffic directly from your virtual network to the service on the Microsoft Azure backbone network

Simple to set up with less management overhead
77. **What is Azure private link?:** Private connectivity from a virtual network to azure platform as a service (PaaS), Customer-owned, or Microsoft partner services
78. **What are the benefits of Azure private link?:** Private connectivity to services on Azure
Integration with on-premises and peered networks
Protection against data exfiltration for azure resources
Services delivered directly to your customers' virtual networks
79. **What is the Azure Load balancer for?:** Delivers high availability and network performance to your applications. It distributes inbound traffic to backend resources using load-balancing rules and health probes.
80. **What are the two types of load balancers?:** Public and internal
81. **How does a public load balancer work?:** it maps the public IP address and port number of incoming traffic to the private IP addresses and port number of the VM
82. **How does a internal load balancer work?:** Directs traffic to resources that are inside a virtual network or that use a VPN to access azure infrastructure. Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint.
83. **What features do standard sku load balancers have that basic sku's dont?-:** up to 1000 instances vs 300

https health probes option

availability zones and zonal frontends

multiple front end option for outbound traffic

Secure by default that closes inbound flows unless allowed by an NSG

SLA of 99.99%
84. **What is a backend address pool?:** it contains the IP addresses of the virtual NICs that are connected to the load balancer for outputting traffic sent through it, your configuration changes by SKU
85. **What are the sku differences for the backend pool endpoints?:** Standard SKU lets you hit any virtual machine in a single virtual network, this includes a blend of virtual machines, availability sets, and virtual machine scale sets.

Basic SKU lets you hit a single availability sets or virtual machine scale sets.
86. **What is a load balancer rule?:** Defines how traffic is distributed to the backend pool. The rule maps a given frontend IP and port combination to a set of backend IP addresses and port combination. Can be used in combination with NAT Rules
87. **What kind of hash is used to map traffic with azure load balancing?:** five-tuple (source IP, source port, destination ip, destination port, and protocol type)
88. **What are the traffic behaviors you can configure with azure load balancing?:** None, Client IP, and Client IP and protocol. Client IP and Client IP and protocol specifies consecutive requests from the same IP or IP and protocol get handled by the same virtual machine.
89. **What are health probes for in azure load balancing?:** It monitors the status of an app, it dynamically adds or removes VMs from the load balancer rotation based on their response to health checks. You can use HTTP or TCP probes.
90. **What is azure application gateway?:** It manages the requests that client applications send to a web app
91. **What is application layer routing?:** It routes traffic to a pool of web servers based on the url of a request. the back end pool can contain azure vms, scale sets, app services, and even on-prem servers
92. **What OSI layer is azure application gateway?:** Layer 7 - Application
93. **What are the methods of routing traffic with azure app gateway?: -** Path-based routing and multiple site routing?
94. **What is path based routing?:** Sends requests with different URL paths to different pools of back end servers
95. **What is multiple site routing?:** You register multiple DNS names (CNAMEs) for the ip address of the application gateway, specifying the name of each site, then the gateway sends requests to listeners at each site, useful for multi tenant applications

96. **What are the components required to run Application gateway?:** Front-end ip addresses to receive client requests

Listeners to receive incoming requests and accepts it based on a combination of protocol, port, host, and ip, then routes to a back end pool based on your rules

Routing rules that specify how to interpret the hostname and path elements in the url of a request

Back end pools that are collections of web servers

Web application firewalls as an optional component that handles incoming requests before the reach a listener

Health probes to determine which servers are available for load balancing
97. **What do you do to control traffic between Azure subnets?:** You need to implement a network security group to deny communications between subnets. By default all subnets can communicate with each other.
98. **How do you prevent network issues when connecting your on prem network to azure?:** Identify the current IP address scheme used on-prem, there cant be overlap for interconnected networks or communication will stop. For example you can use 10.10.0.0/16 and 10.20.0.0/16 address spaces for on prem and azure because they don't overlap
99. **What ip ranges are the private network ip's and unrouteable over the internet?:** 10.0.0.0 to 10.255.255.255
172..16.0 to 172.231.255.255
192.168.0.1 to 192.168.255.255

or

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
100. **How do dynamic public ip addresses work in azure?:** They can change over the lifespan of the azure resource. it gets allocated when you create or start a VM, and released when you stop or delete the VM. This method is used by default and each azure region has a unique public IP pool

101. **How do static public ip addresses work in azure?:** they are assigned addresses that wont change over the lifespan of the azure resource. It only gets released when you delete the resource or change the IP allocation to dynamic
102. **What are the skus for public ip addresses?:** basic and standard, they offer different scale, features, and pricing for load balancing. Both have a default inbound idle timeout of 4 minutes and can be extended to 30 minutes along with a outbound flow idle timeout of 4 minutes
103. **What are the default settings for public ips in the basic sku?:** They are open and NSGs are recommended for security

They are available for inbound only traffic

Available when using instance meta data service (IDMS)

Dont support availability zones

Dont support routing preferences
104. **What are the default settings for public ips in the standard sku?:** Always use static allocation

Are secure and closed to inbound traffic, you need to enable it through an NSG

Are zone redundant and optionally zonal (glued to a specific zone)

Can be assigned to network interfaces, standard public load balancers, application gateways, or vpn gateways

Can be utilized with routing preference for more granular control of how traffic gets routed

Can be used as anycast frontend IPs for cross region load balancers
105. **What is a azure public ip address prefix?:** a reserved, static range of public IP addresses from a pool of available addresses unique to each region of the azure cloud
106. **How many addresses are reserved by default in azure?:** 3 addresses, along with the first and last ip addresses of all subnets. so .0 .1 .2 .3 and .255

107. **What are two questions to ask so you can discover the requirements of a network ip scheme?:** How many devices do you have on the network? and How many devices are you planning to add in the future?
108. **What is virtual network peering?:** a feature to directly connect azure virtual networks, when connected VMs can communicate with each other as if they were in the same network. It only uses private ip addresses and takes advantage of the high bandwidth and low latency of the azure backbone network.
109. **What are the two types of peering connections?:** Virtual network peering and global virtual network peering.
110. **what is reciprocal connections in virtual network peering?:** The concept that connecting two vnets together does not connect the entire set of networks together, you need to establish a peer with each vnet for the communication to occur
111. **Can you use virtual network peering when both networks are in different subscriptions?:** Yes, to allow administrators of different subscriptions to manage the other end of the peer they need to be granted the network contributor role on the virtual network
112. **Are virtual network peering connections transitive?:** No, Suppose, for example, that your three virtual networks (A, B, C) are peered like this: A <-> B <-> C. Resources in A can't communicate with resources in C because that traffic can't transit through virtual network B. If you need communication between virtual network A and virtual network C, you must explicitly peer these two virtual networks.
113. **How do you enable gateway transit?:** You can peer an on prem gateway to a virtual gateway hub network and all virtual devices are able to connect transitively because they are connected to that gateway and the gateway is peered with the prem
114. **Can IP addresses overlap when peering?:** No
115. **What is DNS?:** Its a protocol within the TCP/IP standard, it translates human readable domain names into a known ip address. can also be known as a name server
116. **How does DNS work?:** Maintains a local cache of recently accessed or used domain names and their IP addresses, And maintains a key value pair database of IP addresses and any host or subdomain the DNS server has authority over.
117. **What are some common record types created and used by DNS?:** A
CNAME
MX
TXT
118. **What is an A record in DNS?:** The host record, it maps domain or host names to IP addresses

119. **What is a CNAME record in DNS?:** A Canonical Name record that's used to create an alias from one domain name to another domain name
120. **What is a MX record in DNS?:** The mail exchange record, to map mail requests to your mail server on prem or in the cloud
121. **What is a TXT record in DNS?:** Its used to associate text strings with a domain name
122. **What records cant contain record sets?:** SOA and CNAME
123. **What is an SOA?:** Start of authority
124. **Why use Azure DNS to host your domain?:** Improved security
ease of use
private dns domains
alias record sets
125. **What are the security controls with Azure DNS?:** RBAC for fine grained control of access
Activity logs to track changes
Resource locking to control resource groups, subscriptions, or any azure resources
126. **What do private dns zones do?:** They provide name resolution for VMs within a virtual network and between virtual networks without having to create a custom DNS solution
127. **What do you need to host the domain name with Azure DNS?:** Create a DNS zone for the domain, It holds all the dns entries for your domain
128. **What is an apex domain?:** the highest level of your domain
129. **What can you use to link an apex domain with a load balancer?:** an alias record, you can enable an apex domain to reference other resources from the dns zone,
130. **How is routing controlled in azure?:** System routes, they are automatically created as you provision devices in azure and cant be created or delete. Only overridden through Custom routes.
131. **What hop types are available in system routes?:** Virtual network, internet (0.0.0.0/0 routes to anything), and none
132. **What is service chaining?:** Overriding configured routes to create user defined routes between virtual networks
133. **What options do you have for implementing custom routes?:** Creating user defined routes or using BGP (Border gateway protocol) to exchange routes between azure and on-premises networks.
134. **What is BGP (Border gateway protocol) used for?:** Exchanges routing and information among two networks

135. **How does azure chose between multiple routes in a route table?:** it uses the route with the longest prefix match, for example, 10.0.0.0/16 vs 10.0.0.0/24 azure would select /24 because its more specific
136. **What is an NVA (Network virtual appliance)?:** Virtual machines that control the flow of network traffic by controlling routing. Like Firewalls, a wan optimizer, application-delivery controllers, routers, load balancers, proxies, and an SD-WAN edge
137. **What is a NVA migrosegmentation approach?:** Deploying dedicated subnets for a firewall and deploying web apps and other services in other subnets, then all traffic is routed through the firewall and inspected by the NVAs
138. **What is an availability set?:** Protection from hardware failures within datacenters
139. **What is an availability zone?:** Protection from entire datacenter failure
140. **What is allowed with a basic load balancer?:** Port forwarding
Automatic reconfiguration
Health probes
Outbound connections through source network address translation (SNAT)
Diagnostics through azure log analytics for public-facing load balancers
Can only be used with availability sets
141. **What is allowed with standard load balancers?:** All basic load balancer features
HTTPS health probes
Availability zones
Diagnostics through azure monitor, for multidimentional metrics
High Availability (HA) ports
Outbound rules
A guarenteed SLA (99.99% for two or more virtual machines)
142. **What modes are available for Azure load balancers?:** Five-tuple hash, composed of source IP, source port, destination IP, destination port, and protocol type, the source port changes each session, so clients might be directed to different VMs for each session

Source IP affinity, uses two-tuple hash or a three tuple has, and it ensure the specific client is sent to the specific virtual machine behind the load balancer
143. **How would you configure the azure load balancer to store the users logged in profile as they interact with the portal?:** set the session persistence to client ip in the load balancing rules

144. **Can you use RDP with five-tuple hash?:** No, you need to use source IP affinity to connect with it.

145. **How do you create a internal load balancer?:** Set the type value to internal, and give the load balancer a private ip and a protected virtual network ment to handle requests

146. **What mode offers the greatest scalability and resilience with a internal load balancer?:** Five-tuple hash