- Service tags are used to identify groups of public IPs
- To connect to a FQDN through an Azure Firewall, configure an application rule in the firewall
- Basic VPN gateway only supports S2S and max 10 connections
- Scale units for VPN are in 500 Mbps increments
- Scale units for ExpressRoute are in 2 Gbps increments
- ErGW2Az does not support FastPath, ErGW3Az does
- A Basic virtual WAN is limited to S2S VPN connectivity only, while Standard supports ER circuits.
- CIDR /24 is the minimum address space required to create a hub
- Enabling Direct Server Return (DSR), known in Azure as Floating IP, involves creating a loopback adapter on the virtual machine and assigning the loopback adapter the IP address of the frontend listener
- To ensure that all traffic from a client (TCP and UDP) reaches the same backend machine, we must enable Client IP and protocol for session persistence (for all traffic, only Client IP should be sufficient)
- Global redirection – or Listener redirection – is used to direct traffic to another listener
- An Azure Application Gateway v2 TLS policy supports custom and predefined policies. Only custom policies allow you to choose the TLS version and cipher suite
- When creating a private endpoint or a storage account, you have the following target subresources available: Blob, table, queue, file, web, and dfs.
- Network policies are tenant- or subscription-level policies that contain routes or security group rules that can be applied automatically to subnets.
- A DNAT rule allows certain IPs (or all) to have a destination port/ IP
- The preference order in Azure Firewall is global -> per-site -> per-URI.
- An inbound NAT rule is used for port forwarding
- Associate the route table to zero or more virtual network subnets
- Effective security rules show all the NSGs associated with the virtual machines and the Network interfaces. This tool shows the NSGs that are in the flow of the traffic and blocks traffic flow.
- Private endpoints must be in the same region as the virtual network but can target any resource no matter the region.
- Multi-site listeners use the host header to match
- An Azure NAT Gateway can have a maximum of 16 public Ips
- Azure Firewall requires a /26 subnet allocated to it
- Basic SKU: You can create a gateway subnet as small as /29. However, for all other SKUs, including Standard and High Performance, you must have a gateway subnet of at least /27 or larger
- Standard_v2 or WAF_v2 SKU (for Azure Application Gateway): For these SKUs, it's recommended to have a minimum subnet size of /24
- Gateway Subnet Size: While you can create a gateway subnet as small as /29, it is recommended to create a gateway subnet of /27 or larger (such as /26)
- ExpressRoute virtual network gateway subnet must be /27 or a shorter prefix, (such as /26, /25)
- Connectivity for an ExpressRoute circuit is limited to a single geopolitical region.
- VpnGw1, VpnGw2, VpnGw3 support up to 30 S2S connections
- VpnGw4 and VpnGw5 support up to 100 S2S connections

- You cannot upgrade from Express Route Standard to ErGw3AZ, only to Ultra performance
- A NAT Gateway can be associated to multiple subnets as long as they are in the same VNET.