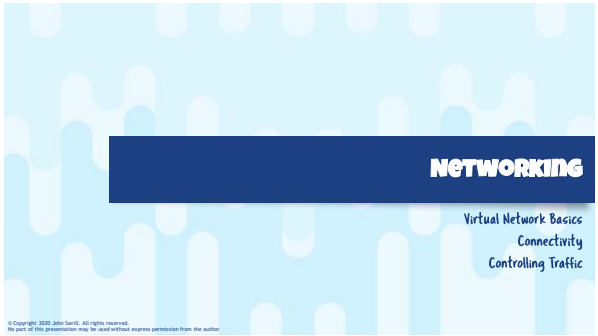

104

VIRTUAL NETWORK BASICS

- A virtual network consists of one or more IP ranges
- Typically from RFC 1918 but not exclusively
- A virtual network exists
  - Within a specific subscription
  - Within a specific region
  - It cannot span subscriptions nor regions
- The address space is broken up into subnets with the smallest subnet possible being a /29 which will give 3 usable IP addresses
- Subnet are regional and span Availability Zones

105

VM NIC

- IP always comes via fabric (OS using DHCP)
- IP can be reserved in ARM
- VMs can be configured with multiple NICs
- Each NIC can be in different virtual subnet in same virtual network or different subnets
- Multiple IP configurations per NIC
- IP configuration has private IP and optional public IP

106

SUPPORTED TYPES OF IP TRAFFIC

- Standard IP-based protocols supported including:
  - TCP
  - UDP
  - ICMP
- Multicast, broadcast, IP-in-IP encapsulated packets and Generic Routing Encapsulation (GRE) blocked
- You cannot ping the Azure gateway or use tools such as tracert
- Traditional Layer 2 VLANs are not supported

107

IPV6?

- Virtual Networks are dual stack enabling IPv4 and IPv6 address ranges assigned
- IPv6 support in NSG, UDR, LB, peering etc.
- NIC CANNOT be IPv6 only
- Can enable IPv6 for existing resources (may require reboot)
- No ExpressRoute IPv6 (yet!)
- Public IPs can be IPv4 or IPv6

108

EXTERNAL ACCESS

- There is no special "DMZ" subnet where resources get a public IP
- By default Azure provides outbound SNAT/PAT enabling resources to access the Internet and receive responses
- To provide services to the Internet either
  - Give the IP configuration an instance level public IP (not a good idea)
  - Place the instances behind an Azure load balancer, gateway or NVA which has a public IP in the front-end configuration
  - Use a network virtual appliance with a public IP
- Care should be taken to only expose the ports required, e.g. 443

110

Don't enable RDP, SSH etc. to the Internet unless you really want to test your passwords!

111

Connecting Virtual Networks

- If you wish to have multiple subscriptions and/or use multiple regions you will have multiple virtual networks
- In the past we could connect virtual networks using S2S VPN or by connecting to the same ExpressRoute circuit but both approaches have problems
- VNet peering enables virtual networks to be connected via the Microsoft backbone in the same or different regions (global peering)
- There is a small ingress and egress charge for traffic via network peering
- IP address spaces CANNOT overlap
- Can span subscriptions and even AAD tenants
- Peers are not transitive, but they can be!

112

Connecting to On-Premises

- Many Azure services have external, Internet facing endpoints however often private connectivity is required
- There are a number of options to connect to virtual networks
  - P2S VPN – Connects a specific device to a virtual network
  - S2S VPN – Connects a network to a virtual network
    - S2S VPN gateways enable multiple VPN connections to different networks if route not policy based
  - ExpressRoute Private Peering – Connects a network to a virtual network via ExpressRoute Gateway
    - ExpressRoute circuits enable multiple virtual networks to be connected to a single circuit but vnet to vnet better via peering!
- Most enterprises will leverage ExpressRoute which has the benefit of not going over the Internet, consistent latency and can also provides optional Microsoft peering via route filter

114

Controlling Traffic Flows

- By default traffic can freely flow within a virtual network and to any connected network
- To segment and control traffic within a virtual network, between networks and/or external a number of approaches can be utilized
  - Azure Firewall or an NVA with traffic routed to it via UDR
  - Network Security Groups, Application Security Groups and Service Tags
- NSGs can be applied at the subnet or NIC level but are always enforced at the NIC
- NSGs are made up of rules based on IP ranges/tags, ports and actions
- ASGs are tags applied to NICs which can be used instead of IP ranges in rules which may be easier to utilize

116

Service Endpoints and Service Endpoint Policies

- NSGs are focused on traffic into and out of the virtual network
- Many Azure PaaS offerings have their own firewall capabilities to lock down access
- It is often required to restrict a service to only specific subnets of specific virtual networks
- Service endpoints make a specific subnet known to a specific Azure service and add optimal path to service
- The virtual firewall on the service can then be configured to allow only that specific subnet
- Service Endpoint Policies allow specific instances of services to be allowed from a virtual network which is not possible with NSG service tags

118

DNS in Azure

- Virtual networks can use Azure DNS or custom DNS
- Azure DNS can provide public and private zones
- Private Zone you pick name and full management
- VNets can be linked to Private DNS Zones in addition to the built-in internal.cloudapp.net which is always there
  - 1 private zone for auto-registration
  - 1000 private zone for resolution

119

Azure Private Link

- When an externally facing Azure PaaS service is accessed from a resource in a VNet the traffic stays on the Azure network
- The PaaS service still has an external facing endpoint that some companies do not want even with firewall/authentication lockdown
- Azure Private Link enables PaaS services to have a private endpoint for a service instance created in a virtual network that is an avatar for that service instance
- Can also project custom services that are behind a standard load balancer
- Resources in the VNet can interact via the private endpoint directly to the service using the most efficient path
- Because it is instance specific helps stop data exfiltration
- Removes the need to peer VNets which can be important where VNets may have overlapping IP ranges

120

Questions?

122