**Architecting and Implementing Azure Networking**

Azure Service Manager, Cloud Services:

Virtual Ips: Azure a bunch of public IP addresses that are constantly being added to. Range of public IP addresses (what Daniel was referring to, with people watching the IP addresses). Do not whitelist all public IP addresses, anyone can provision services on that IP address. It is a public cloud, i.e. you’re sharing resources with the public. When you configure a VMs public IP address, you only keep the address for as long as the VM is running. When its powered down, you lose the IP address. The DNS name is static, which will resolve the public IP address changing.

Reserving Virtual IPs: In some cases, you may want to keep the Public IP static. This can be done by reserving a Public IP address, from PowerShell CLI or in Azure Portal.

Inbound traffic is not paid for. Outbound data is charged for. This is to remove barriers to entry for moving data to the cloud, get people hooked then make them pay.

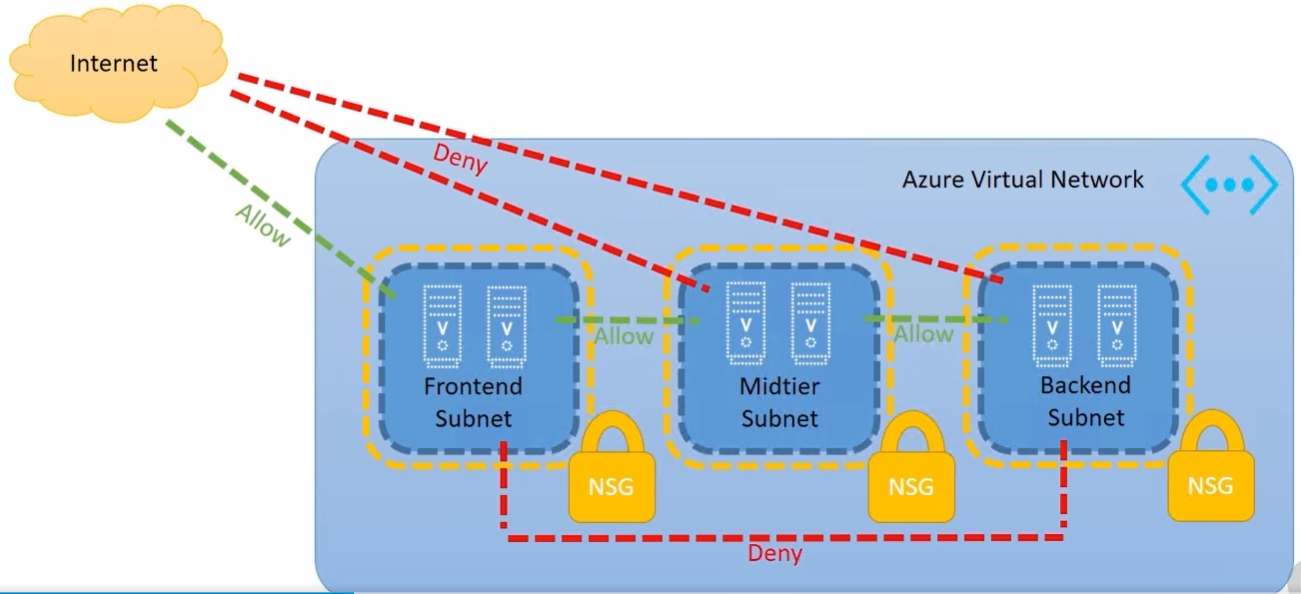
Virtual Networks:

Virtual Network is a construct that exists within a subscription, within a certain a region. VN are not visible from other subscriptions, but they can be linked together. Virtual Networks have one or more IP ranges assigned to it. You might see something like 10.0.0.0/16, 16 is the Netmask and tells you number of bits in IP range. Can have multiple address spaces. Any VM in a Virtual Network gets its IP address from the IP range > Subnet range. All Machines within a Virtual Network can communicate, even across subnets.

CIDR Notation (IP ranges): 10.0.0.0/16 = 10.0.0.1 to 10.0.255.254. Subnet mask determines what portion of the IP address needs to match for communication to occur between two resources. A 24 bit subnet mask means the first 24 bits of the IP address (out of 32) need to match. The last 8 bits can be whatever and the resources can communicate. https://www.youtube.com/watch?v=xYGTjKnVOFA

10.0.0.0-10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255, ranges cannot be used on public internet, which makes them ideal/safe for internal networks.

Network Security Groups and Virtual Appliances:

Network security groups lets you create rules to apply to resource groups, maybe a subnet. 

Azure VPN to Connect On-Prem and User Machines

Cross cloud management, single provisioning system – go to portal and control resources on-prem or in Azure. Only thing published out to internet should be internet facing services, i.e. the stuff you intend clients to directly use. Need to use unique IP range for Azure resources. Don’t want to conflict IP address with on-prem. Don’t use same scheme for Azure and on-prem, even if you don’t intend to connect them. This is essential because you cannot route between resources that use the same schemes.

Connection between Azure and OP (on-prem) occurs over public internet. VPN Gateway is created. On-premise gateway device is required. On prem needs pre-shared key and IP address of Azure side of the Gateway. Two types of Gateway: static routing (policy based) and dynamic routing (route-based VPN). Subnet needs to be called explicitly “GatewaySubnet.” Tunnels refer to number of on-premise pathways you can have. Cannot route connections together through Azure (No A -> Azure -> B location).

Understanding/Using ExpressRoute

ExpressRoute is a substitute for Site-to-Site VPN. Providers layer 3 location from your location to Azure, private connection (think client to Azure).