Azure Networking
https://squasta.github.io
Updated : 22th of July 2024

Name Resolution
- Azure-provided DNS Service (168.63.129.16)
- Azure DNS
  - Public DNS zone
  - Private DNS zone
    - Autoregistration
    - Virtual network link
    - [conditional] forwarder
    - Private DNS Scenarios
- DNS Private Resolver
- Bring your own DNS

Virtual Network
- Regional resource
- IP
  - IPv4
  - IPv6
- Adress space
  - RFC1918
  - Public IP address
- Subnet
  - Default outbound access
  - Subnet Delegation
- integration for Azure Services
  - dedicated instances of the service
    - Azure App Service
  - Private Link
  - Service Endpoints
- Security
  - Azure Bastion
    - SKU
      - Developper
      - Basic
      - Standard
      - Premium
  - DDoS Protection
    - Basic
    - Standard
  - Azure Virtual Network Encryption
- Topology
  - Hub
  - Spoke

Connectivity
- Cross-VNet
  - VNet Peering
    - Service chaining (to NVA using UDR)
    - Allow Gateway Transit (to on-premises)
    - Use Remote Gateway
  - Global VNet Peering
- On-Premises
- Azure Virtual WAN
  - Virtual Hub
    - BGP
    - Route table
    - VirtualConnection
  - Spoke
  - Virtual WAN Partner Devices
    - SD WAN CPE
  - Global transit network architecture
    - Microsoft Backbone
  - Site to Site VPN
  - Point to Site VPN
  - Express Route
  - SKU
    - Standard
    - Basic

Private Access
- Service Endpoint
  - Enabled on Subnet
  - For some Azure Services
    - VNet ACL on Azure services
  - Service Endpoint policies
    - Azure Storage
- Private Link
  - Private link service (service provider)
    - Azure Service (Storage, Cosmos DB...)
    - Your own service
      - Corporate
      - ISV
  - Private endpoints (service consumer)
- Differences between Service Endpoints & Private Endpoints?

Filtering
- Network Virtual Appliance
- Azure Firewall
  - SKU
    - Standard
    - Premium
      - TLS Inspection
      - IDPS
      - URL Filtering
      - Web categories
      - PCI DSS Compliant
      - ICSA Labs certified
  - Layers 3-7
  - Firewall policy
    - Rule collection Group
      - Rule Collection
        - Rules
          - D-NAT rules
          - Network rules
          - Applications rules
  - Azure Firewall Manager
- Services Tags
- Network Security Group
  - Application Security Groups
  - NSG Flows
    - Feature of Azure Network Watcher
    - Storage Account
  - Apply on
    - Subnet
    - vNIC

Hybrid Networking
- Point to Site VPN
  - VPN clients authentication
    - Azure certificate
    - Active Directory (AD) Domain Servers
      - RADIUS Server
      - Native VPN Client
        - Windows
        - MacOS
    - Azure Active Directory (EntraID)
      - Azure VPN Client
        - Windows 10 et >
      - MFA, conditional access
  - VPN Protocols
    - OpenVPN
      - Linux
      - Android
      - iOS
      - MacOS
      - Windows 7 and later
    - IKEv2 VPN
    - SSTP
- Site to Site VPN
  - Azure Gateway Health probe
  - Azure VPN Gateway
    - SKU
      - Basic
        - IKEv1 connections
        - Policy-based VPN
      - Generation 1
        - Route-based VPN
      - Generation 2
        - IKEv2 connections
  - On-premises VPN Device
    - Local network gateway
  - High Availability
  - BGP
- Express Route
  - Circuits
    - Primary
    - Secondary
  - Peering
    - Azure Private Peering
      - on-premises Core network
      - Bidirectional Forwarding Detection
    - Microsoft Peering
      - on-premises DMZ
    - Public peering (deprecated)
  - Express Route Gateways
    - SKU
      - Massive Data Ingestion
      - Physical Isolation
      - Granular control of circuit distribution
      - Encryption over ExpressRoute
        - MACsec
  - Express Route Direct
  - Express Route Partners
    - Internet Exchange (IX)
    - VPN MPLS
    - Internet by Satellite
  - SKU
    - Standard
    - Premium
      - Higher routing table limit
      - More VNet and ExpressRoute Global Reach connections
      - Connectivity to Microsoft 365
      - Express Route Global Reach
  - Express Route FastPath
    - Ultra Performance gateway
    - ErGw3AZ gateway

Routing
- Azure NAT Gateway
  - Regional Service
  - Standard Static Azure Public IP Address
  - Azure Public IP Prefixes
  - Subnet(s)
  - Outbound
    - TCP
    - UDP
- Azure Traffic Manager
  - DNS Load Balancer
  - Global Service
  - Routing methods
    - Priority
    - Weighted
    - Performance
    - Geographic
    - Multivalue
    - Subnet
  - endpoints
  - endpoint monitor settings
- Azure Front Door
  - Global Service
  - Layer 7
  - SKU
    - Standard
      - Optimized for delivery
    - Premium
      - Azure Web Application Firewall
      - Optimized for Security
      - Private Endpoint
  - Frontends/domains
  - Backend pools
  - Routing rules
    - Latency
    - Priority
    - Weighted
    - Session affinity
  - Health probes
- Azure Application Gateway
  - Application Delivery Controller
  - Layer 7
  - Front end IP
  - HTTP/HTTPS Listener
    - Basic
    - Multi-site
  - Rule
  - HTTP Setting
  - Custom Probe
  - Backend Pool
  - SKU
    - v1
    - v2
      - Autoscaling
      - Zone redundancy
      - Rewrite HTTP headers & urls
      - AGIC
      - Azure Key Vault integration
      - Mutual Authentication
      - SSL Profile
  - WAF
  - Regional Service
- Routes
  - Custom routes
    - 0- NAT Gateway (0.0.0.0/0)
    - 1- User Defined Routes
      - Route Table
        - IP Forwarding on NVA
    - 2- Border Gateway Protocol (BGP)
    - 3- Default system routes
- Route Server
  - fully managed service
    - support AZ
    - architecture
  - dynamic routing between your network virtual appliance (NVA) and your virtual network
    - no longer need to update User-Defined Routes
  - supports Border Gateway Protocol (BGP) only
  - IPv4 only
- Network Load Balancing
  - Azure Load Balancer
    - Private
    - Public
    - Layer 4
    - SKU
      - Basic
      - Standard
        - Availability Zones
        - Secure by default
        - SLA 99.99%
        - Tier
          - Regional
          - Global (cross region)
            - Home region
            - participating region
    - Load Balancing Rule
      - Health probes
      - Frontend IP address
      - Backend IP / ports
    - Outbound rule
    - Inbound NAT rule
- routing preference
  - Routing over public Internet (ISP network)
    - Hot potato routing
    - To Microsoft closest POP (Point of Presence) for a service
  - Through POP (165 WW)
  - Via Microsoft global network
    - Cold potato routing
    - Closest to user