# Azure Networking Services 101

David Frappart

# agenda.

1. Network Building blocks
2. Load Balancing basics
3. Public or Private – way to access PaaS services
4. Live: Adding a spoke and trying to break things !
5. The crazy pace of new Azure things – chosen examples and conclusion, for today

# Today's Speaker

## About me

- Still exploring the Cloud platform capabilities (which get new stuff all the time)
- Breath IaC and Automation (but more Hashicorp stuff than other ^^)
- Still struggles in the K8S landscape
- MVP Azure since 2019
- Huge Final Fantasy fan

devoteam | M Cloud

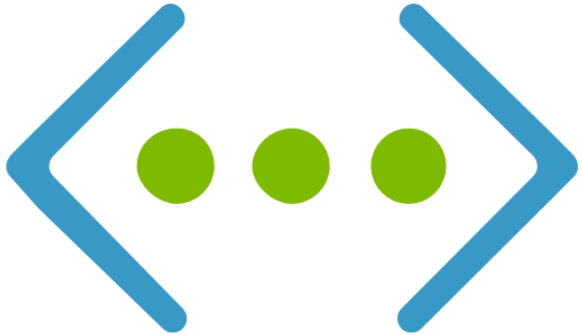
# 1

# Network Building blocks

# Building block – Azure virtual network

https://docs.microsoft.com/en-us/azure/virtual-network/

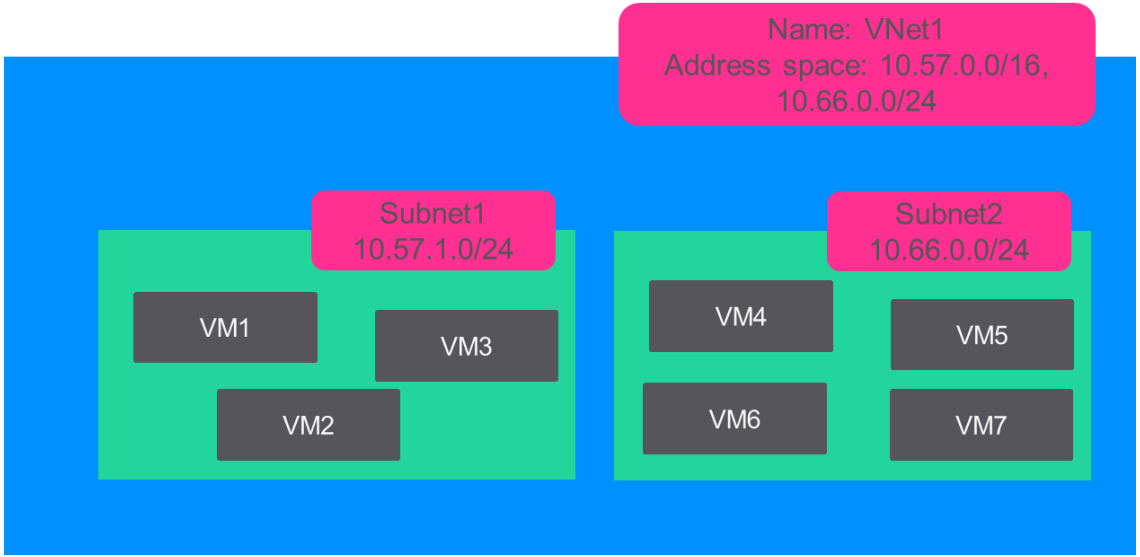
- Isolated, logical network providing connectivity for Azure virtual machines
- User-defined address space
  - Can be multiple disjointed IP ranges
  - Not necessarily RFC 1918, but best practice
  - Max of 65535 private IPs
- Connectivity to external network or on-premise
- Internet connectivity



# Building block – Azure subnet

- Provides full layer 3 semantics and partial layer 2 semantic
  - DHCP
  - ARP
  - No broadcast / multicast

- Subnet can span only one range of contiguous IP addresses
- VMs can be deployed only to subnets (not VNets)
- First 4 addresses and last address are reserved by Azure

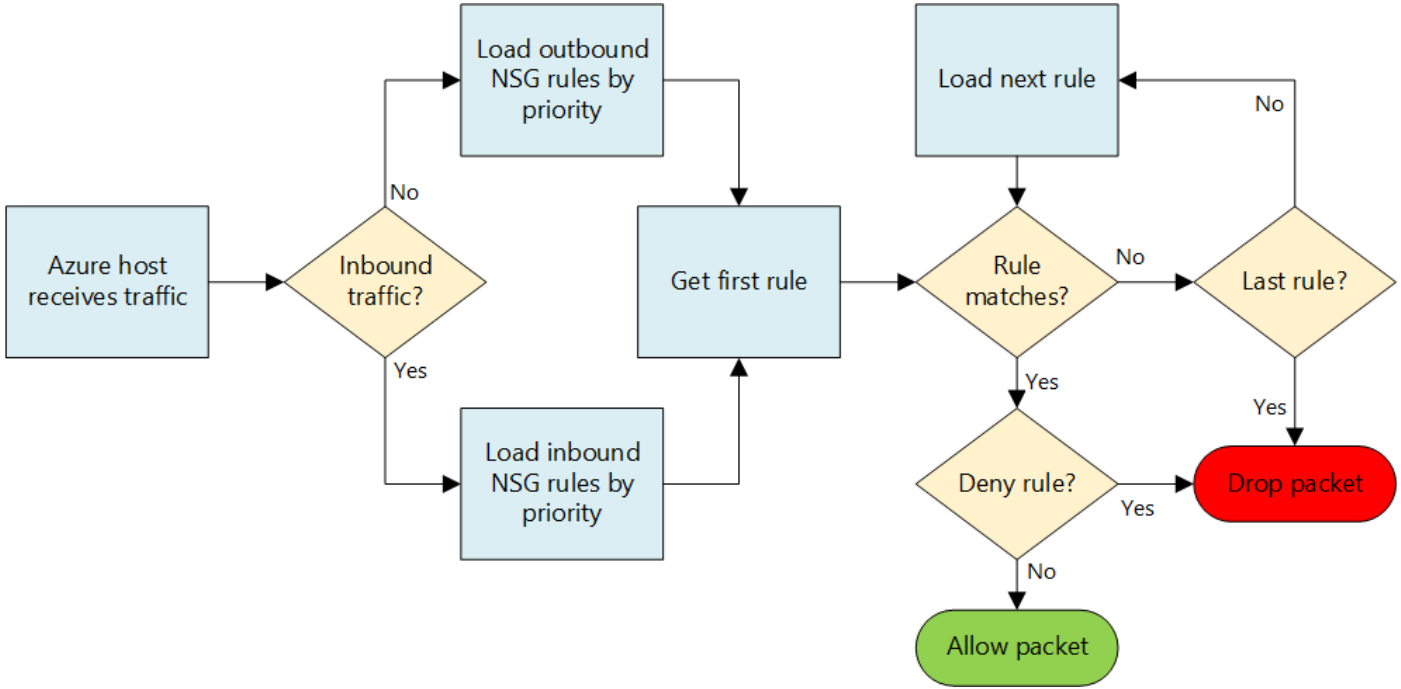


# Building block – Network Security Group

https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

- Stateful distributed firewall: no need to define rule for return traffic
- 5 tuple ACLs:
  - Source IP
  - Destination IP
  - Source Port
  - Destination Port
  - Protocol (TCP, UDP, Any)
- Actions: Allow or Deny
- Priority: 100-4096 (lower value = higher priority
- Apply to subnet and NIC Level
  - Rules still apply to the NIC
  - For inbound traffic, first applied rule from subnet
  - For outbound traffic, first applied rule from NIC
- No more than 2 NSGs applied to a VM:
  - 1 on subnet, 1 on NIC

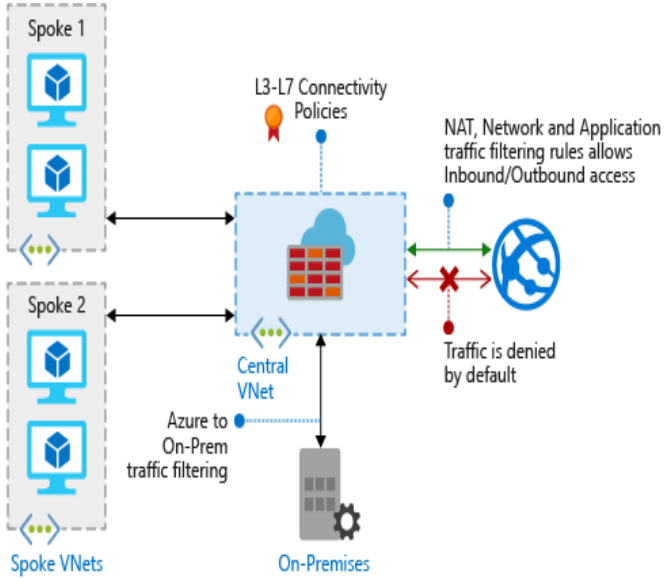
# Building block – Network Security Group



# Yes, but I want a firewall like on-premise !

https://docs.microsoft.com/en-us/azure/firewall/

- A managed, cloud-based network security service that protects Azure virtual network resources
- Fully stateful firewall, with built-in HA
- Provides:
  - Network traffic filtering rules
  - Application FQDN filtering rules
  - FQDN tags
  - Outbound SNAT support
  - Inbound DNAT support
  - Azure Monitor logging



# About routing in Azure

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

- By default, everything is routed inside the VNet
- Change the default routing with User Defined Routes (UDR)
- 3 routes sources
  - Default routes
  - BGP propagation (coming from ExpressRoute)
  - UDR
- Longest prefix (highest CIDR mask) always wins
- For equivalent prefix, apply in order:
  - User-defined route
  - BGP route
  - System route

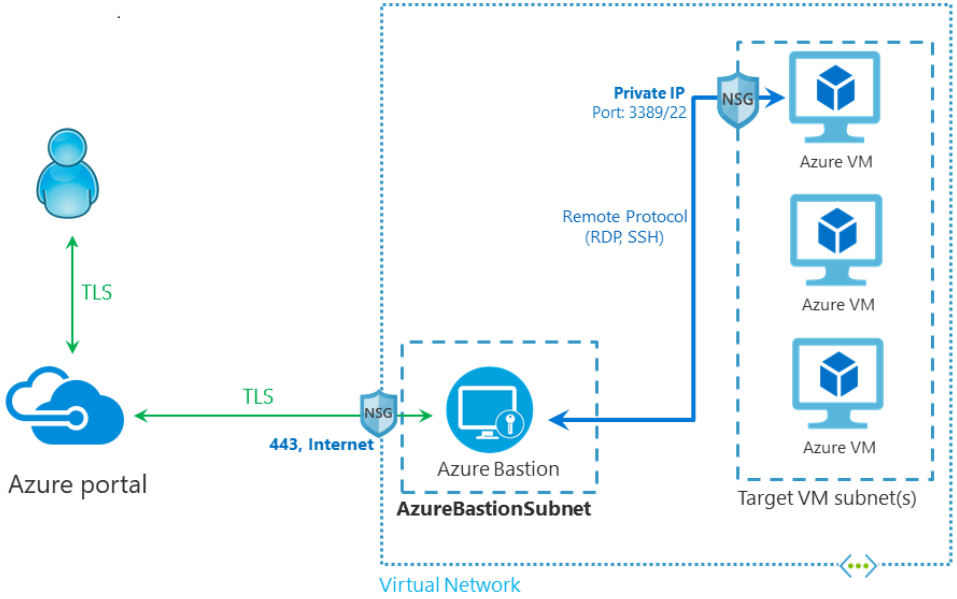
# About routing in Azure

| Source | Address prefixes | Next hop type | Subnet within virtual network that route is added to |
|---|---|---|---|
| Default | Unique to the virtual network | Virtual network | All |
| Default | 0.0.0.0/0 | Internet | All |
| Default | 10.0.0.0/8 | None | All |
| Default | 192.168.0.0/16 | None | All |
| Default | 100.64.0.0/10 | None | All |
| Default | Unique to the virtual network, for example: 10.1.0.0/16 | VNet peering | All |
| Virtual network gateway | Prefixes advertised from on-premises via BGP, or configured in the local network gateway | Virtual network gateway | All |
| Default | Multiple | VirtualNetworkServiceEndpoint | Only the subnet a service endpoint is enabled for. |

# Accessing Virtual Machine securely – Azure Bastion

https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

- Access SSH / RDP without public IP
- Control connection with Azure Diagnostic logs



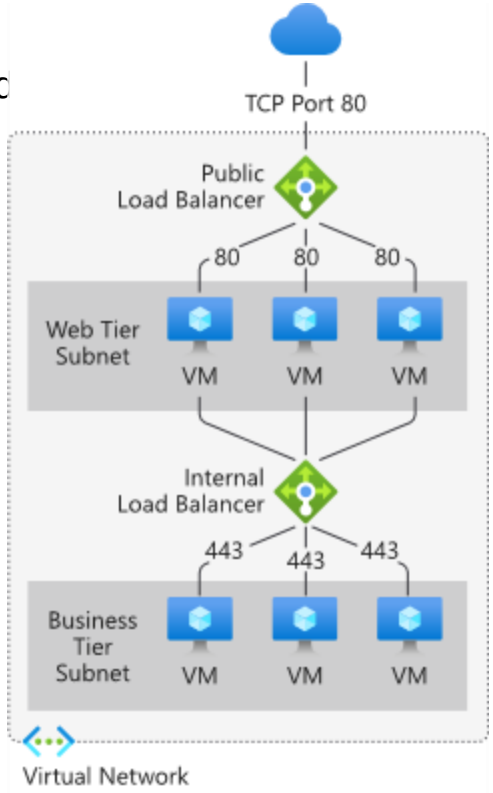
# 2

# Load Balancing basics

# Azure Load Balancer

https://docs.microsoft.com/en-us/azure/load-balancer/loac

- The L4 load balancing service
- Available in Public or Internal
- Pay for the LB rule and associated public IP
- Still issue with the diagnostic settings

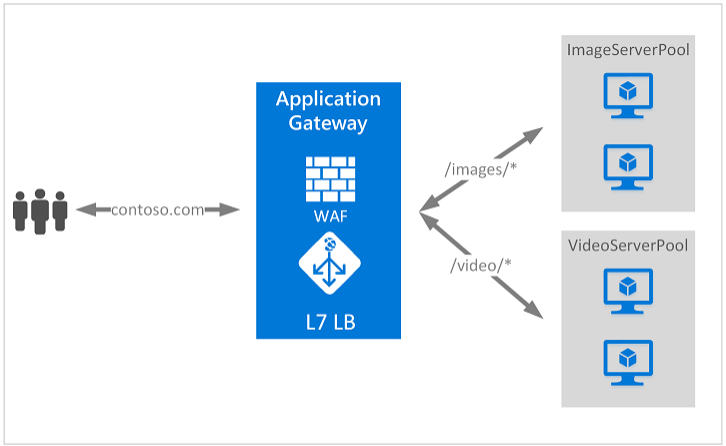


# Application Gateway

https://docs.microsoft.com/en-us/azure/application-gateway/overview

includes the following features:

- Secure Sockets Layer (SSL/TLS) termination
- Autoscaling
- Zone redundancy
- Static VIP
- Web Application Firewall
- Ingress Controller for AKS
- URL-based routing
- Multiple-site hosting
- Redirection
- Session affinity
- Websocket and HTTP/2 traffic
- Connection draining
- Custom error pages
- Rewrite HTTP headers and URL
- Sizing



# Traffic Manager

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

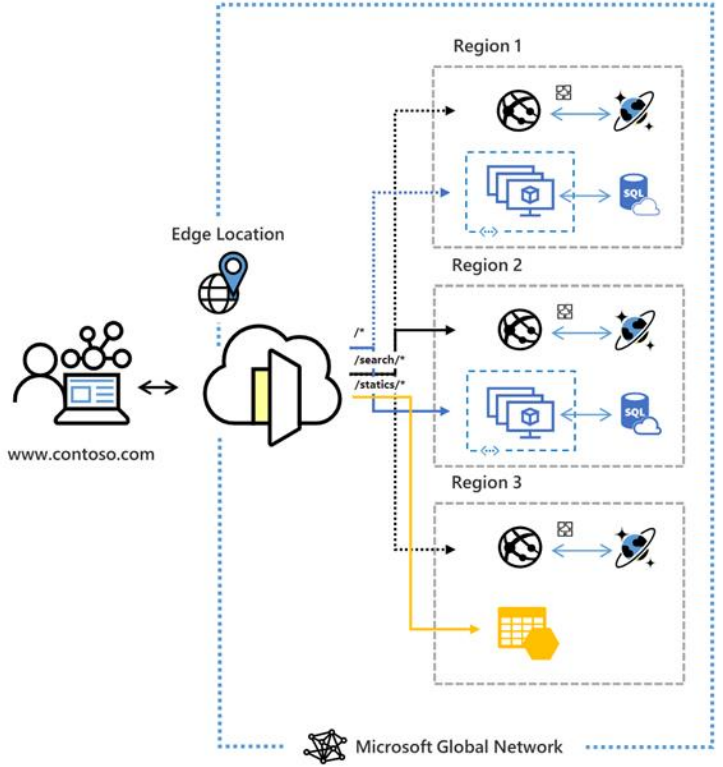
- A DNS-based traffic load balancer

| Routing methods | Description |
|---|---|
| Priority | Select Priority routing when you want to have a primary service endpoint for all traffic. |
| Weighted | Select Weighted routing when you want to distribute traffic across a set of endpoints based on their weight. |
| Performance | Select Performance routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency. |
| Geographic | Select Geographic routing to direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. |
| Multivalue | Select MultiValue for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. |
| Subnet | Select Subnet traffic-routing method to map sets of end-user IP address ranges to a specific endpoint. |

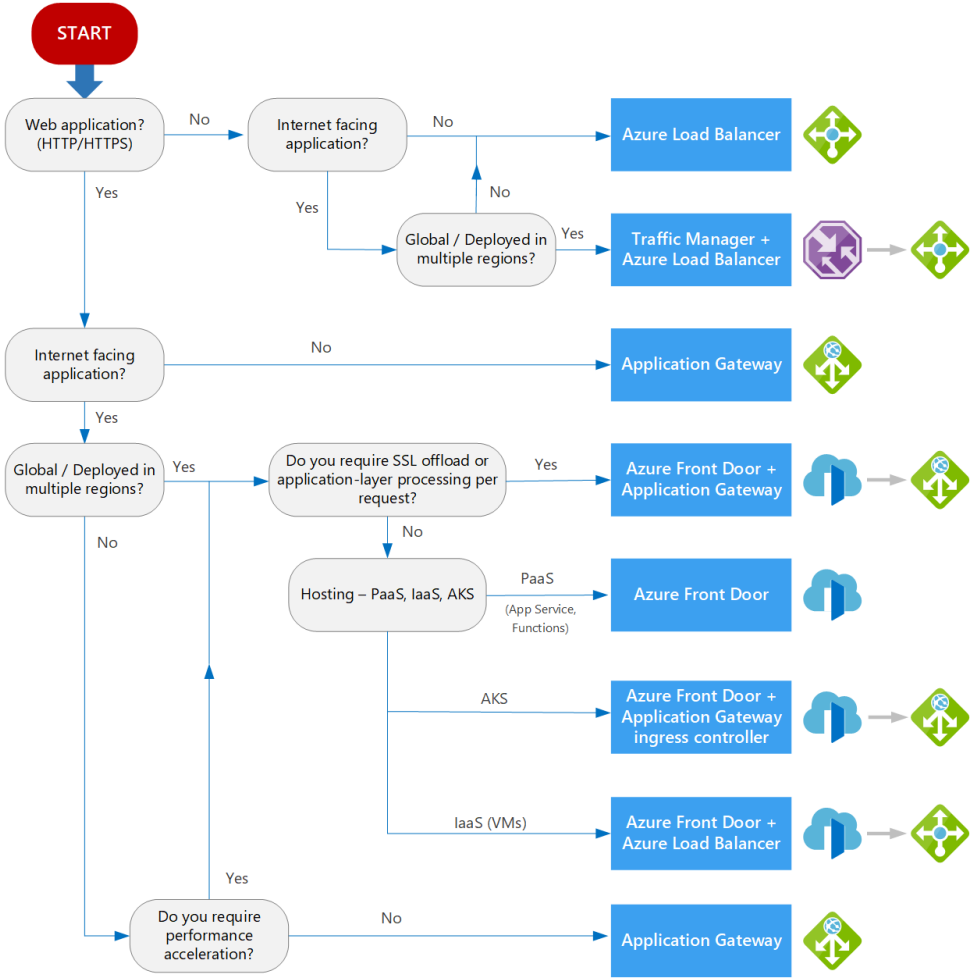
# Front Door Service

https://docs.microsoft.com/en-us/azure/frontdoor/front-doc

- A global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications.



# Decision tree



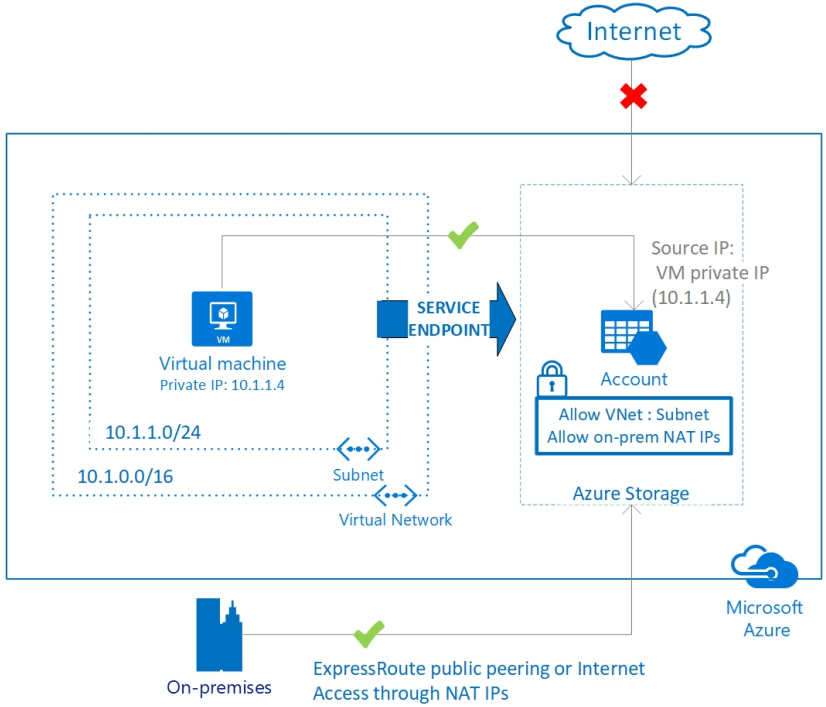
# 3

## Public or Private – way to access PaaS services

# Service Endpoint

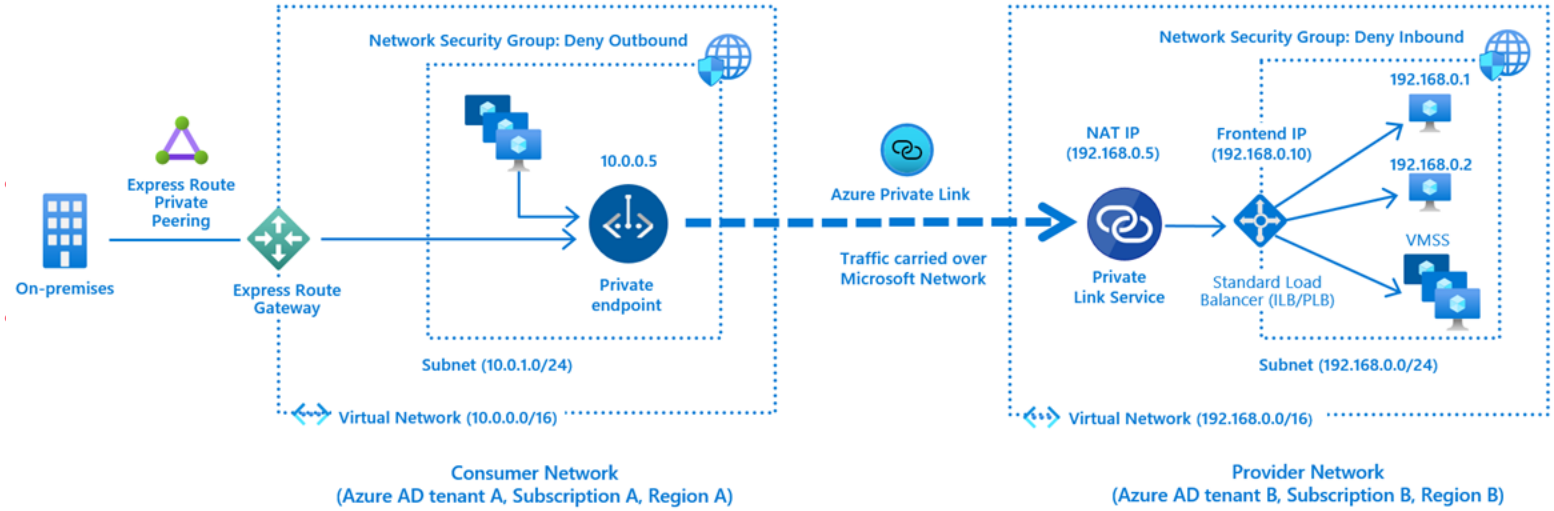
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview

- Provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network.
- Endpoints secure critical Azure service resources to only virtual networks.
- Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.



# Private link Endpoint

https://docs.microsoft.com/en-us/azure/private-link/private-link-overview?toc=/azure/virtual-network/toc.json
https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-dns
https://blogit.michelin.io/azure-private-endpoints-implementation-at-scale-dns-deep-dive/



# 4

## Live: Adding stuff and trying to break things !

# 5

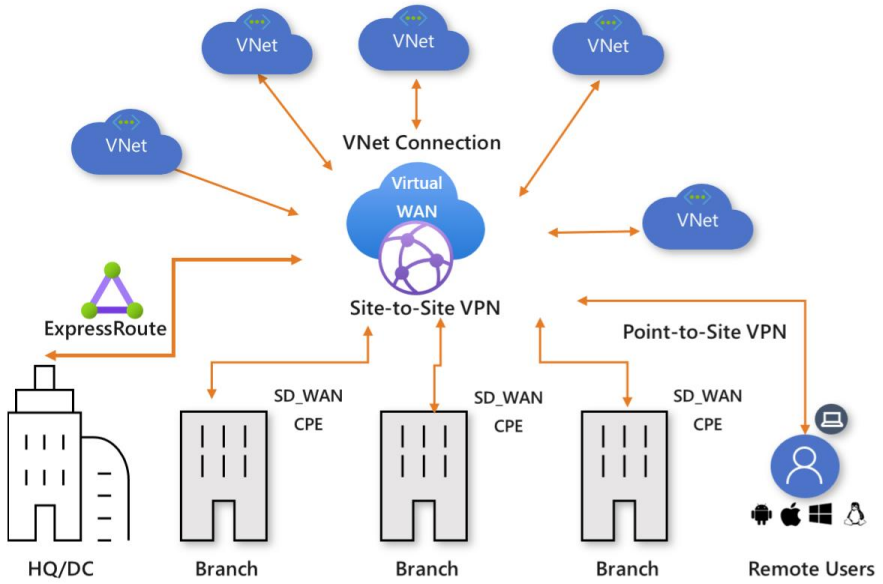
# The crazy pace of new Azure things – chosen examples

# Virtual WAN

https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

The TL;DR:

- "a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface."
- The future of the Hub?

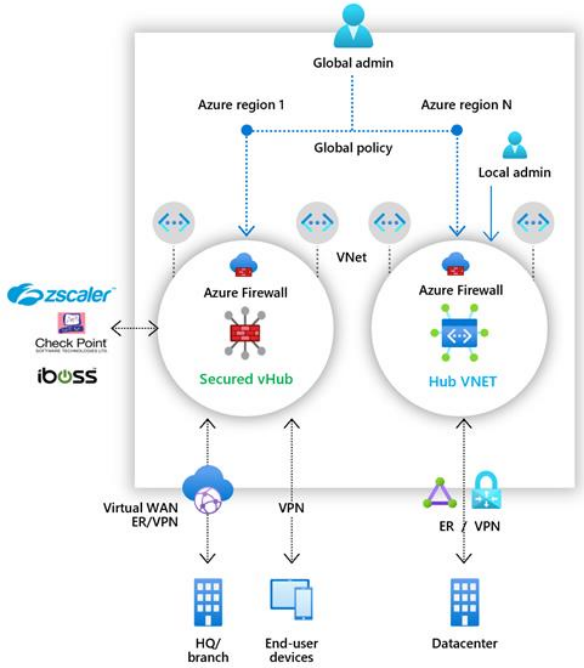


# Secured virtual hub

https://docs.microsoft.com/en-us/azure/firewall-manager/secured-virtual-hub

The TL;DR:

- "A security management service that provides central security policy and route management for cloud-based security perimeters."

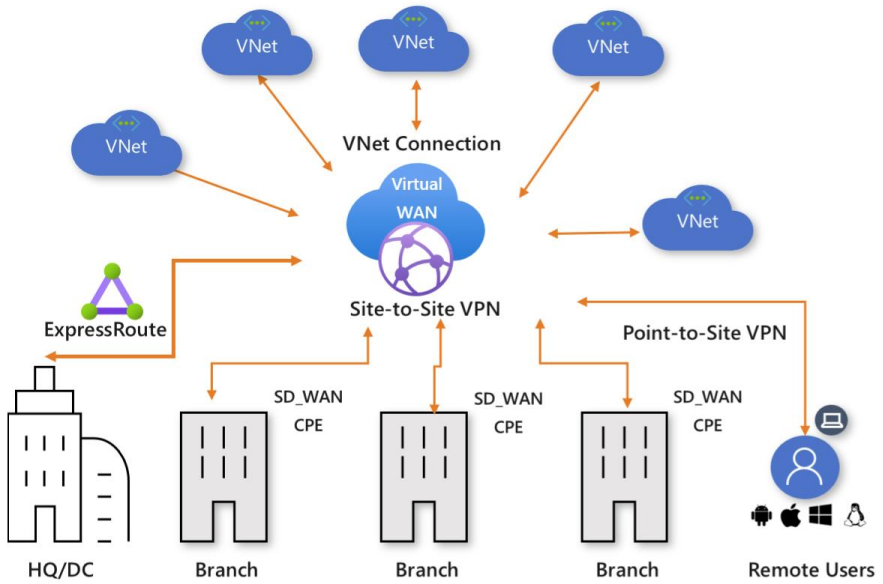


# Azure Firewall Manager

https://docs.microsoft.com/en-us/azure/firewall-manager/overview

The TL;DR:

- "A secured virtual hub is an Azure Virtual WAN Hub with associated security and routing policies configured by Azure Firew Manager."



any question?


thank you.
#TechforPeople.
devoteam