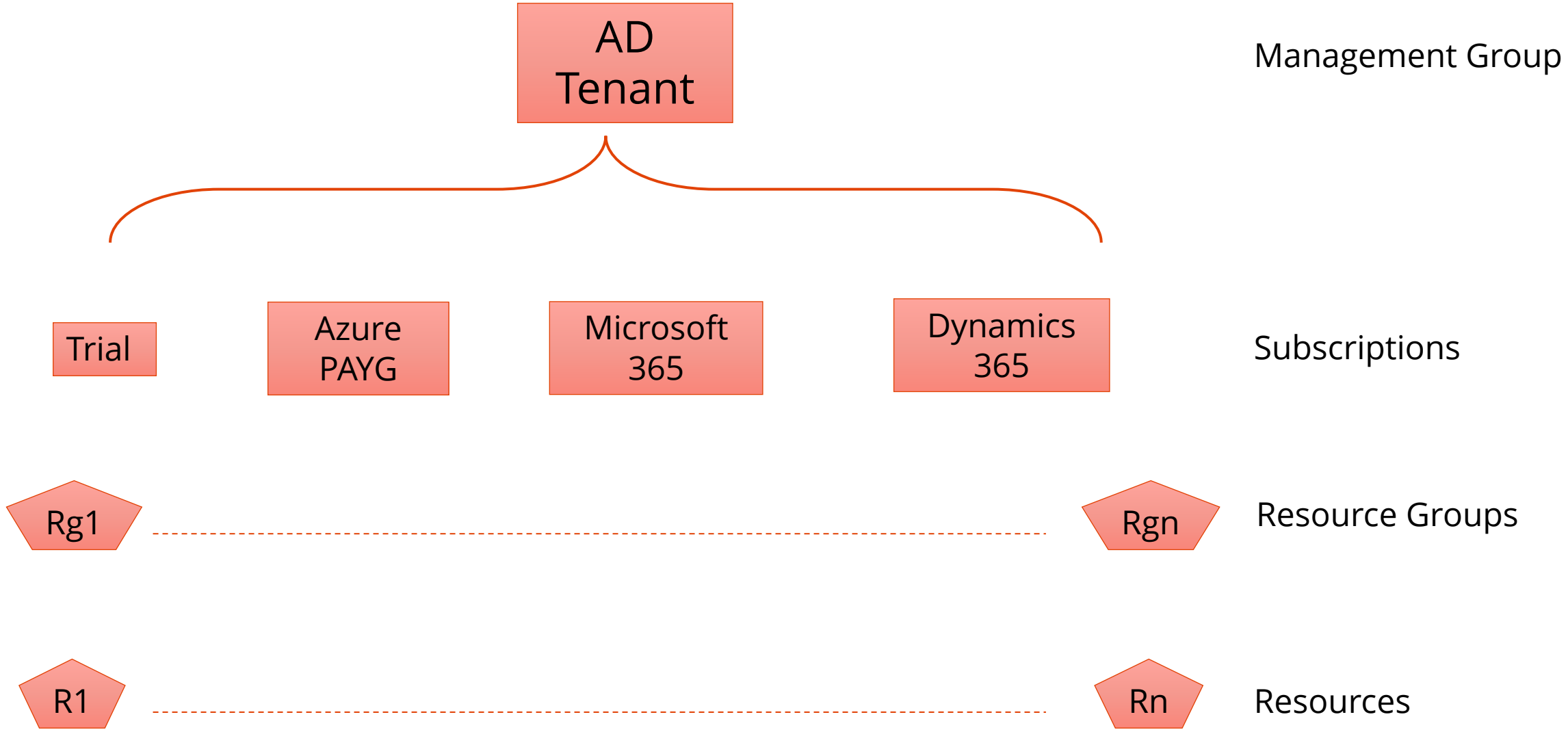
Azure Networking 101

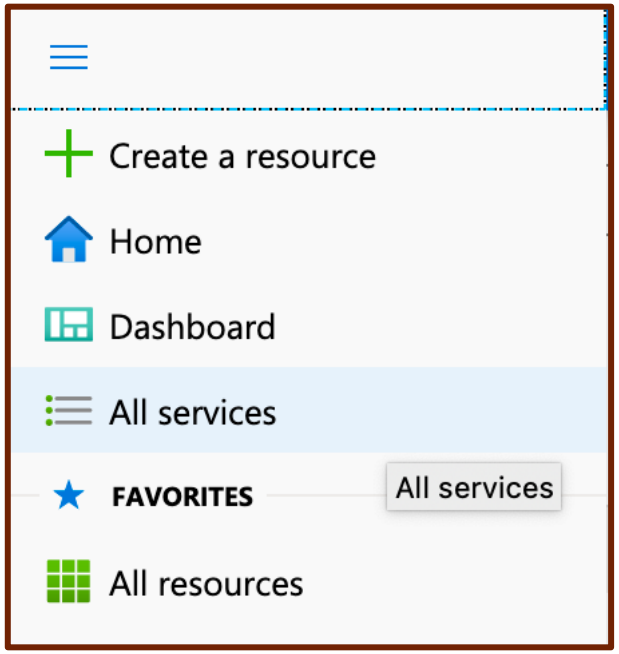
ACE Solutions Architecture Team

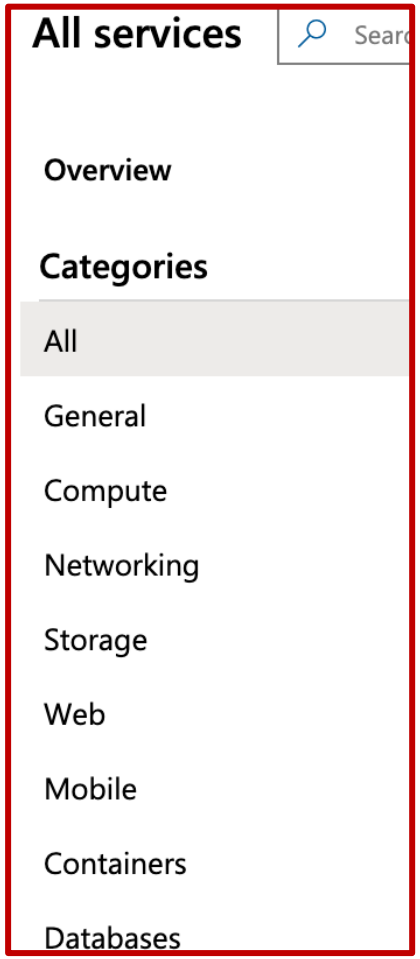
Azure Hierarchy

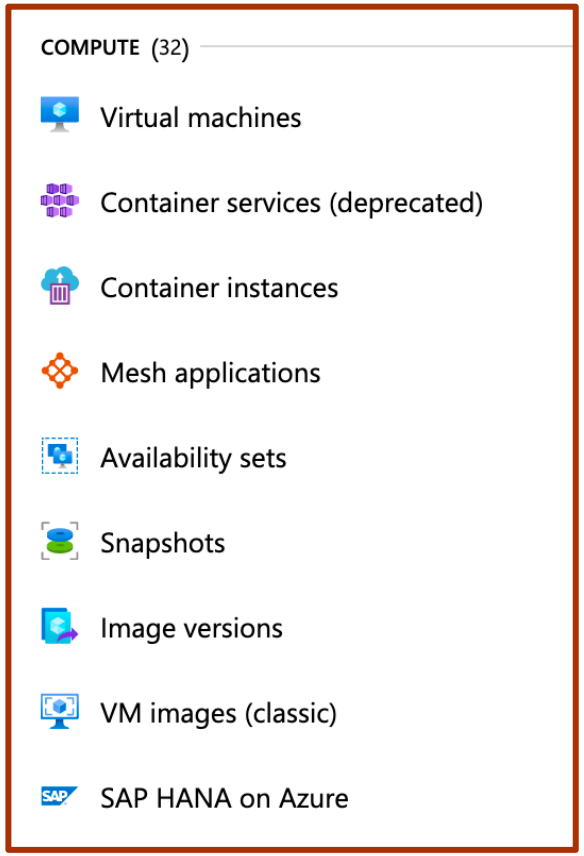


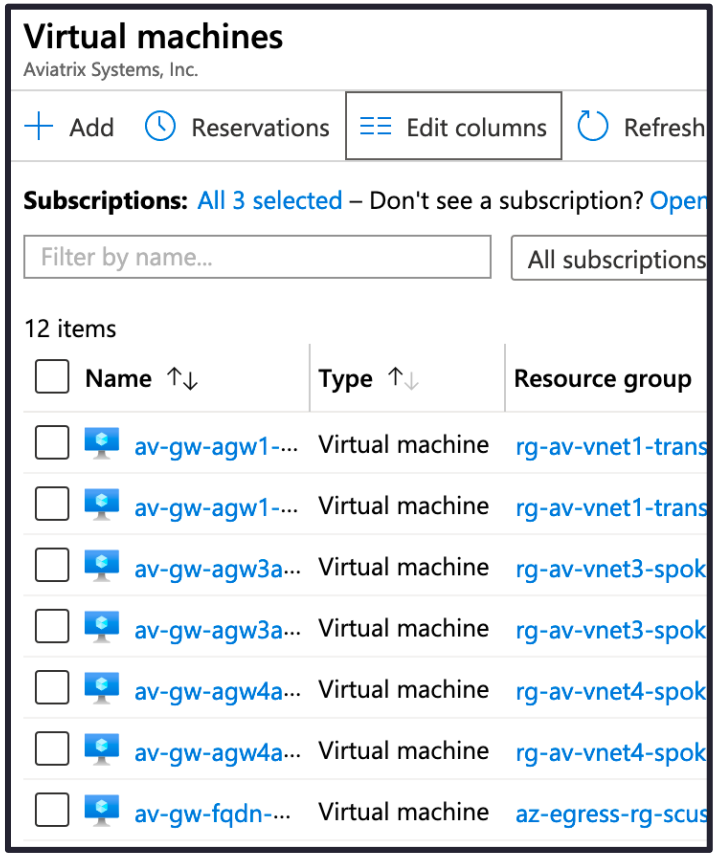
Microsoft Azure Service and Resource

Ability to See All Services	List of Service (categories)	Resources are grouped inside each Service	Resource is an instance of a Service in a Resource Group









Azure Service Categories

Category Name	Example Services
Compute	Virtual Machines, WebApps, Virtual Machine Scale Sets, Azure Virtual Desktop
Storage	Blob Storage, Disk Storage, Azure NetApp Files
Networking	Virtual Network, DNS, VPN Gateway, ExpressRoute, CDN
Databases	Azure SQL, Azure Cosmos DB, Azure Cache for Redis
Containers	Azure Kubernetes Service, Azure Red Hat OpenShift, Container Registry, Container Instances
Identity	Azure Active Directory
Security	Microsoft Defender for Cloud, Azure Sentinel, Azure Firewall, Web Application Firewall
AI + Machine Learning	Azure Databricks, Azure Cognitive Services

Azure Core Networking Services

Virtual Network

Address space can be one or more networks either public or private

- Isolated, logical network providing connectivity for virtual machines and some PaaS services

Subnets

Provides full Layer 3 semantics and partial Layer 2 semantics (DHCP, ARP, no broadcast/multicast)

- Networks within a VNet which can be used for more granular separation of virtual machines

Network Interface

Provides network services to virtual machines

- Up to 8 NICs supported on a VM depending on the SKU.
- All NICs must belong to the same Virtual Network

DNS

Provides name resolution services for resources deployed in Virtual Networks and the Internet

- All VMs in a VNet belong to the same internal DNS zone by default. It is possible to create custom public and private DNS Zones

Public IP Address

Provides communication from the Internet to services deployed in a Virtual Network

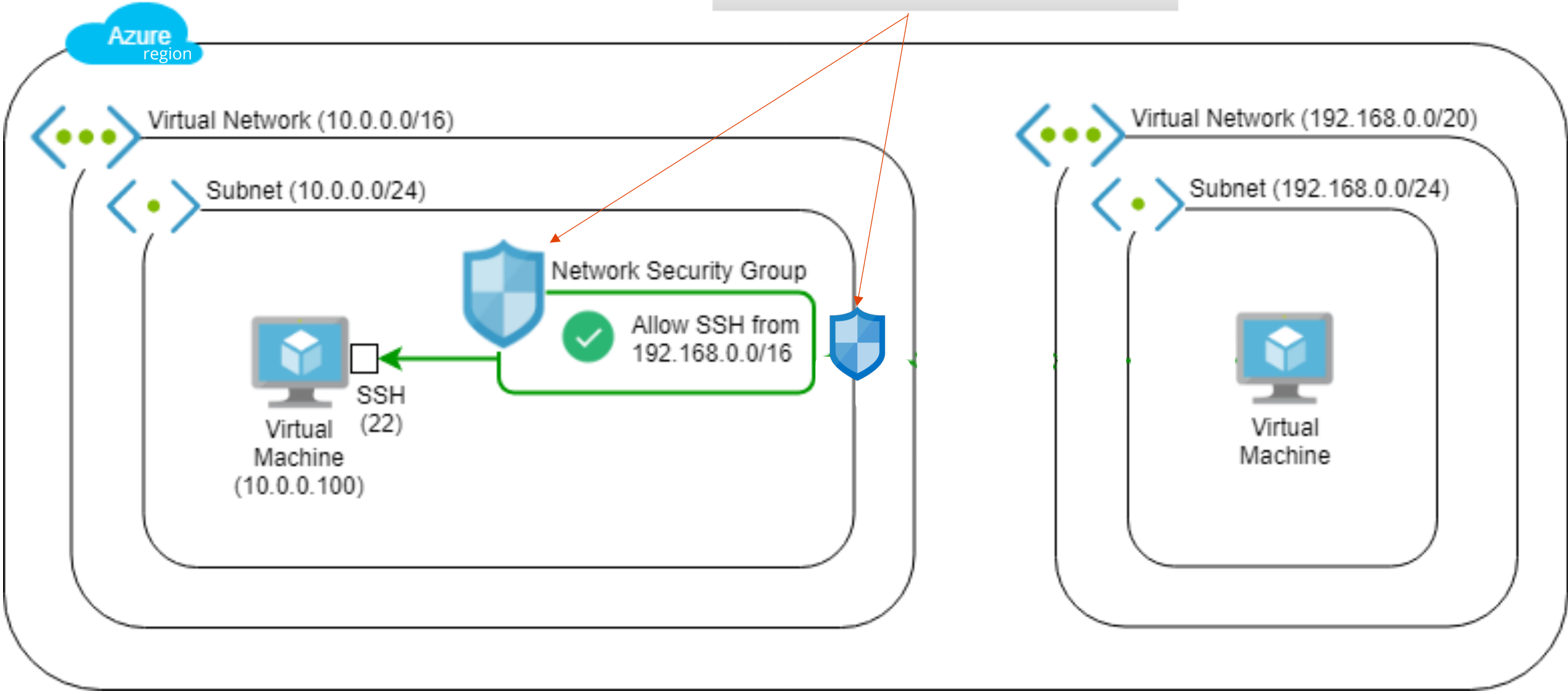
- Can be static or dynamic. Assigned by Microsoft
- Used for Internet inbound connectivity

aviatrix

NSG

NSG can be at Subnet level or NIC level

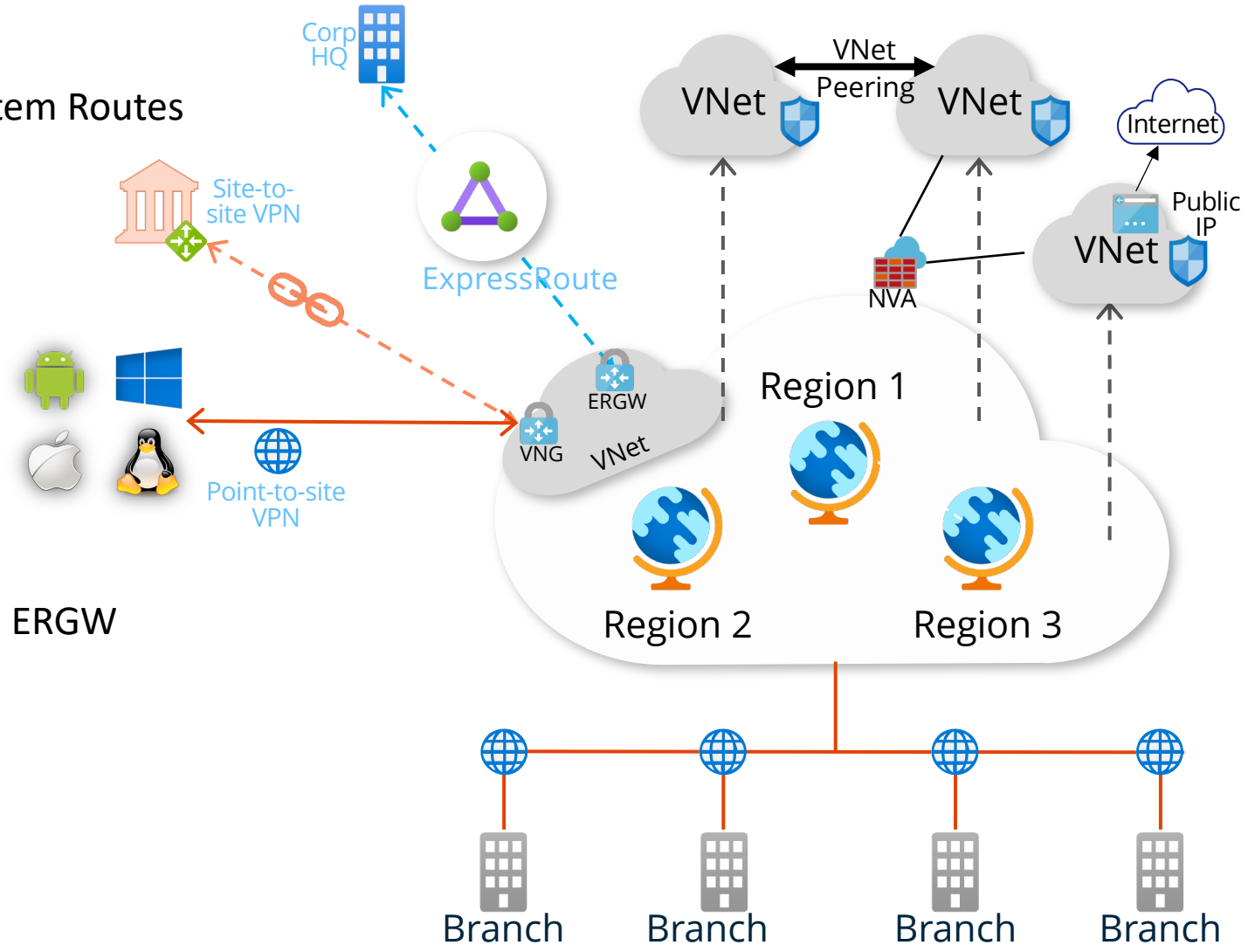
You can have NO NSG at all



Azure Networking Components

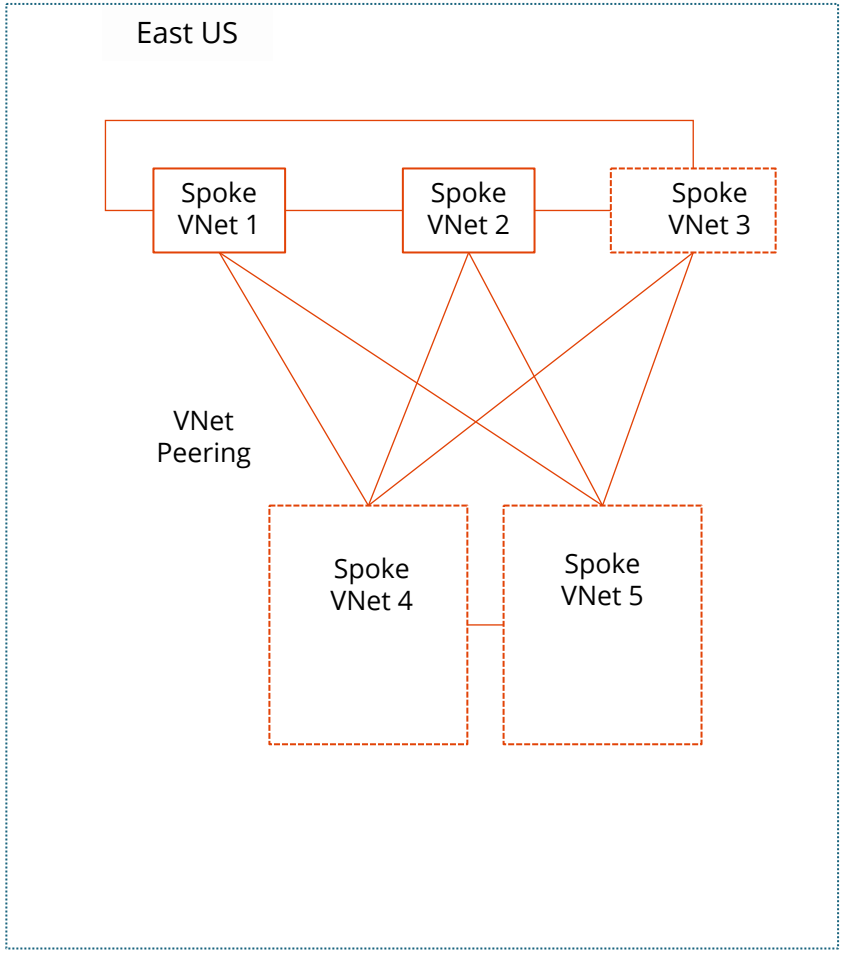
- VNet (Virtual Network)
- Routing: User-Defined Route (UDR), BGP and System Routes
- Availability Zones (not all regions)
- Network Security Group
- Virtual Network Gateways
  1. VPN Gateway (VNG)
     - S2S (max 30 tunnels) and P2S VPN
     - Local Network Gateway (on-prem entity)
  2. ExpressRoute Gateway (ERGW)

  Note: No communication path between VNG and ERGW
- Public and Private IP Address
- VNet Peering
- NVA (Network Virtual Appliance)



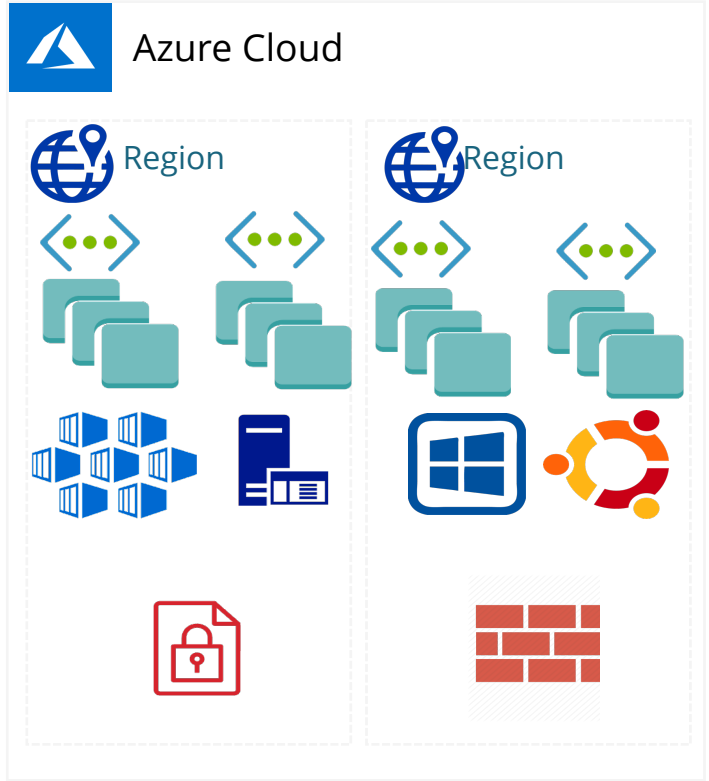
Azure VNet Peering

- Preferred Method by Microsoft Product Group for Transit in Azure
- No Real BW Limitation
- 1-to-1 Mapping
- Does not scale
- No easy way to insert FWs
- No granularity (all or none subnets)
- VNet peering data charges for ingress and egress in both directions
- Inter-region supported (Global VNet peering)

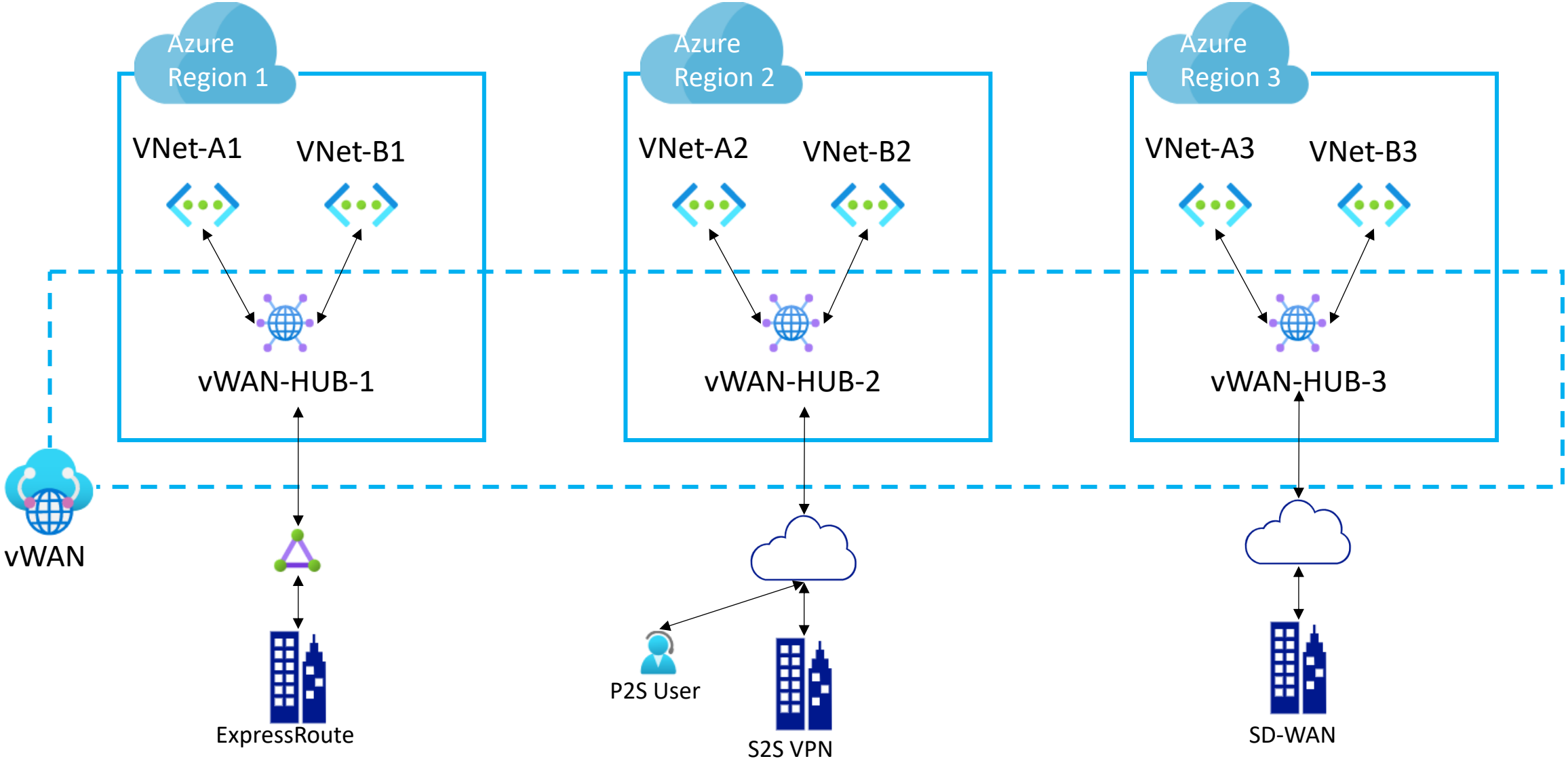


Transit in Azure

- Transit is the most important part of any cloud network
  - Transit is responsible for scale out way of interconnecting VNets
  - It connects VNets within a region, across-regions, and with
    VNet equivalents (VPC, VNC, etc.) in other clouds
  - Azure official documentation recommends to use Transit VNet using VNet Peering
- Transit with HUB VNet using VNet Peering is provided by the following Deployment models:
  1. via ExpressRoute Edge routers
  2. via Network Virtual Appliance in Transit/Hub VNet



Azure Virtual WAN



Next: GCP Networking 101