Azure Network Manager & Azure Virtual WAN - better together!

Markus Klein, Azure Networking Experte
Microsoft Deutschland GmbH

Markus Klein

- Microsoft Mitarbeiter seit ca. 6 Jahren
- Networking, Datacenter-Exit & BCDR Experte
- ehemaliger MVP CDM
- +25 Jahre Projekterfahrung

Agenda

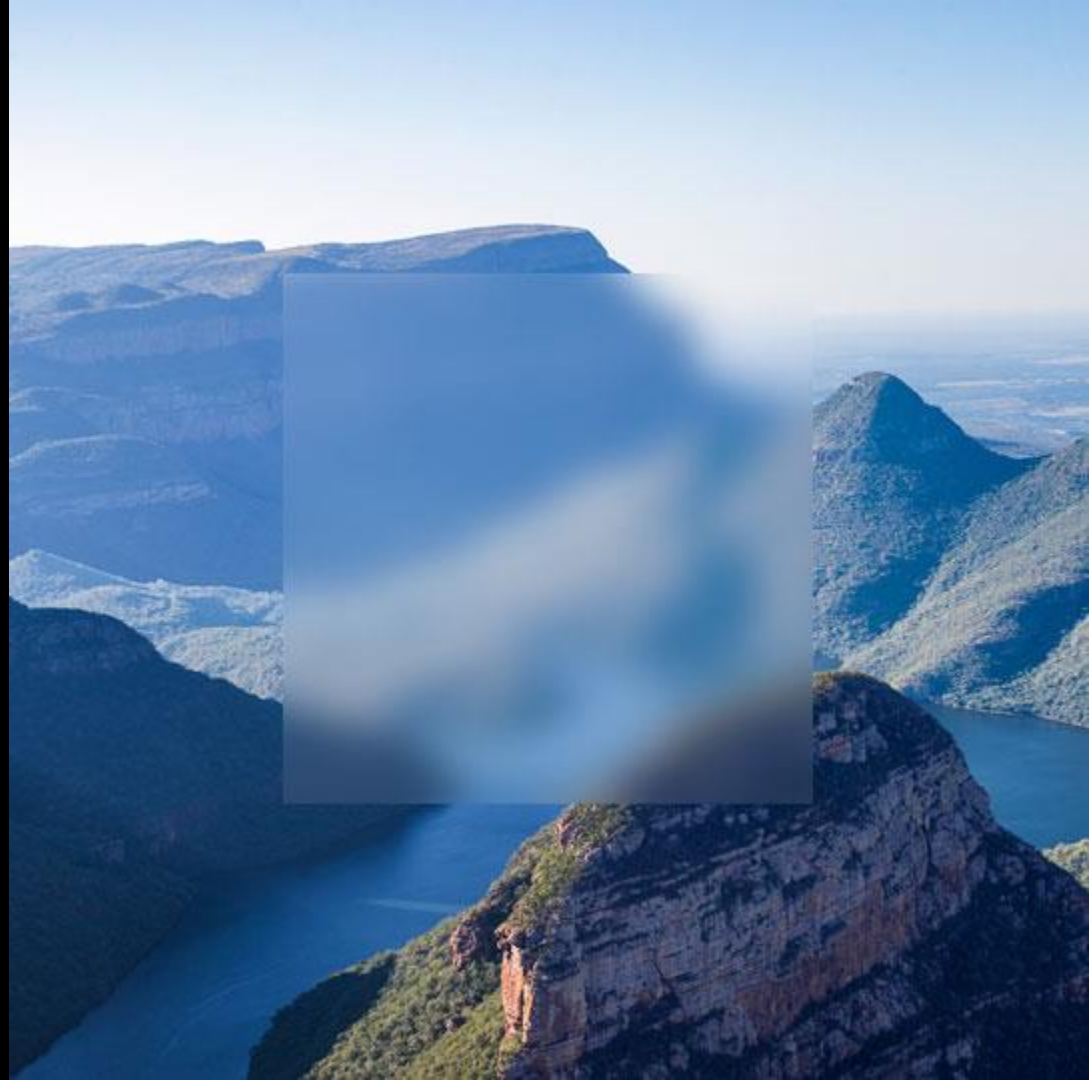
Azure Virtual WAN (recap)

Azure Virtual Network Manager

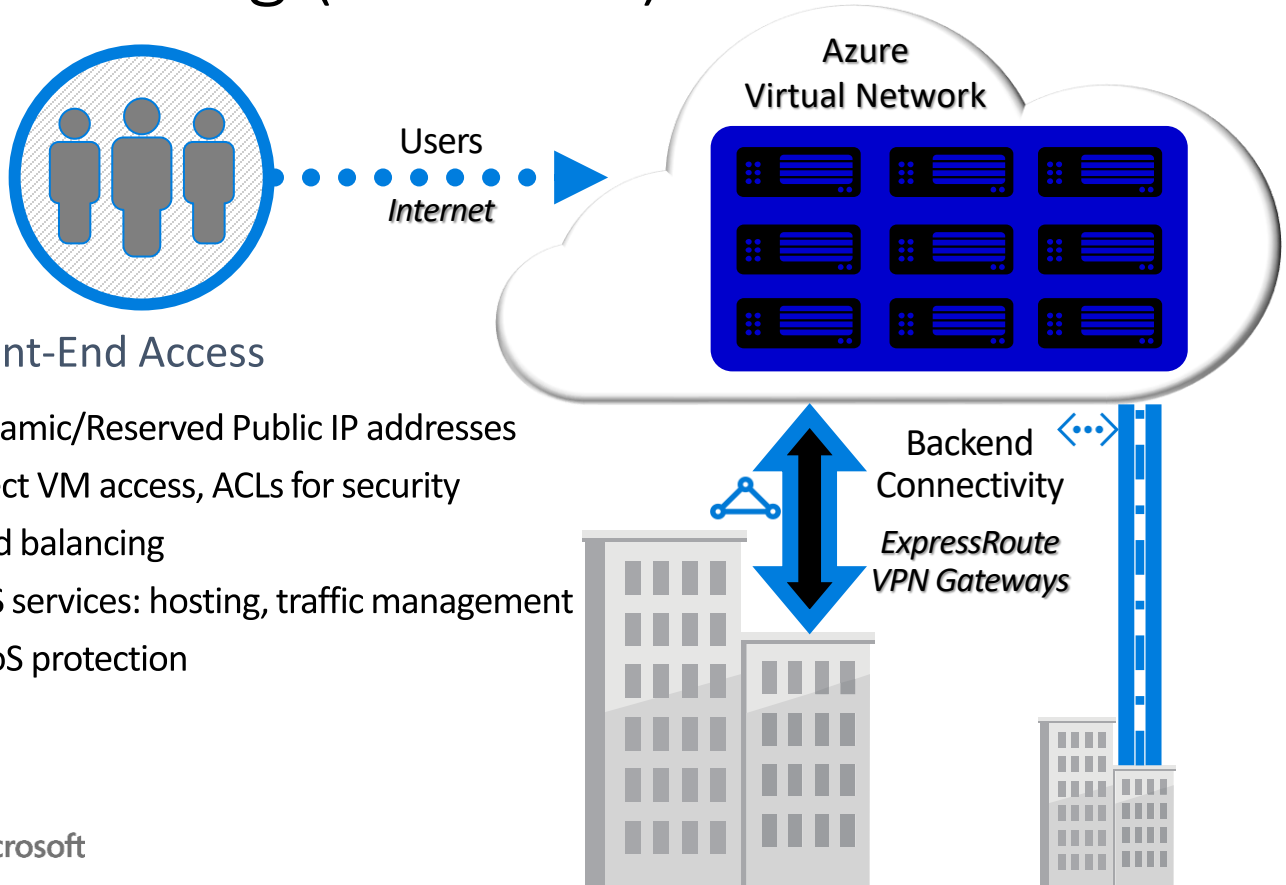
- Today
- The future

Ask me anything

Azure Virtual WAN



The Big (Network) Picture



Front-End Access

Dynamic/Reserved Public IP addresses

Direct VM access, ACLs for security

Load balancing

DNS services: hosting, traffic management

DDoS protection

Virtual Network

"Bring Your Own Network"

Segment with subnets and security groups

Control traffic flow with User Defined Routes

Backend Connectivity

Point-to-site for dev / test

VPN Gateways for secure site-to-site connectivity

ExpressRoute for private enterprise grade connectivity

The network needs are changing…

Scenario	Traditional	Cloud centric
Majority of Workloads	Data Center/On-Prem	Public Cloud/IAAS
Applications	Enterprise Apps on-Prem	Distributed/Cloud/PAAS/SAAS
Traffic Patterns	Branch-to-DC/Back Haul	Branch-to-Cloud/Internet
Branch Connectivity	WAN/DC-HQ-as-Hub	SDWAN/Internet-Breakout/Direct to Cloud
Users	On-prem/VPN-to-Corp	Mobile/Distributed/VPN to Cloud
Network Security	Enterprise Perimeter	Perimeter in the Cloud
Network Management	Central On-Prem	Cloud Based/Managed/MSP

Azure Virtual WAN

Key Scenarios

Managed Hub-and-Spoke Architecture

- Public (VPN) and Private (ExpressRoute) Connectivity

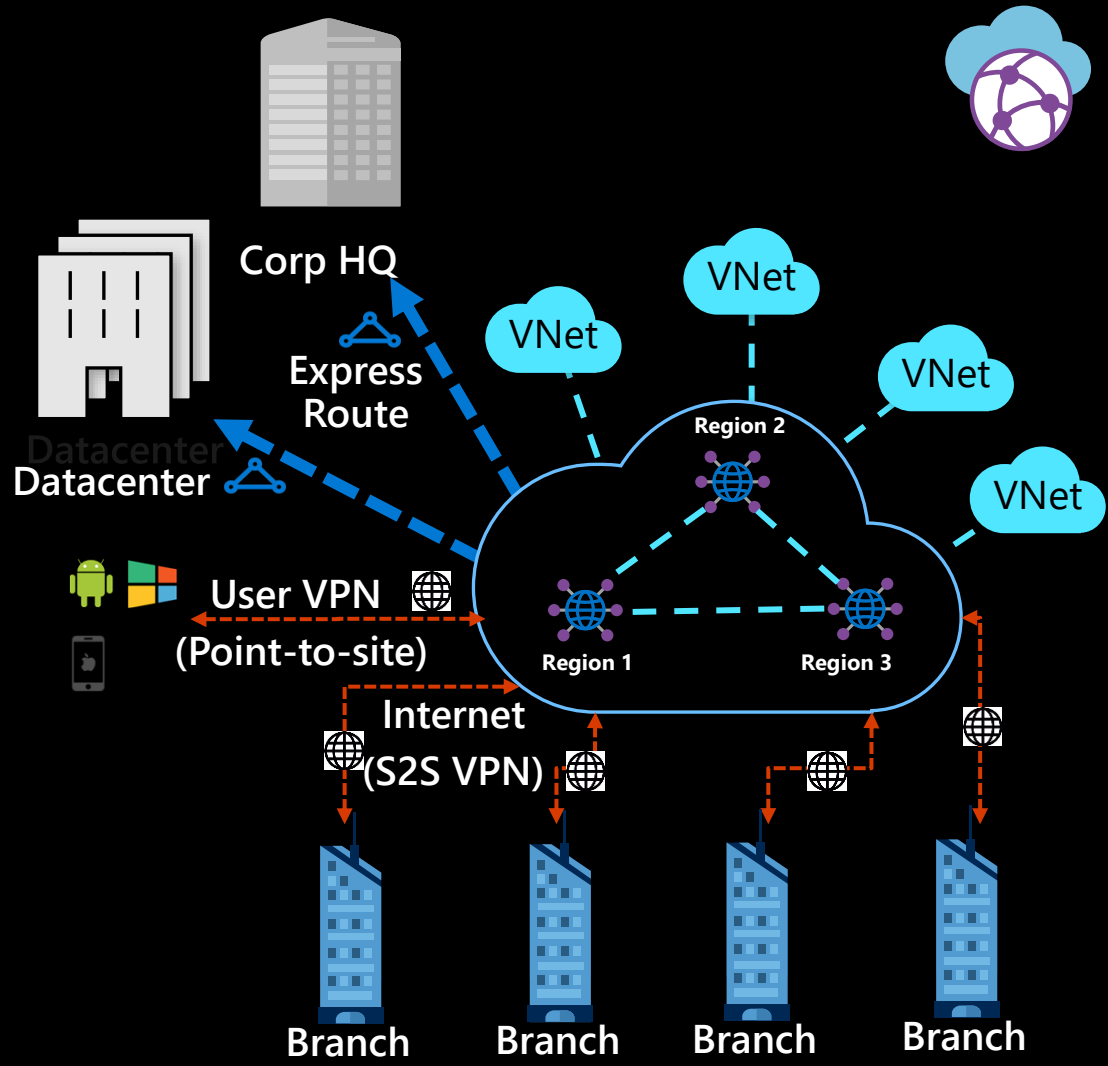
Global Scale

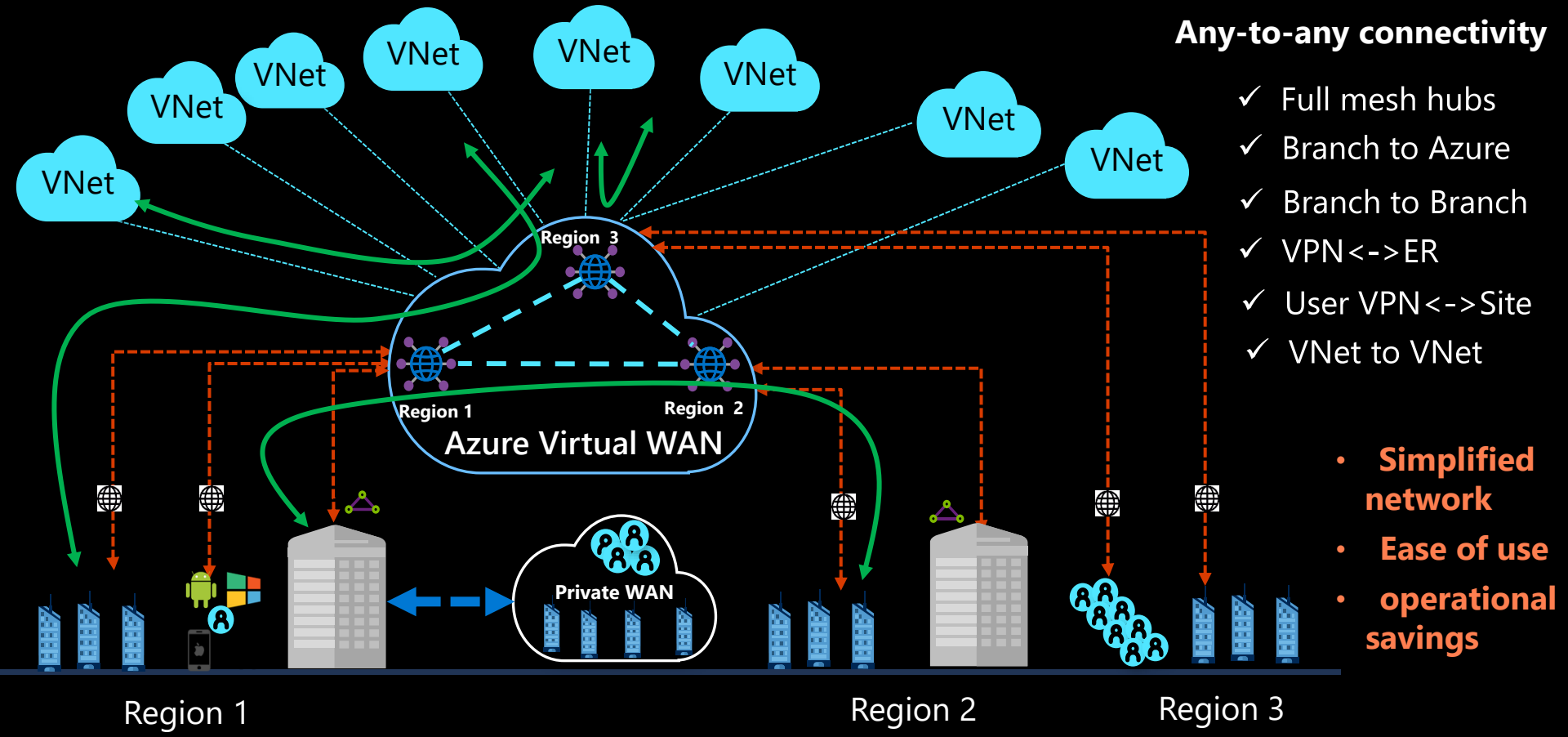
- 20 Gbps S2S VPN + 20 Gbps ER + 20 Gbps User VPN (P2S)
- 10K Users per hub
- 1,000 sites per hub

Transit Routing

Cloud Network Orchestration

- Automated large-scale branch/SDWAN CPE connectivity





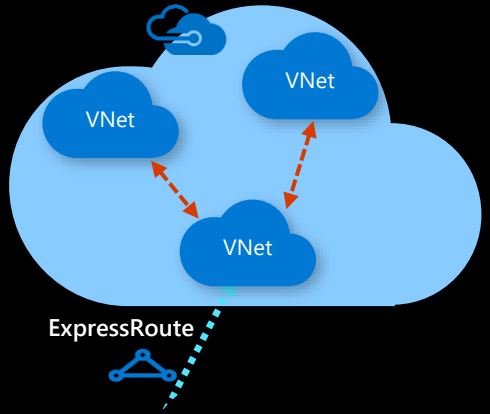
Any-to-any connectivity

- ✓ Full mesh hubs
- ✓ Branch to Azure
- ✓ Branch to Branch
- ✓ VPN<->ER
- ✓ User VPN<->Site
- ✓ VNet to VNet

- **Simplified network**
- **Ease of use**
- **operational savings**

Transit Architecture with Azure Virtual WAN

Traditional WAN



Carrier WAN/MPLS/VPN

VPN

Remote Users

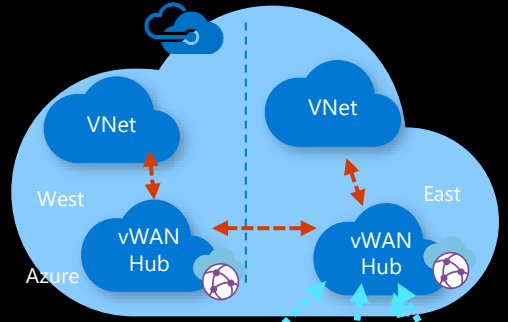
HQ/DC

Branch

Branch

Traffic Backhauled to HQ

Azure Virtual WAN



ExpressRoute

Business Class Internet (Microsoft Peering Service)

Carrier WAN/MPLS

P2S VPN

Redmond HQ Branch

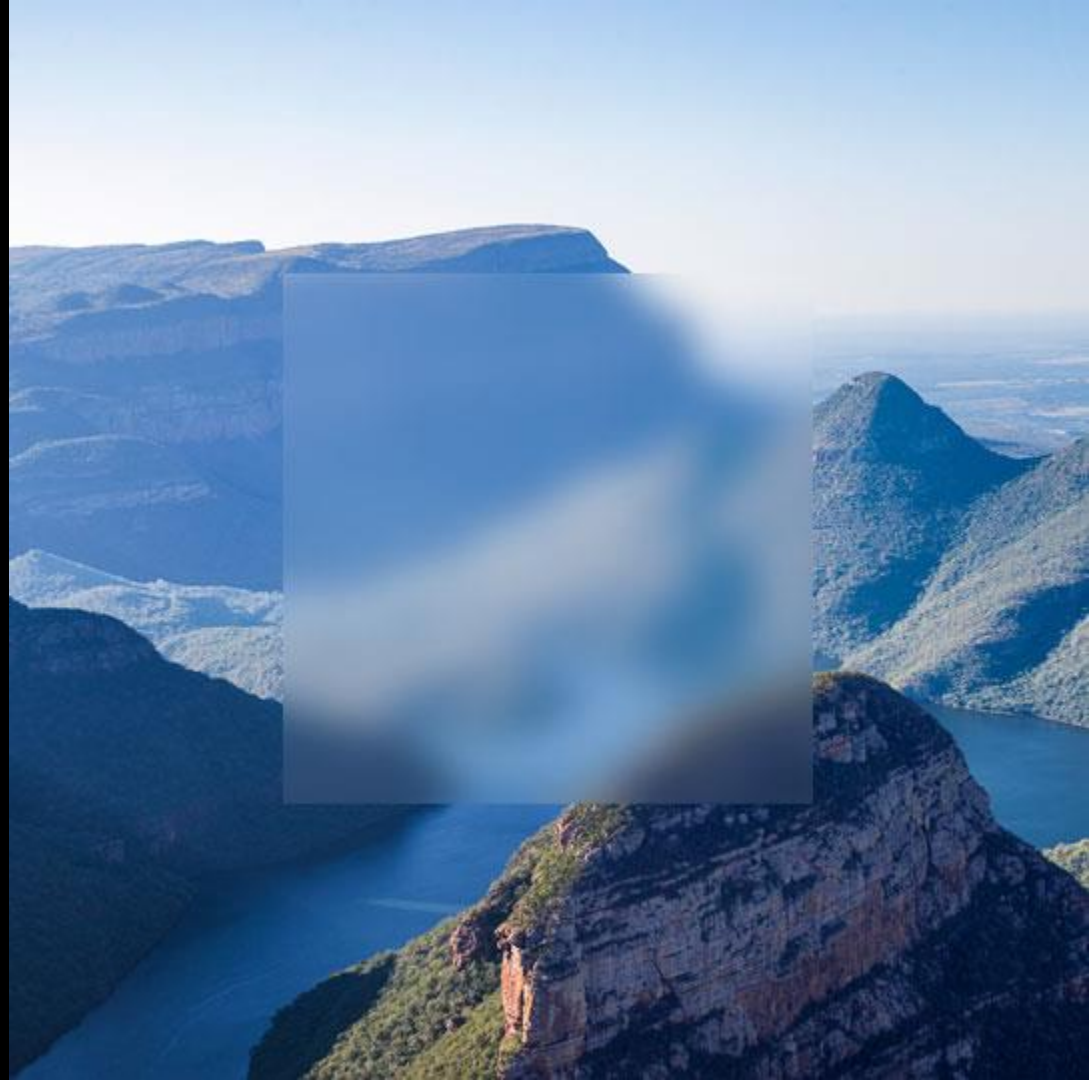
Branch

Remote Users

Branch

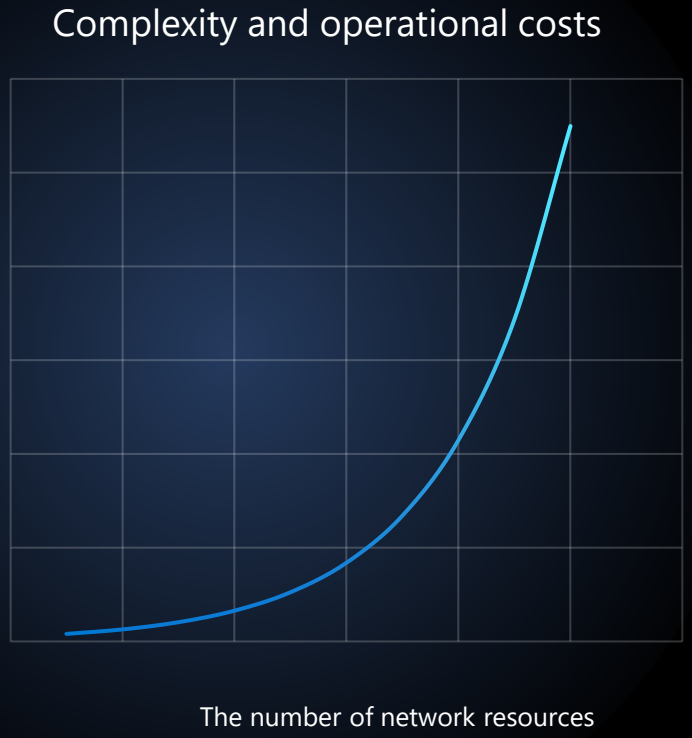
Branch

Azure Virtual Network Manager



Customer challenges with network management

Building networks at scale
Operational overhead and cost
Using multiple solutions
Errors are costly
Re-architecting to adapt to changes



Our Solution: Azure Virtual Network Manager

Simplify and centrally manage Azure Networks at scale

Features

Network segmentation features:

Create network groups to segment network resources by org/function

Define network group across regions and subscriptions

Automatically apply network configurations for changes in network groups

Connectivity configuration features:

Build and manage complex network topologies

- Mesh
- Hub-and-Spoke/direct connectivity

Security configuration features:

Admin rules

- Enforce organizational level rules without being overwritten
- Apply automatically to old/new resources

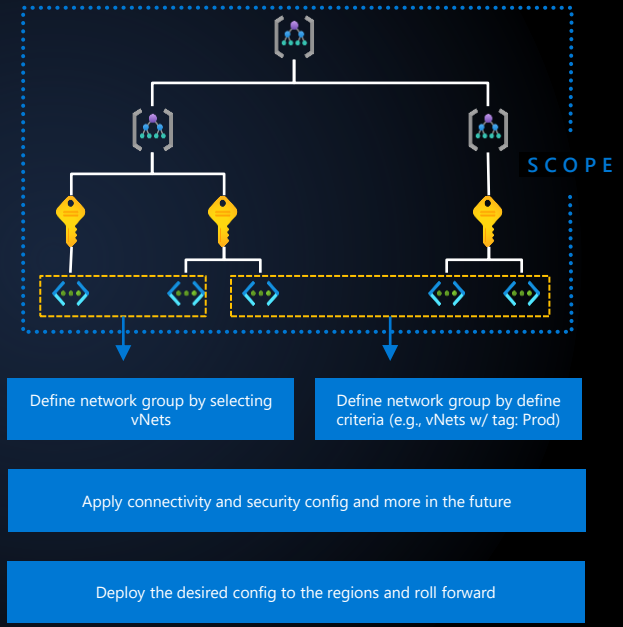
NSG management

- Define NSG rules in a simpler way and manage at scale
- Manage NSGs in a scalable way
- Modularity of rules: mix-and-match rule sets

Safe deployment features:

Safe deployment of configuration to designated region

Fix and roll forward



Network segmentation features

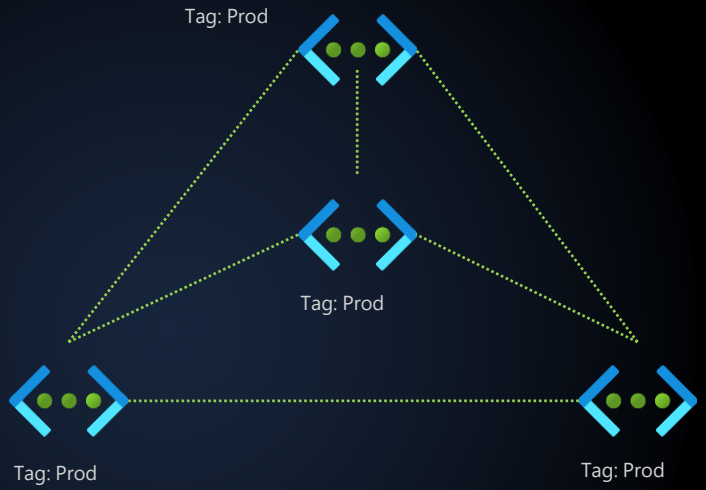
Network Group
Simplified management

Segment your network into Dev, Prod, Test or by team

Group your vNets at subscription, management group or tenant level

Static/dynamic grouping using name or tags

Apply configuration to you network groups



E.g., Defined network group:
vNets w/ tag: Prod
Mesh connectivity config

Connectivity configuration features

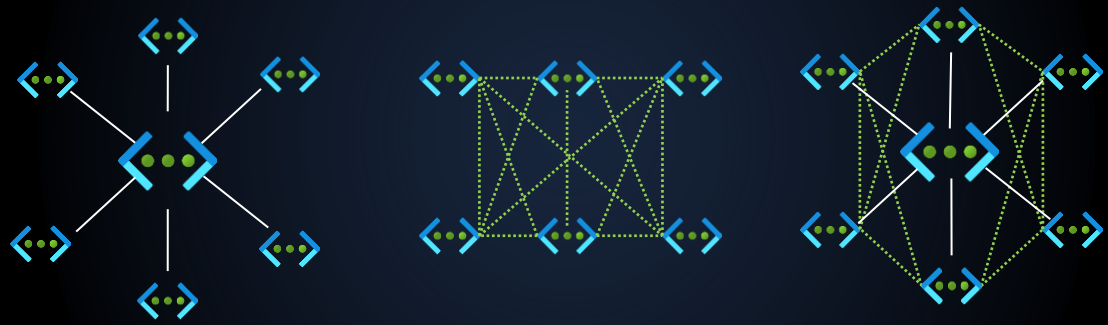
Create different topologies with a few clicks

Create different virtual network topologies with a few clicks

Hub-and-Spoke, Mesh, and Hub-and-Spoke with direct connectivity

Scale to 1000+ in Mesh

Same region and cross region peering



Security configuration features

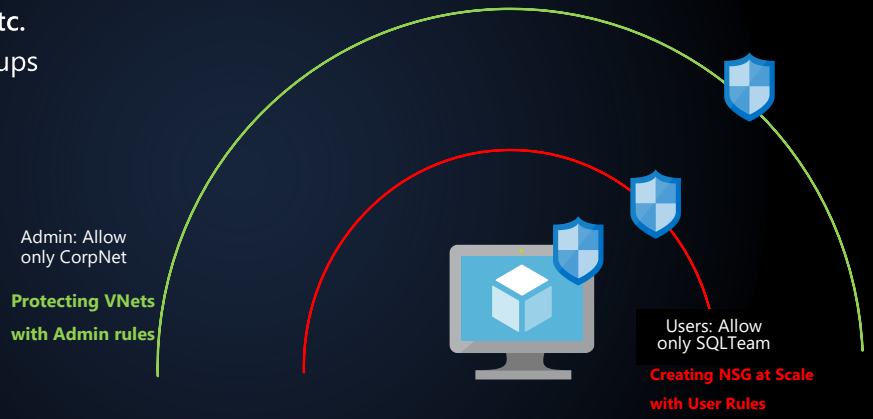
Secure at scale with admin rules and NSG management

Admin rule (this is not NSG)

- **Target audience: network admins, central governance teams, etc.**
- Admin level rules applied to all resources in desired network groups
  - Overwrite all conflicting rules
- Input: security policy -> output: admin rule
- New VMs will get these rules after they are created
- Enforced rules

User rules created and managed by ANM:

- **NSG management capability**
- **Target audience: product/service teams**
- Input: security policy -> output: NSGs, ASGs
- Micro segmentation (Mail, DNS, …)
- Conflict-free rules with modularity
  - Teams can edit and work together



Management and Monitoring Features

Manage and Monitor your Networks in Azure

Greater visibility

VNET level monitoring

Integrate with Azure Monitor for Networks

View your topologies. ANM will integrate with Network Watcher (future)

Run what-if analysis before applying network configs (future)

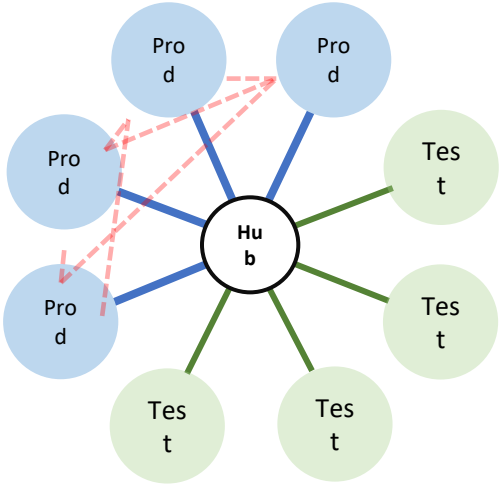
What-if ?

Azure Network Manager

	Simplified Management	Connectivity and Security	Safe Deployment	Monitoring
What?	Simplify Management of connecting Virtual Network, Security rules and routing rules across regions and across subscriptions.	Build advanced network topologies and enforce Security rules to your entire organization with few lines of config!	Safely rollout network changes across regions and stop deployment if needed.	View your network topologies across regions and run flow logs. Run what-if analysis before applying network polices.
How?	Network admins can group their resources (Dev, Test and Prod) into different network groups (static/dynamic) Customers define network configurations **(connectivity, Routing, Security)** that applies to these network groups	Network Admin can build hub and spoke and mesh topologies with less than 10 lines of config. InfoSec/IT admin can define global security admin rules like allow only Corp-Net IPs or block certain high-risk ports.	Network/IT admin can define a roll out plan for their configuration changes They can roll it per region If the networking change breaks any of their deployments, they can stop the roll out	After applying connectivity policy, customers can view their updated topologies and modify the policies. We will integrate with network watcher for monitoring.

Simplified Network Connectivity

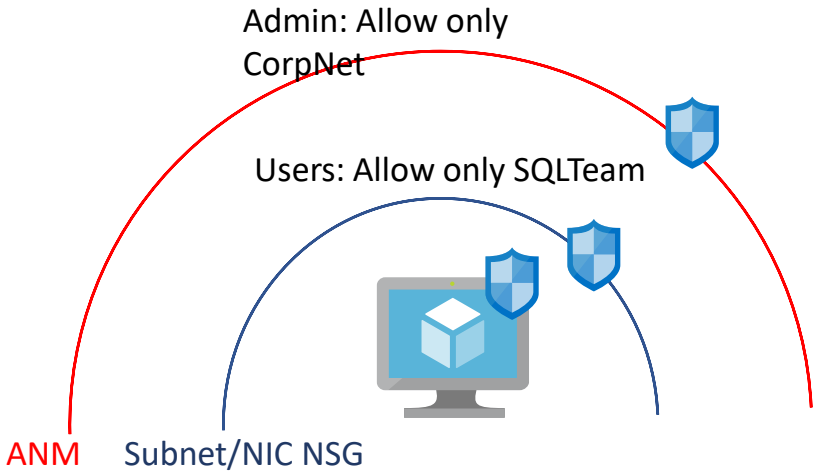
- Different Network connectivity Configurations: Hub and Spoke, Mesh, Transitive Hub and Spoke
- Customers can create multiple peering policies for different environment Dev, Prod, Test, Stage, etc.
- Scalable underlying mesh for spoke to spoke
- Native Peering Bandwidth




```
"Name": "ProdConfig",
"Type": "hub-and-spoke",
"spokeGroup": {
        "Description":"All production spokes",
        "filter":{
                "tag.name": "spoke-type",
                "tag.value" : "Test"}
  },   "hubVnet":"/subscription/.../virtualNetwork/hub"
```

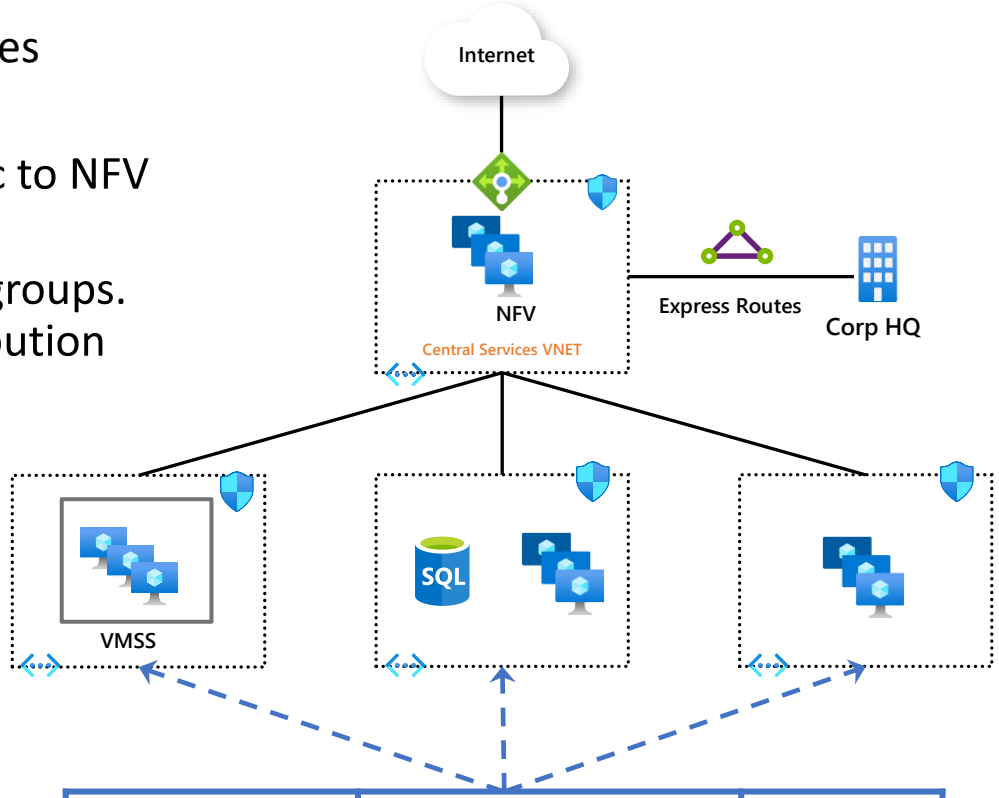
Admin Rules: A powerful security tool

- Global Network security rules that applies to all resources in a sub or management group.
- InfoSec use cases:
  - Restrictive Allow
    - Allow only SAW IP to access Prod
  - Forced allow
    - Allow Agent on port 5234
  - Forced Deny
    - Block all high-risk ports from Internet
- Rules are enforced once applied.
- Rules cannot be deleted or overridden by resource owner



Routing Rules

- Global UDR Policy pushed as System routes
- Network Admin use cases
  - Apply Route to all spokes to send traffic to NFV in the Hub for IPS/IDS or FW
  - Push routes to multiple NFV based on groups. Dev NFV, Prod NFV, ..etc for load distribution
- Will integrate with BGP service



Dest	Type	NextHop
0.0.0.0/0	Network Appliance	NFV-IP


Radial
Radial
Radial
Radial
Panasonic
M-AUDIO

Standard Features – Available NOW!

Simplified Management


Cross Subscription


Management Group Support


Green Field and Brown Field Handling


Conditional Network Membership

Connectivity/Security


Security Admin rules


Connected Mesh


Hub and Spoke (with Transitivity)

Safe Deployment


Cross Region


Staging and Config Rollout

vWAN Management using AVNM


FUTURE
loading...


Q&A

Wanna get in touch? Klein.Markus@microsoft.com

Thanks to our Sponsors!