NIC

EMPOWER

November 13-15, Oslo Spektrum

Patrick de Kruijf

Azure Architect

https://www.linkedin.com/in/patrickdk
https://www.azurefreakconfessions.com

Understanding Azure Virtual WAN & lessons learned

NIC
EMPOWER

Xebia

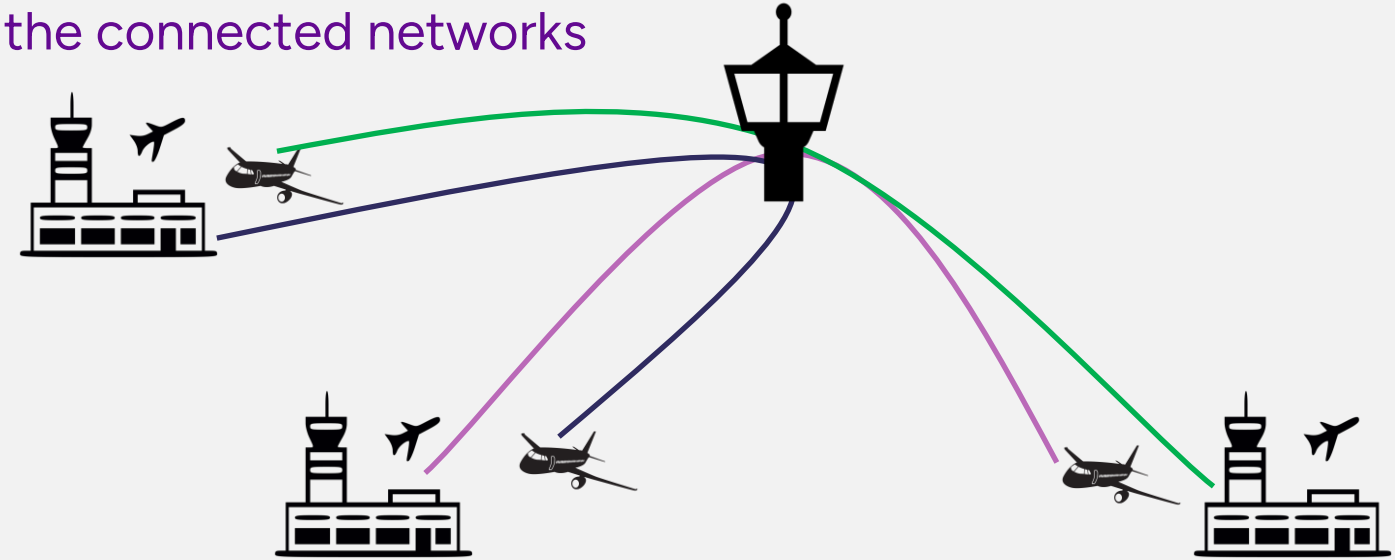
(Your) goals for this session

- Learn about Hub and Spoke
- Learn about Azure Virtual WAN (vWAN)
- See the vWAN resource in the Azure Portal
- Learn about tricky stuff you can encounter
- Ask questions and try to challenge me

What is this Hub and Spoke everyone talks about?

Hub and spoke

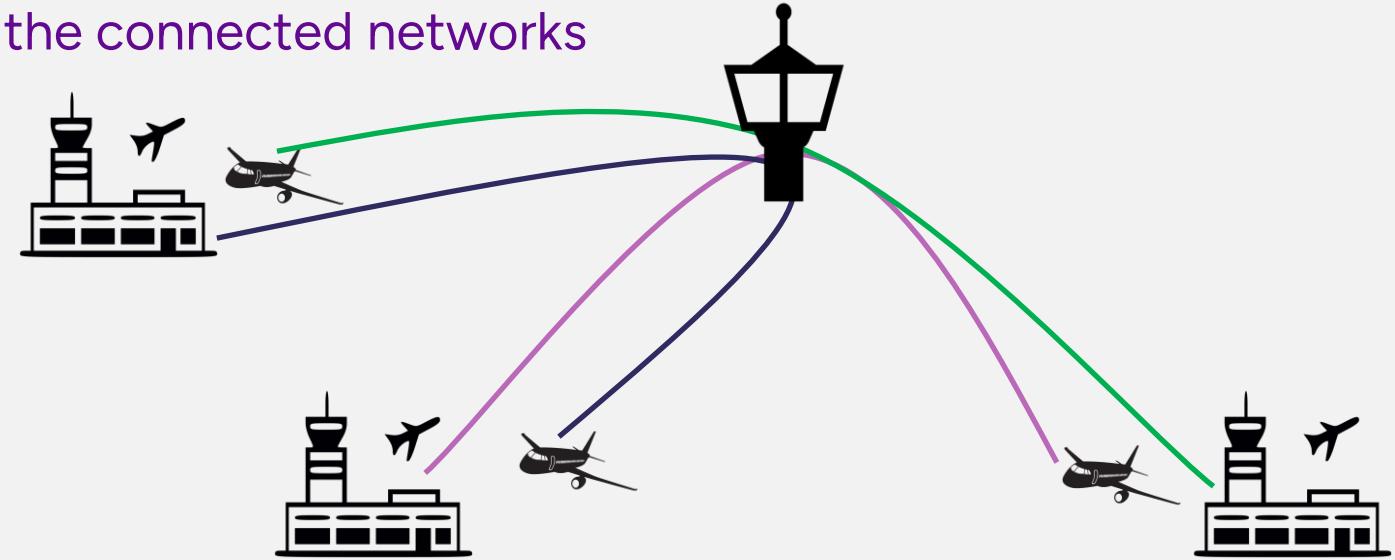
- The centralized hub is responsible for managing and directing all traffic between connected networks
- Spokes are the connected networks



NIC
EMPOWER

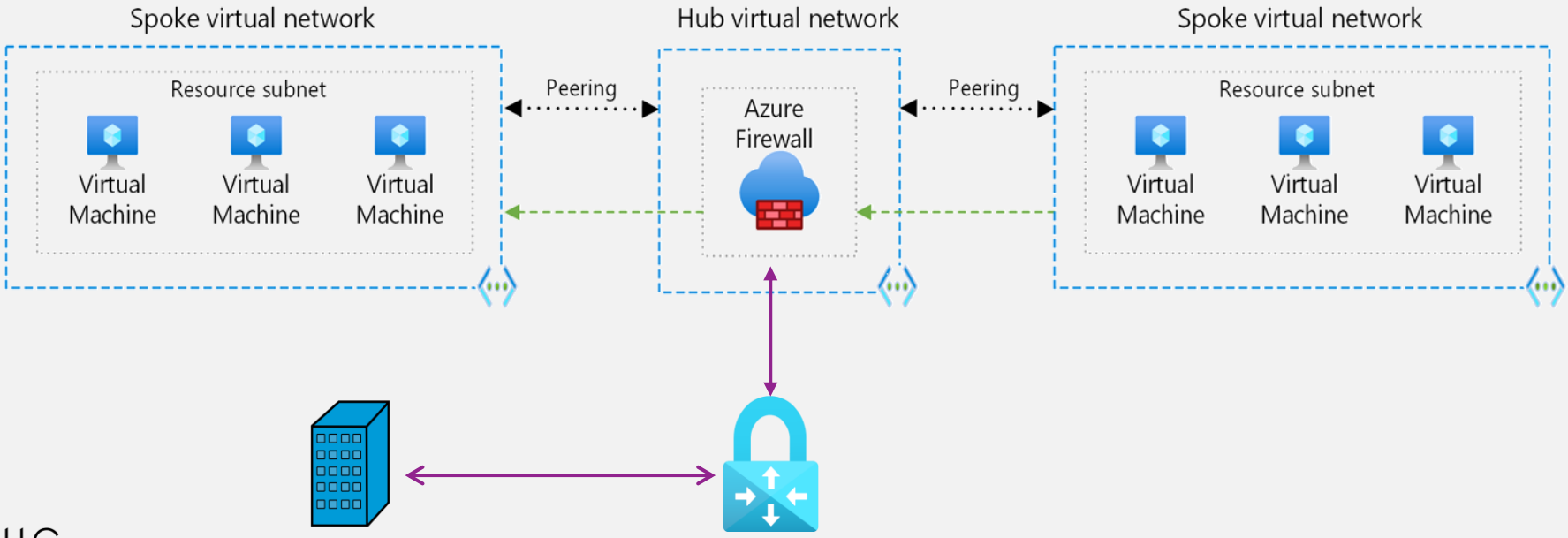
Hub and spoke

- The centralized hub is responsible for managing and directing all traffic between connected networks
- Spokes are the connected networks

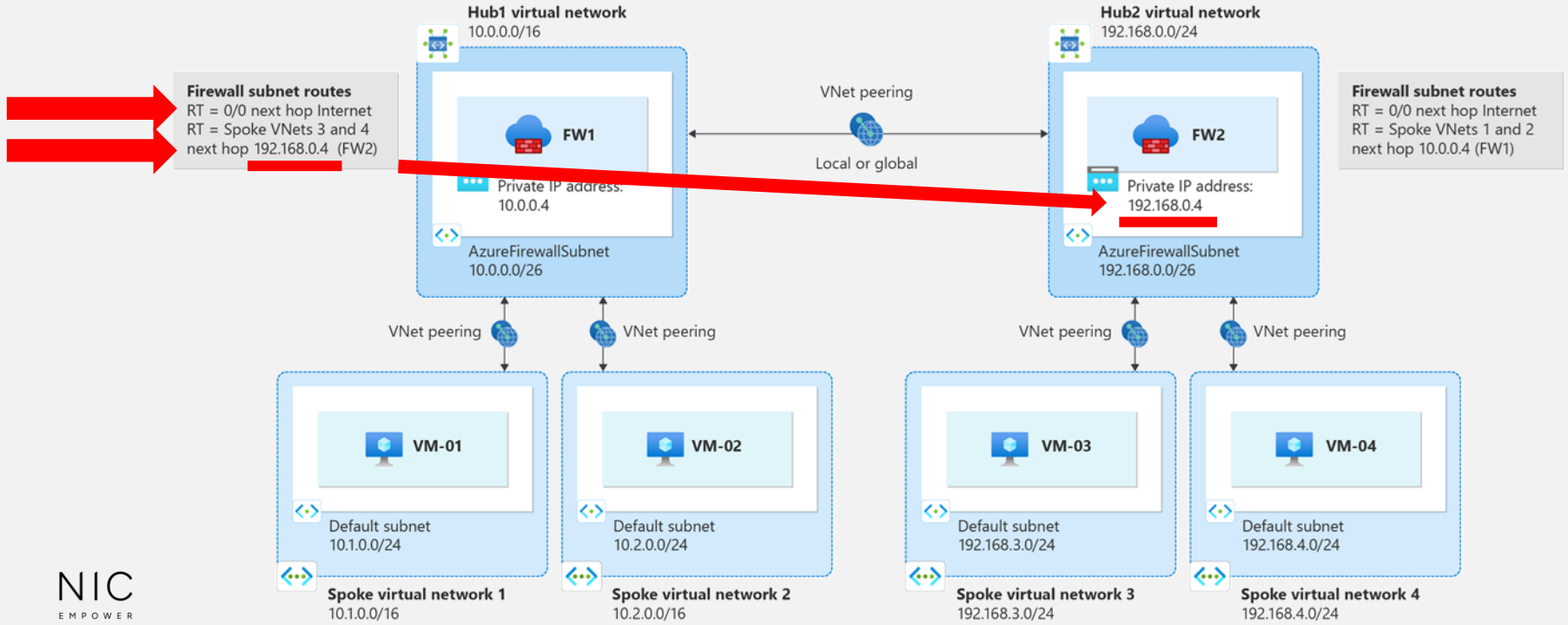


NIC
EMPOWER

Hub and spoke - single region



Hub and spoke - multi region



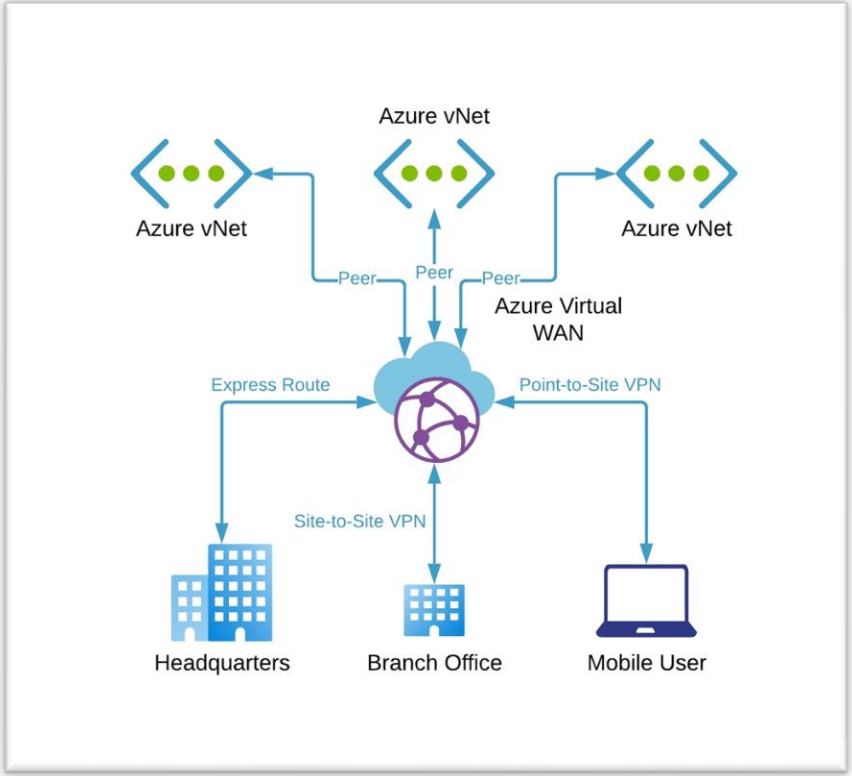
NIC
EMPOWER

Azure Virtual WAN

Azure Virtual WAN

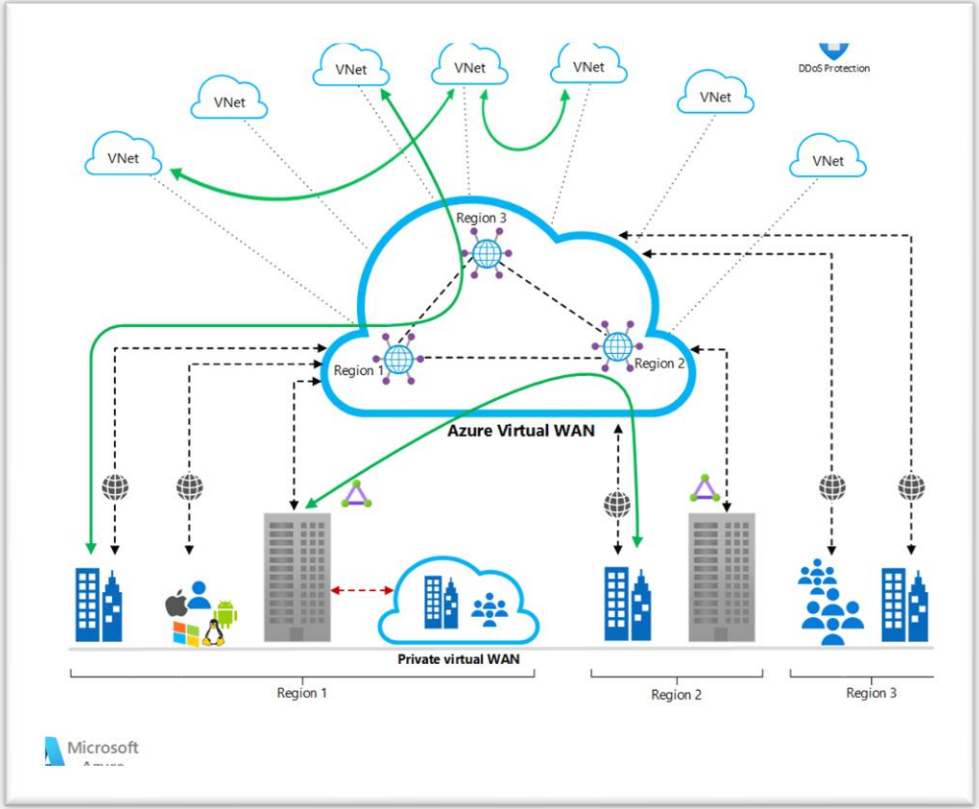
- Centralized management
- Pricing / SKU
  - Basic vs Standard SKU
  - € 270.41 / NOK 3,201.63
  - Data processing (€0.019 / NOK 0.219)
- Scalable
  - Multi regional
  - Scale units
- Gateways
- Security Providers
  - Zscaler, Check Point, iboss
- Third-party providers
  - Aruba, Barracuda, Checkpoint, Cisco, Fortinet, VMWare (NVA)
  - Palo Alto (SaaS)

Azure Virtual WAN – single region



NIC
EMPOWER

Azure Virtual WAN – multi region



NIC
EMPOWER

Routing in Virtual WAN

- BGP
- Routing Intent
- Propagated
- Spoke route tables

Demo time!

Now tell me about the tricky stuff!

Resource visibility

- You won’t see most of the resources in the resource groups
- Making debugging hard

Firewall SKU

- Firewall resource has a very specific SKU for use with vWAN

- [--sku {AZFW_Hub, AZFW_VNet}]

Secure routing

- If you forget to set your routing intent correct, default routing is not set to your firewalls
- Updating your secure routing settings will briefly interrupt your virtual network connections

Other networking services

- Cannot directly integrate other network services, examples:
  - Bastion
  - Application Gateway
  - DNS Private Resolver

- This requires an additional virtual network resource as a connected ’spoke’

Application Gateway

- The default route should always route 0.0.0.0/0 to the Internet
- You will get the Application Gateway in an error state if it is not configured correctly

Spoke Route Tables

- If you create custom Route Tables for your spoke networks, remember to **NOT** turn off gateway propagation

P2S VPN configurations

- Point-to-Site configuration are created on the Virtual WAN resource
- A configuration is linked to a Virtual Hub within your Virtual WAN
- You can only link a single Point-to-Site VPN configuration to a Virtual Hub

Thanks!

Patrick de Kruijf
Azure Architect | Global Landing Zone Solution Lead

Xebia