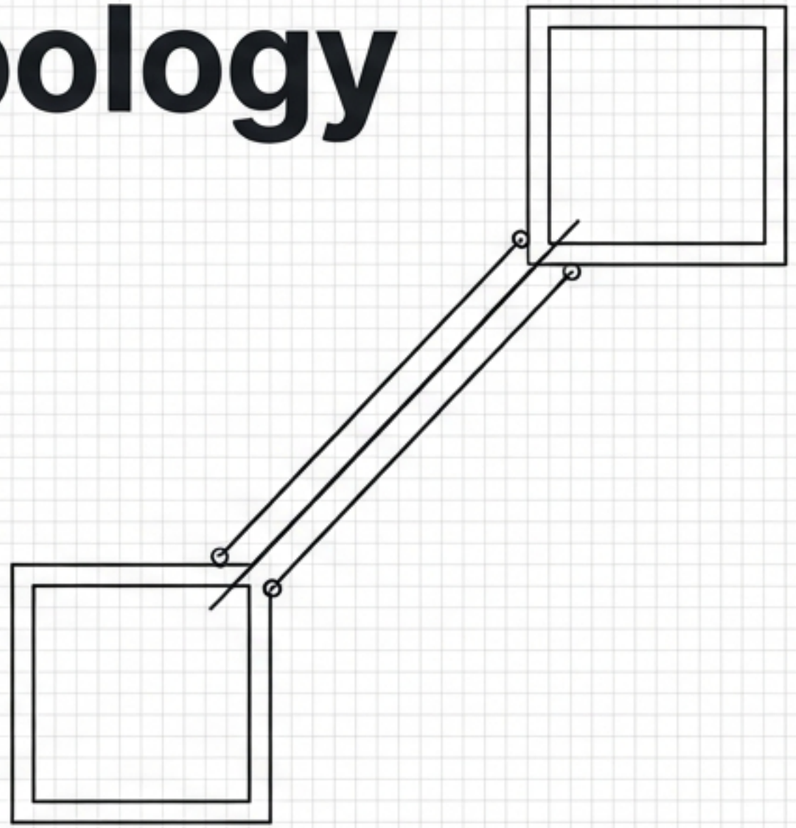
Azure Hub-Spoke Topology

Infrastructure Definition

Technical analysis of the “nf-hub-spoke” ARM deployment template.



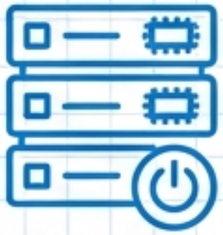
AUTHOR	DEPLOYMENT DATE	REGION	SCHEMA VERSION
Nick Fennell	06/20/2025	West Europe	1.0.0.0

THE TOPOLOGY OVERVIEW

HUB ZONE (Connectivity & Compute)

```
Resource: nf-hubvnet
CIDR: 172.16.0.0/16
```

VPN Gateway



Virtual Machines

VNet Peering

SPOKE ZONE (Ingress)

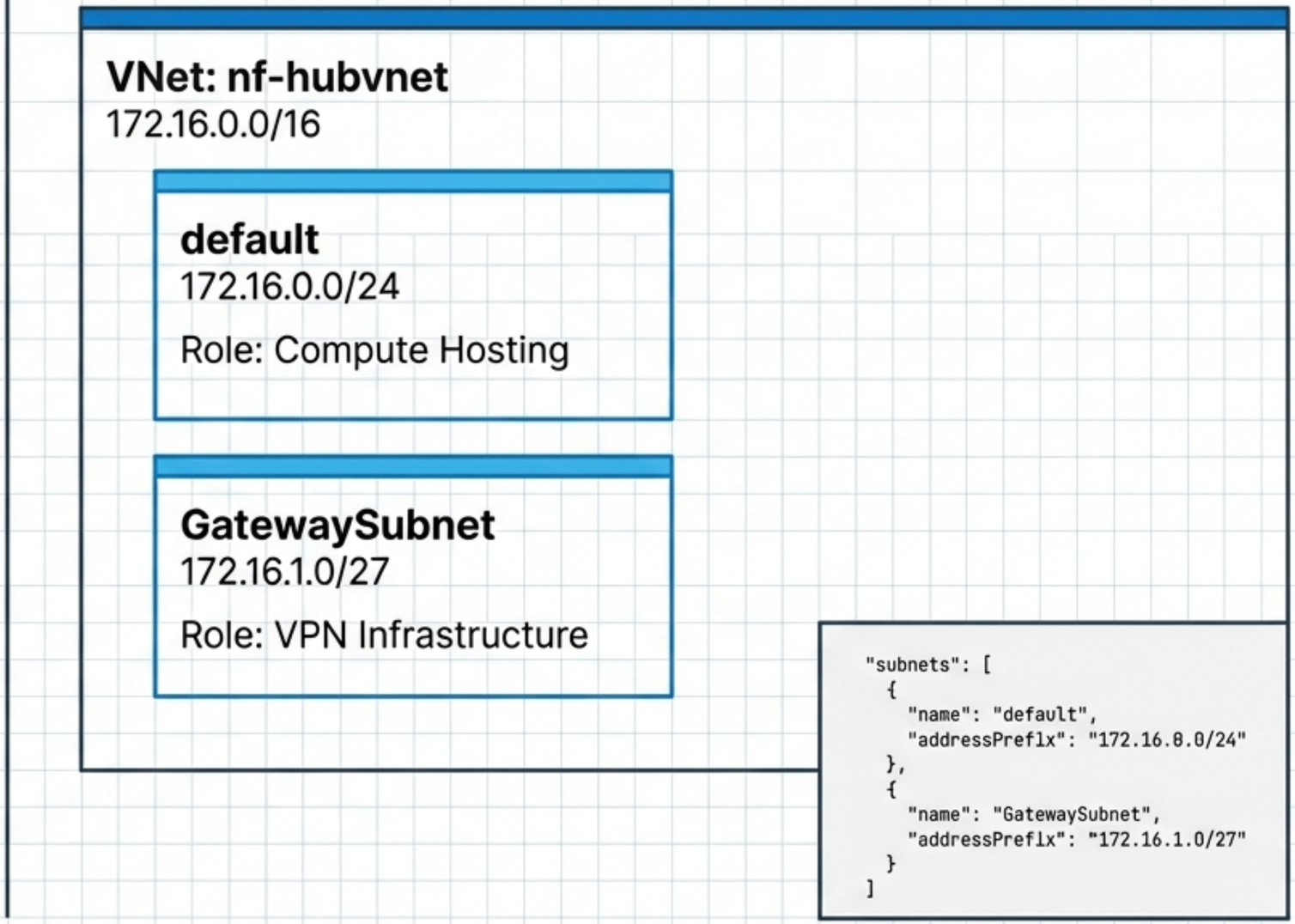
```
Resource: nf-vnet-appgw
CIDR: 10.14.0.0/16
```

Application Gateway

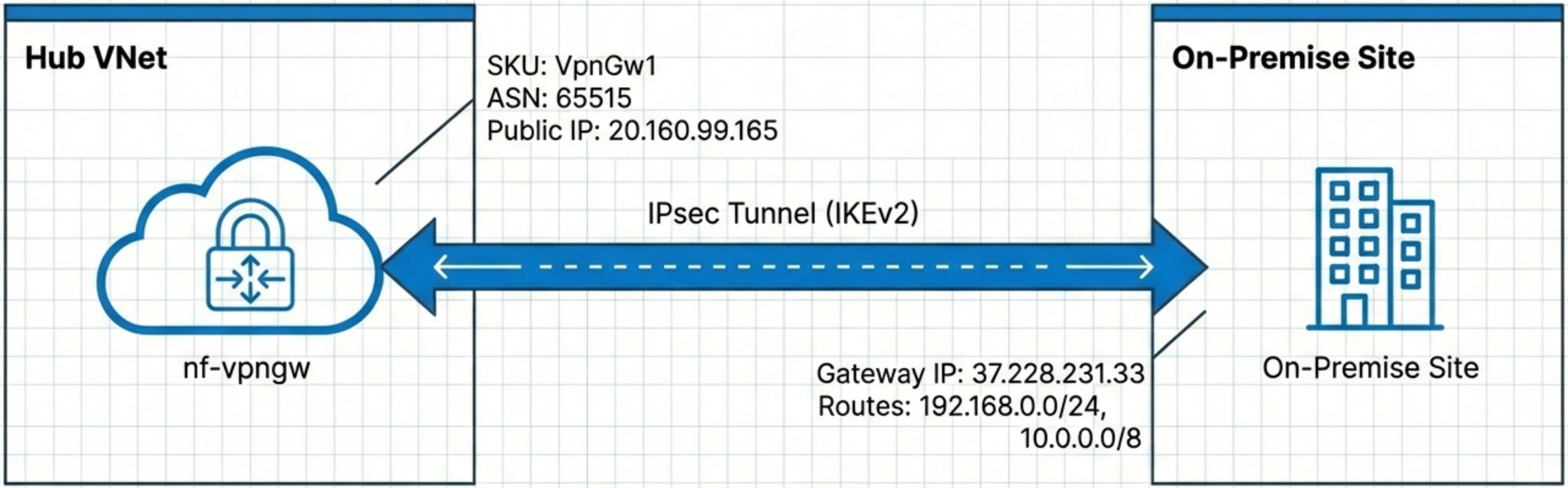
KEY INSIGHT: A decentralized ingress model where the Spoke manages external web traffic, while the Hub manages on-premise connectivity and compute workloads.

Hub Infrastructure: nf-hubvnet

Address Space	172.16.0.0/16
Location	West Europe
DDoS Protection	Disabled
Encryption	Disabled

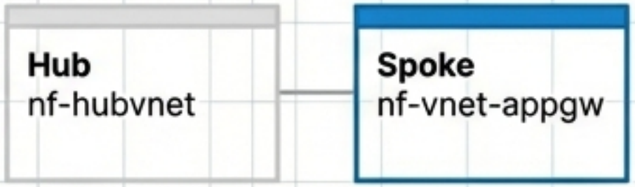


Hybrid Connectivity: VPN Gateway



KEY INSIGHT: The Local Network Gateway instructs Azure to route traffic for the 10.x and 192.168.x ranges through the IPsec tunnel to 37.228.231.33.

Spoke Infrastructure: nf-vnet-appgw



Network Identity

Name: `nf-vnet-appgw`

Address Space: `10.14.0.0/16`

Subnet Configuration

default Subnet

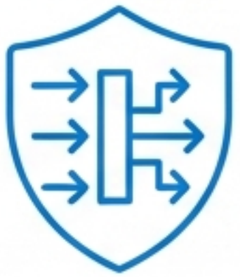
Range: `10.14.0.0/24`

Delegation: None

Strategic Context

This VNet is dedicated to Ingress. By isolating the Application Gateway in a separate 10.14.x.x network, we decouple edge security management from the 172.16.x.x compute/hub environment.

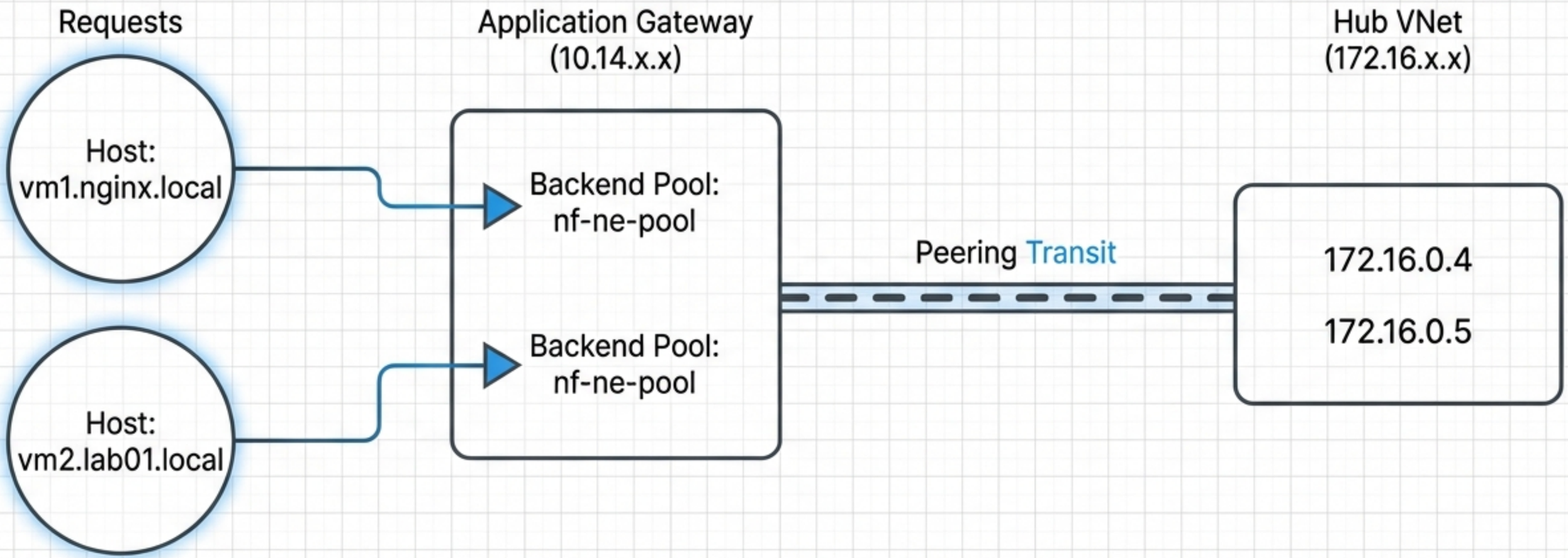
Intelligent Ingress: Application Gateway



Resource: nf-appgw	
Hardware Tier:	Standard_v2 (Generation 1)
Scaling:	Autoscale: Min 1 / Max 10 Instances
Resilience: Frontend:	Availability Zones: 1, 2, 3 Public IP: 132.220.237.71
Listener:	Port: 80 (HTTP)

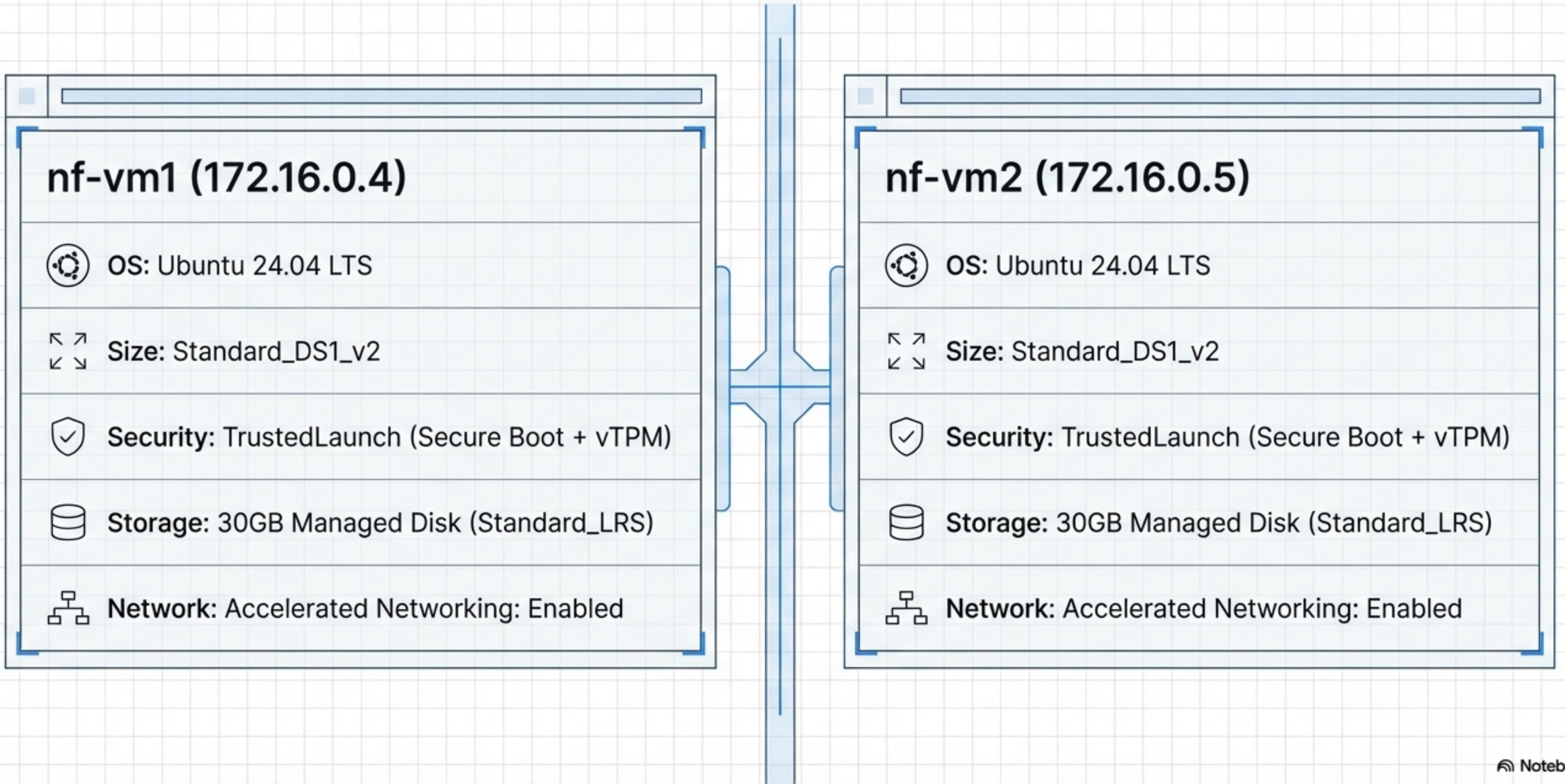
ⓘ WAF Policy: Not Enabled (Basic Load Balancing Only)

Ingress Routing Logic



Cross-VNet Routing: The Application Gateway in the Spoke (10.14.x.x) targets IP addresses located in the Hub (172.16.x.x), relying on the peering link for connectivity.

Compute Resources: The Workload



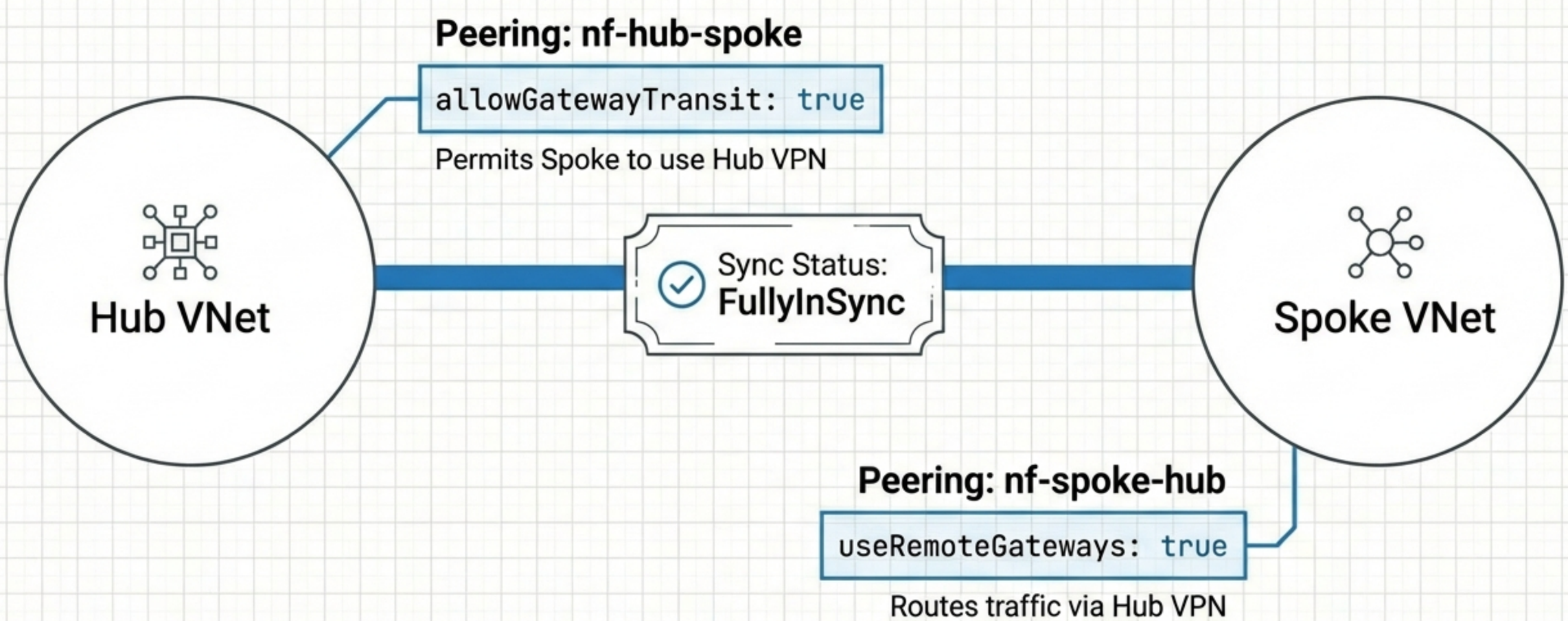
Network Security Groups (NSG)

Active Rules (nf-vm1-nsg, nf-vm2-nsg)

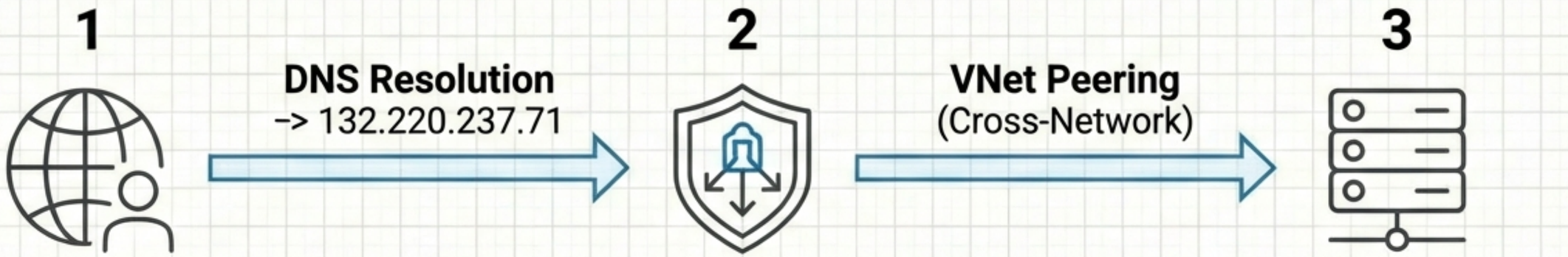
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	ACTION
1000	default-allow-ssh	22	TCP	* (Any)	Allow

SECURITY CONFIGURATION NOTE: SSH (Port 22) is currently exposed to the entire internet (‘*’). Production hardening is recommended to restrict Source Address Prefix to known admin IPs or VPN ranges.

Inter-Network Connectivity: Peering



End-to-End Traffic Flow



Total Hops: 2 (Public Edge -> Private Hub)

Governance & Deployment Summary

Tagging Strategy

Creator:	Nick Fennell
DateCreated:	06/20/2025

Resource Checklist

- [x] Hub VNet & Gateway Subnet
- [x] VPN Gateway (ASN 65515)
- [x] Spoke VNet (Ingress Isolation)
- [x] Application Gateway (Standard_v2)
- [x] Compute (Ubuntu 24.04 VMs)
- [x] Peering (Gateway Transit Enabled)

TOPOLOGY DEFINED AND VALIDATED FOR WEST EUROPE DEPLOYMENT.