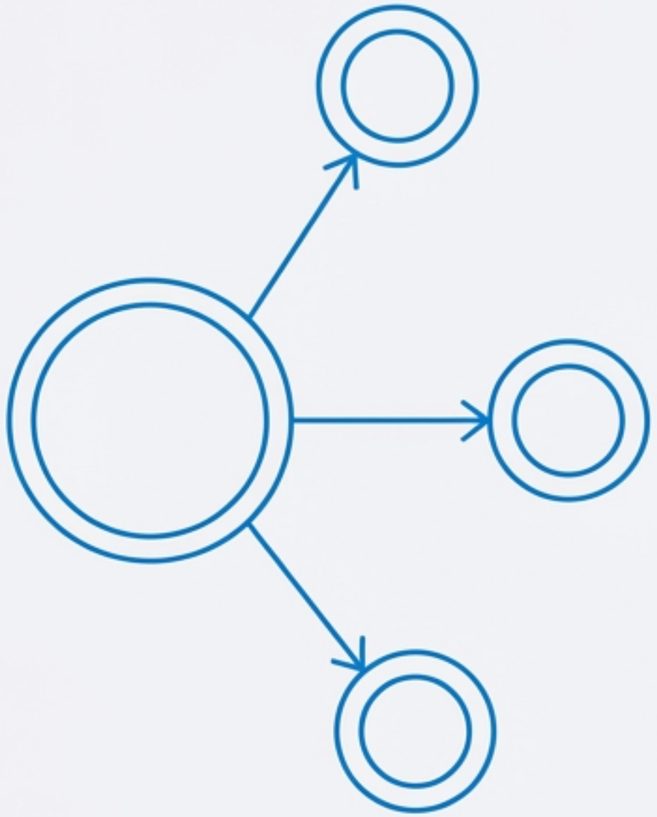
Azure Virtual WAN & Private DNS Architecture

Infrastructure-as-Code Deployment Blueprint

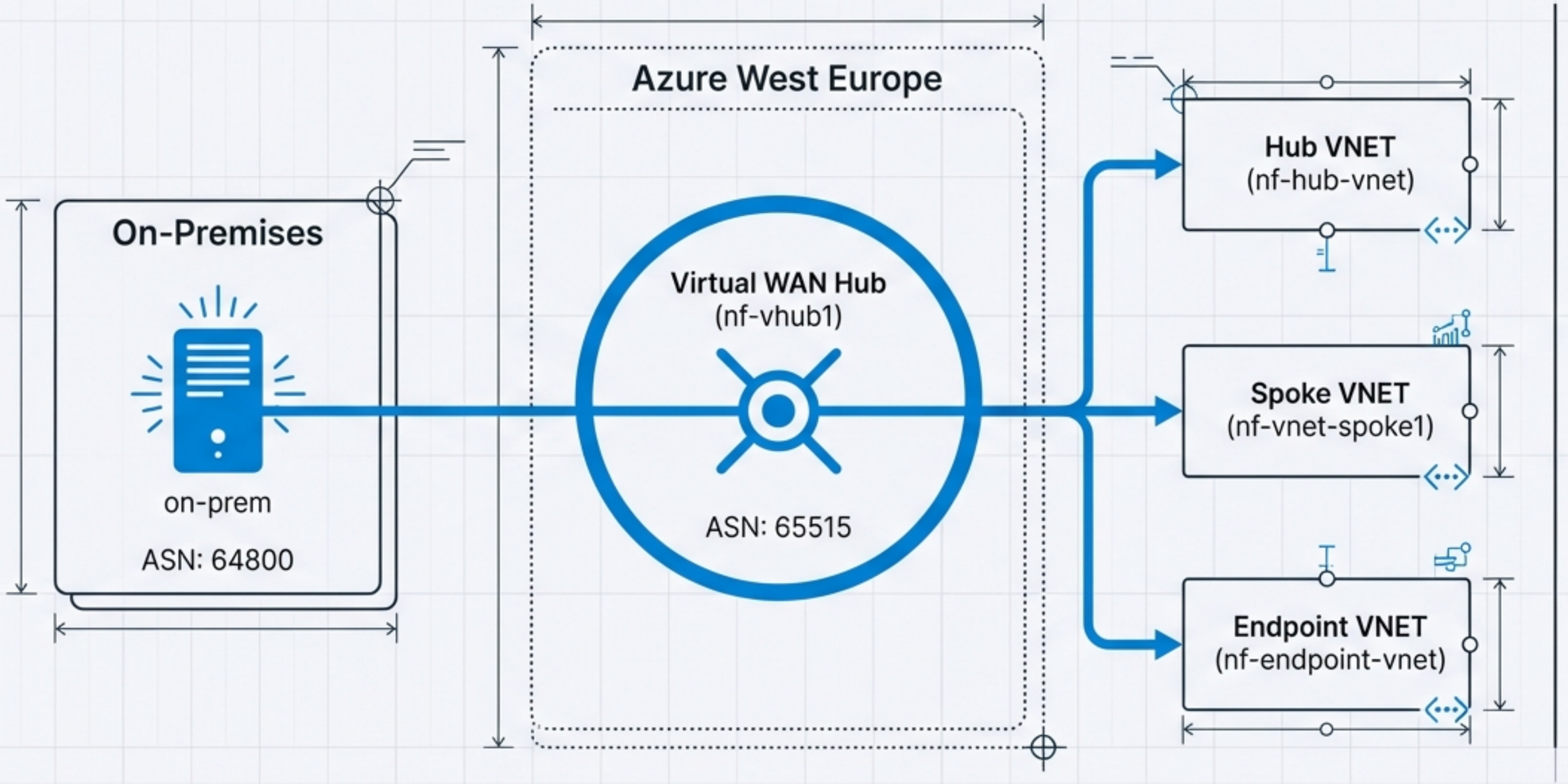


DEPLOYMENT REGION: West Europe

RESOURCE GROUP: NF-RG01

ARCHITECTURE TYPE: Hybrid Hub-and-Spoke

Architectural Topology: The Big Picture



Key Metrics

Primary Hub Address:
172.17.0.0/24

Hub Routing Preference:
VpnGateway

Virtual Router ASNs:
65515 (Azure) /
64800 (Remote)

The Connectivity Core: Virtual WAN & Hub

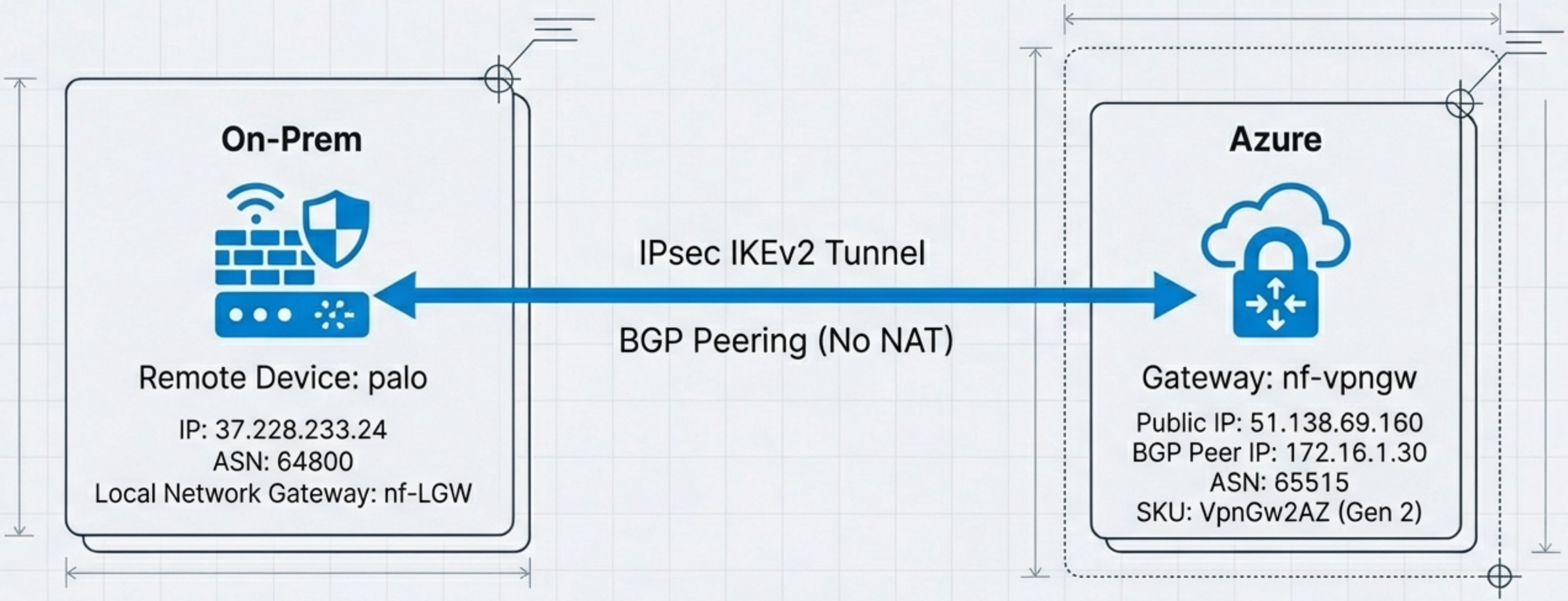
Resource Configuration

- **Resource:** nf-vwan (Type: Standard)
- **Feature:** allowBranchToBranchTraffic: true
- **Feature:** disableVpnEncryption: false
- **Virtual Hub:** nf-vhub1
- **Routing Engine:** Virtual Router
- **Hub IPs:** 172.17.0.69, 172.17.0.68
- **Scaling:** minCapacity: 2

```
{
  'type': 'Microsoft.Network/virtualHubs',
  'name': 'nf-vhub1',
  'properties': {
    'sku': 'Standard',
    'virtualRouterAsn': 65515,
    'hubRoutingPreference': 'VpnGateway',
    'virtualRouterIps': [
      '172.17.0.69',
      '172.17.0.68'
    ]
  }
}
```

Technical Blueprint / Engineering Precision

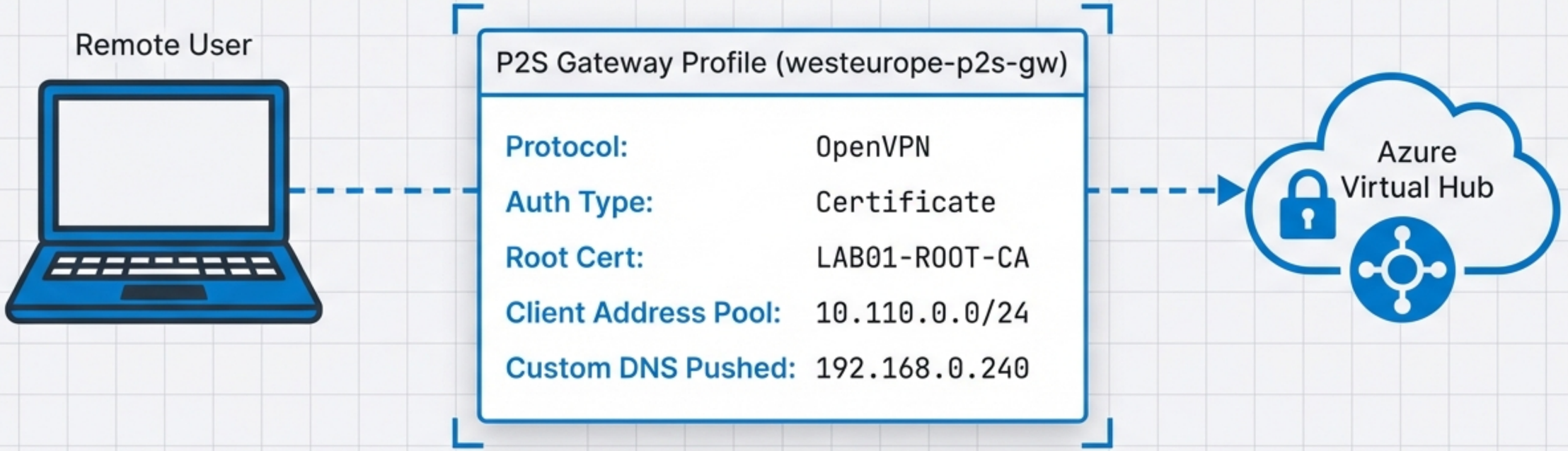
Hybrid Integration: Site-to-Site VPN



Direct BGP peering exchanges routes between On-Prem (10.0.0.0/8) and Azure aggregate.

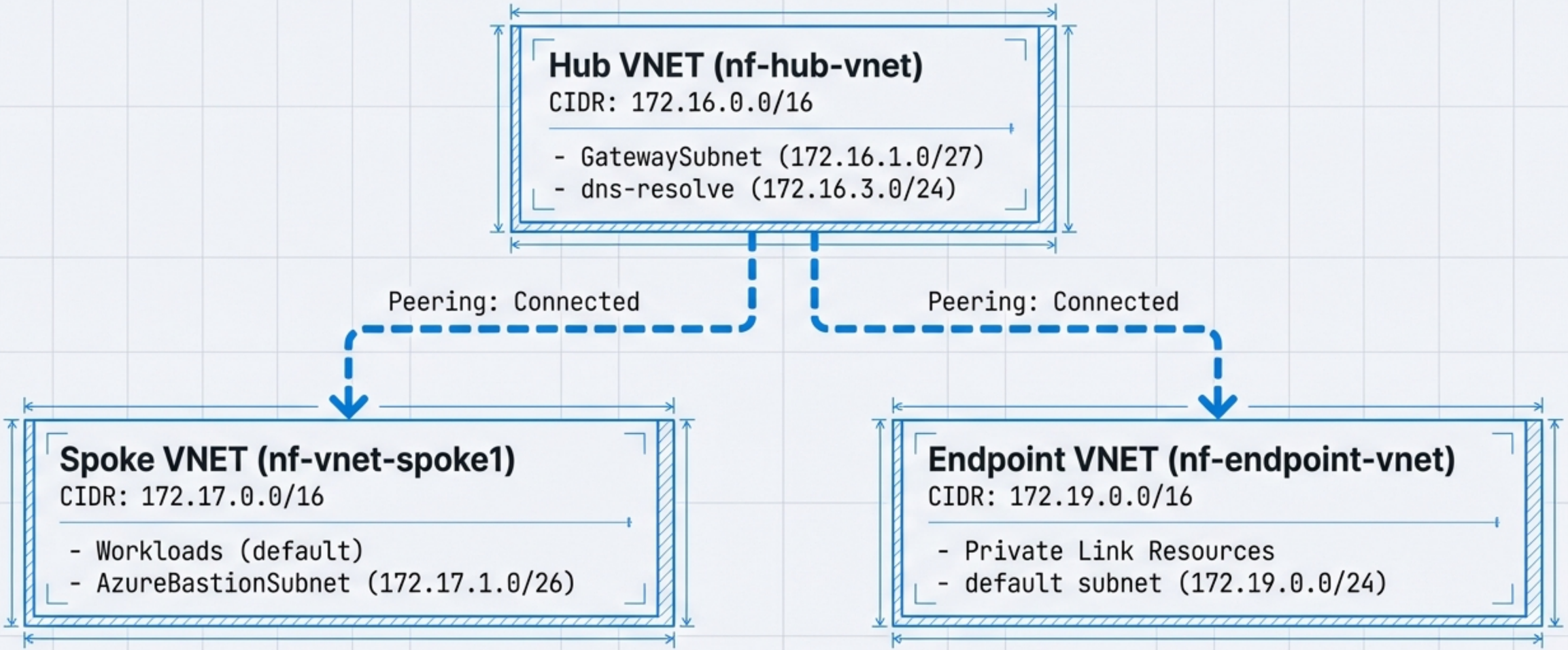
Technical Blueprint / Engineering Precision

User Access: Point-to-Site VPN Configuration



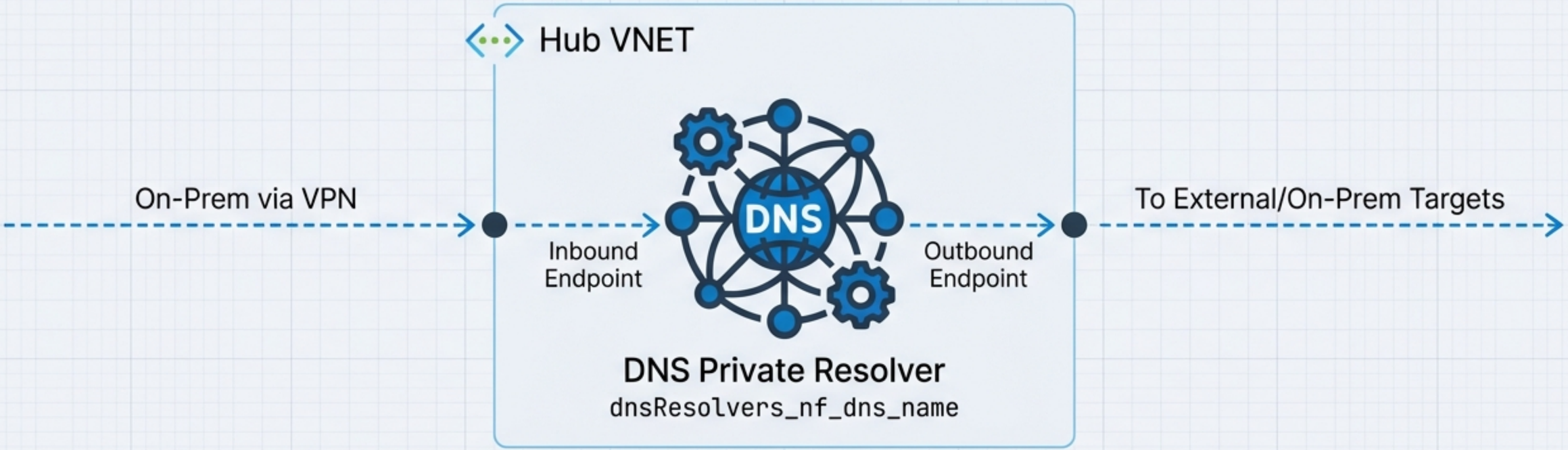
Technical Blueprint / Engineering Precision

Network Segmentation: The VNET Ecosystem



The Hybrid Bridge: DNS Private Resolver

Technical Blueprint / Engineering Precision

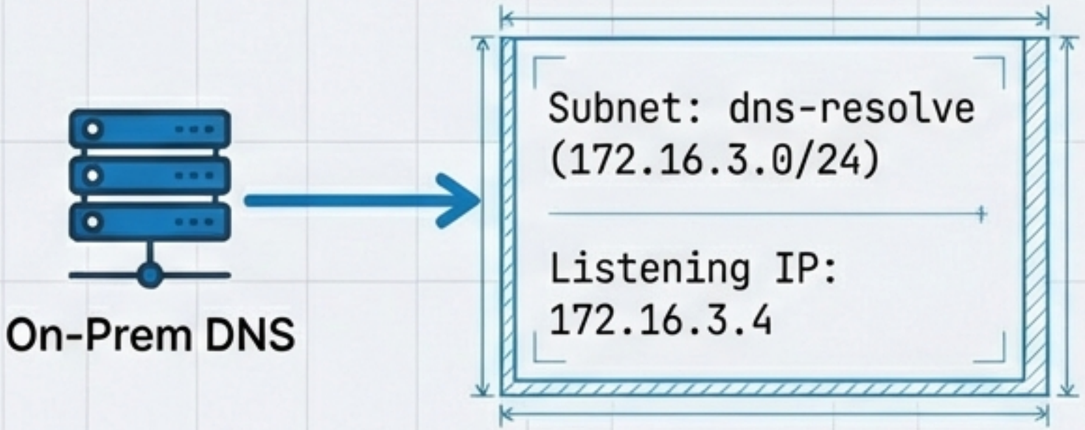


- **Function**: Bridges native Azure DNS with On-Premise servers.
- **Location**: Strictly deployed within `nf-hub-vnet`.
- **Scope**: Shared service accessible to all peered spokes and connected VPN clients.

Technical Blueprint / Engineering Precision

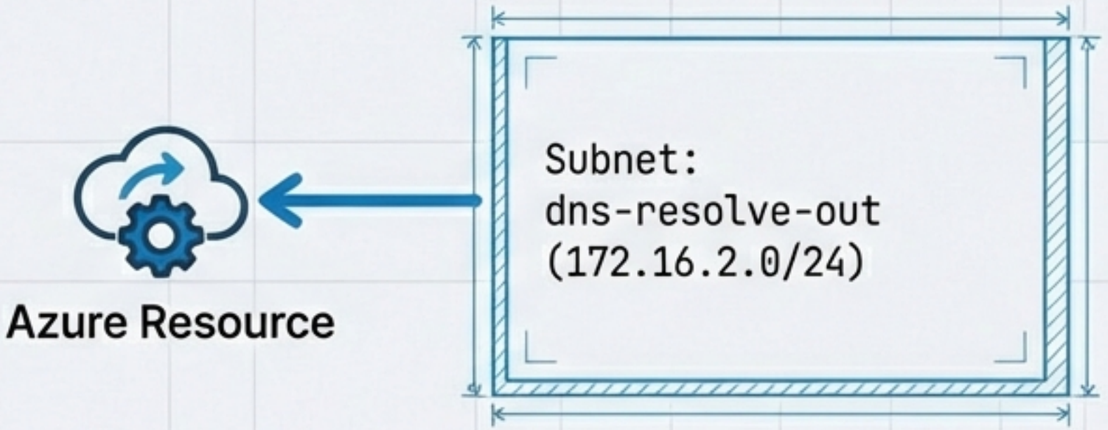
DNS Mechanics: Inbound & Outbound Flows

Inbound Configuration



Receives queries for *.core.windows.net from on-premise.

Outbound Configuration



Exit point for DNS traffic originating in Azure resolving custom external domains.

Intelligent Resolution: DNS Forwarding Rulesets

Technical Blueprint / Engineering Precision

Virtual Network Links

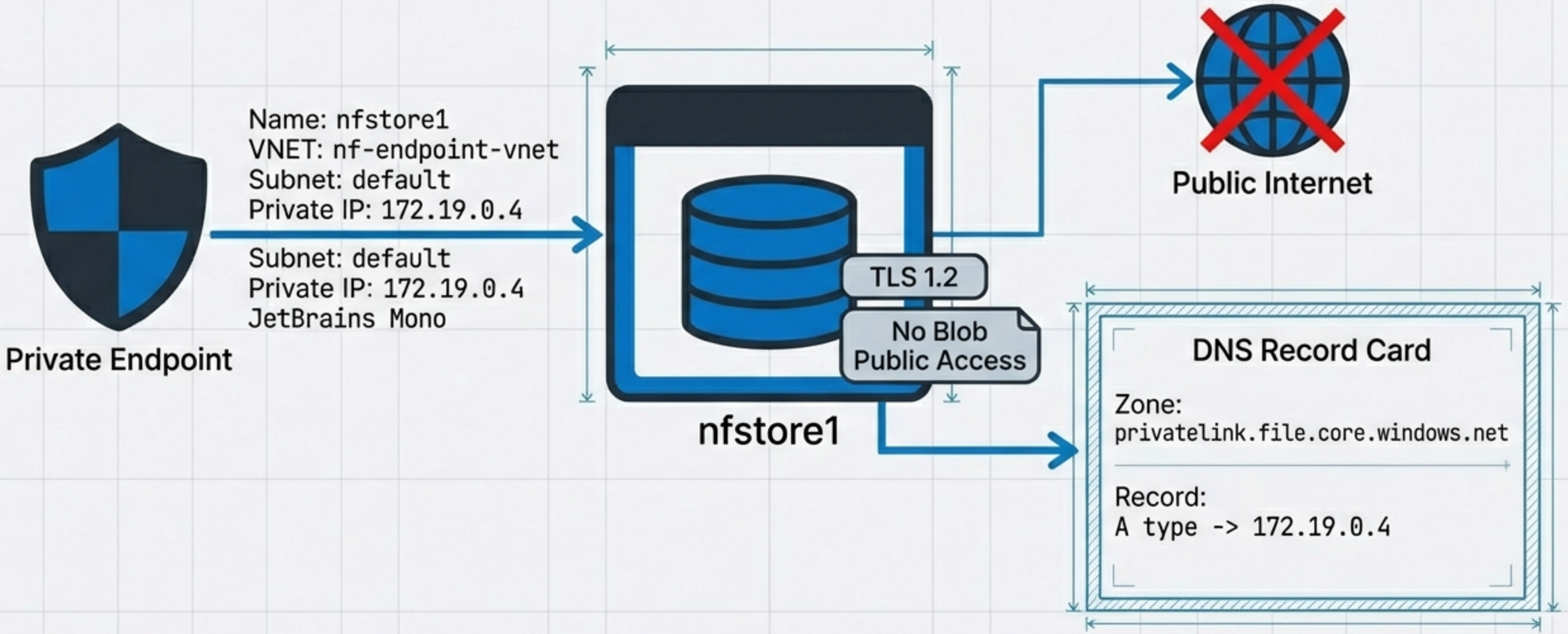
Linked to: nf-hub-vnet

Linked to: nf-endpoint-vnet

Loopback configuration ensures Azure resources use managed resolver logic for Private Endpoint mapping.

Technical Blueprint / Engineering Precision

Secured Data: Private Link & Storage



Workload Infrastructure: The Spoke VM

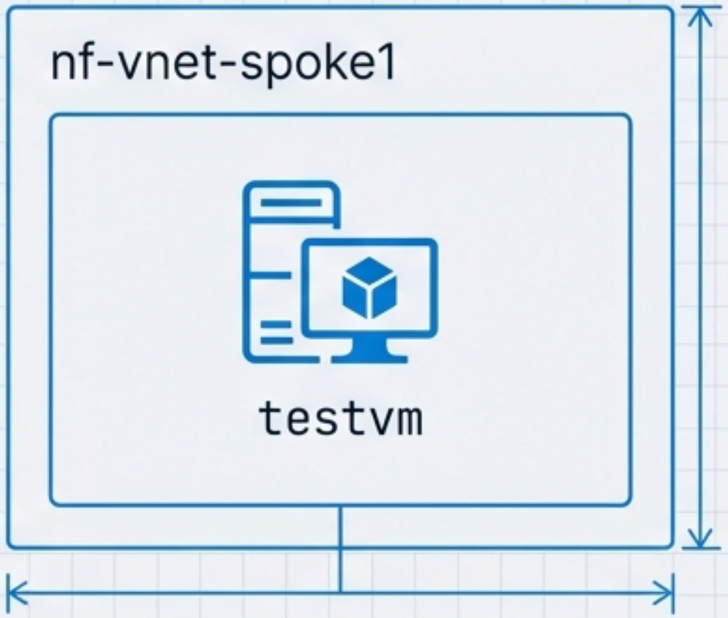
Technical Blueprint / Engineering Precision

Spec Sheet

Resource: testvm

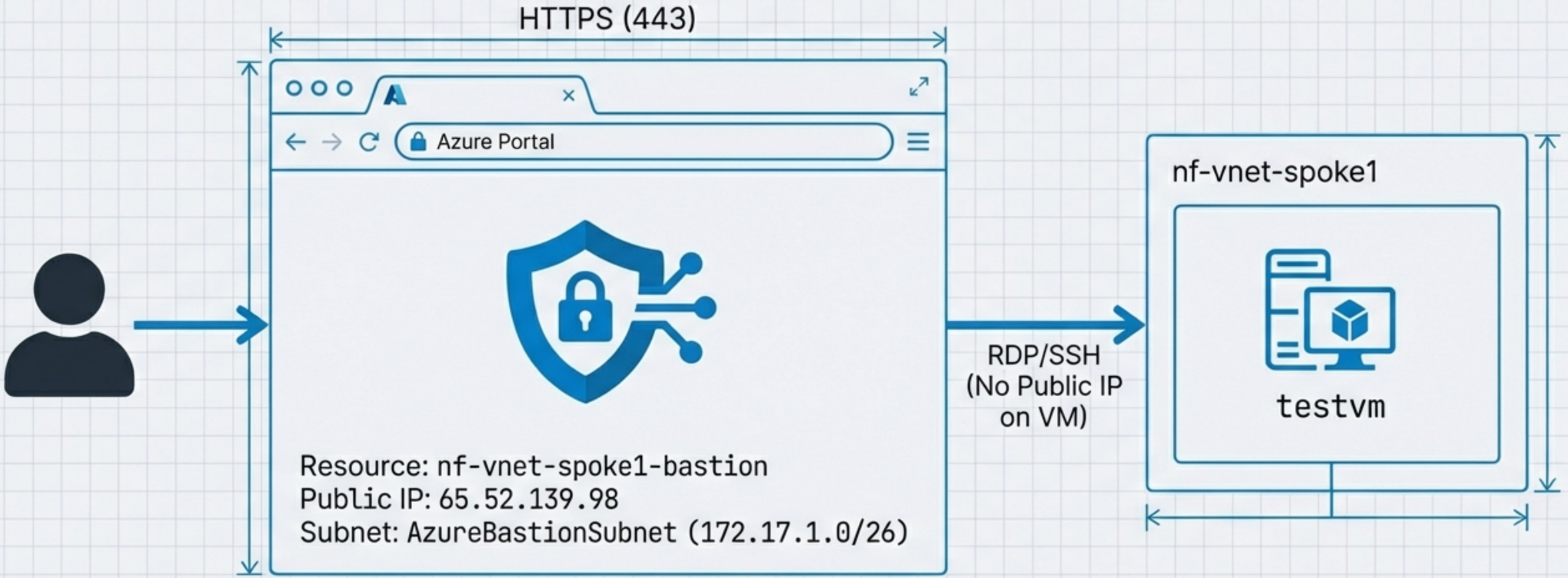
Location: nf-vnet-spoke1

Size	Standard_D2s_v3
OS	Ubuntu 24.04 LTS (Canonical)
Disk	30GB Managed Disk (Standard_LRS)
Interface	testvm896
Private IP	172.17.0.4 (Dynamic)
Features	Accelerated Networking: Enabled



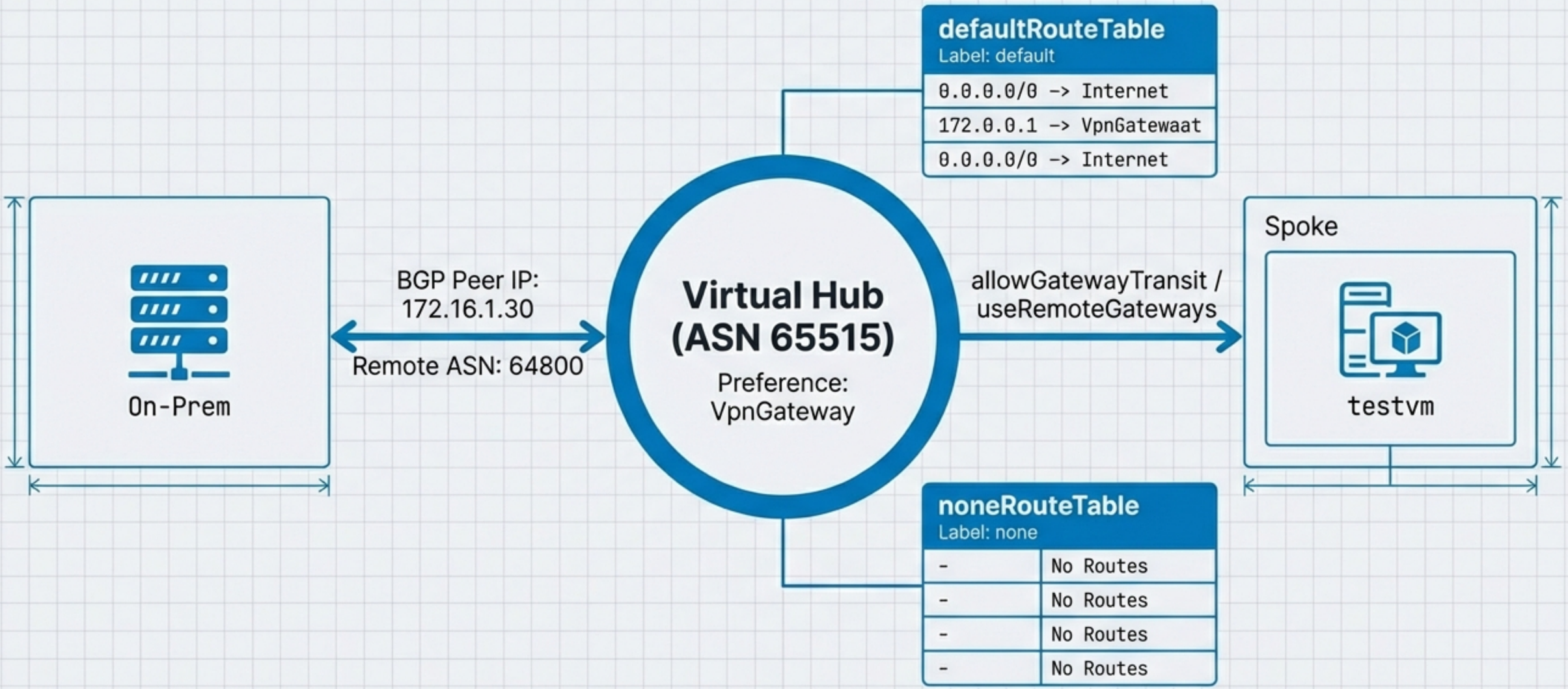
Secure Management: Azure Bastion

Technical Blueprint / Engineering Precision



Traffic Control: Routing & BGP

Technical Blueprint / Engineering Precision



Security Boundaries: Network Security Groups

Technical Blueprint / Engineering Precision

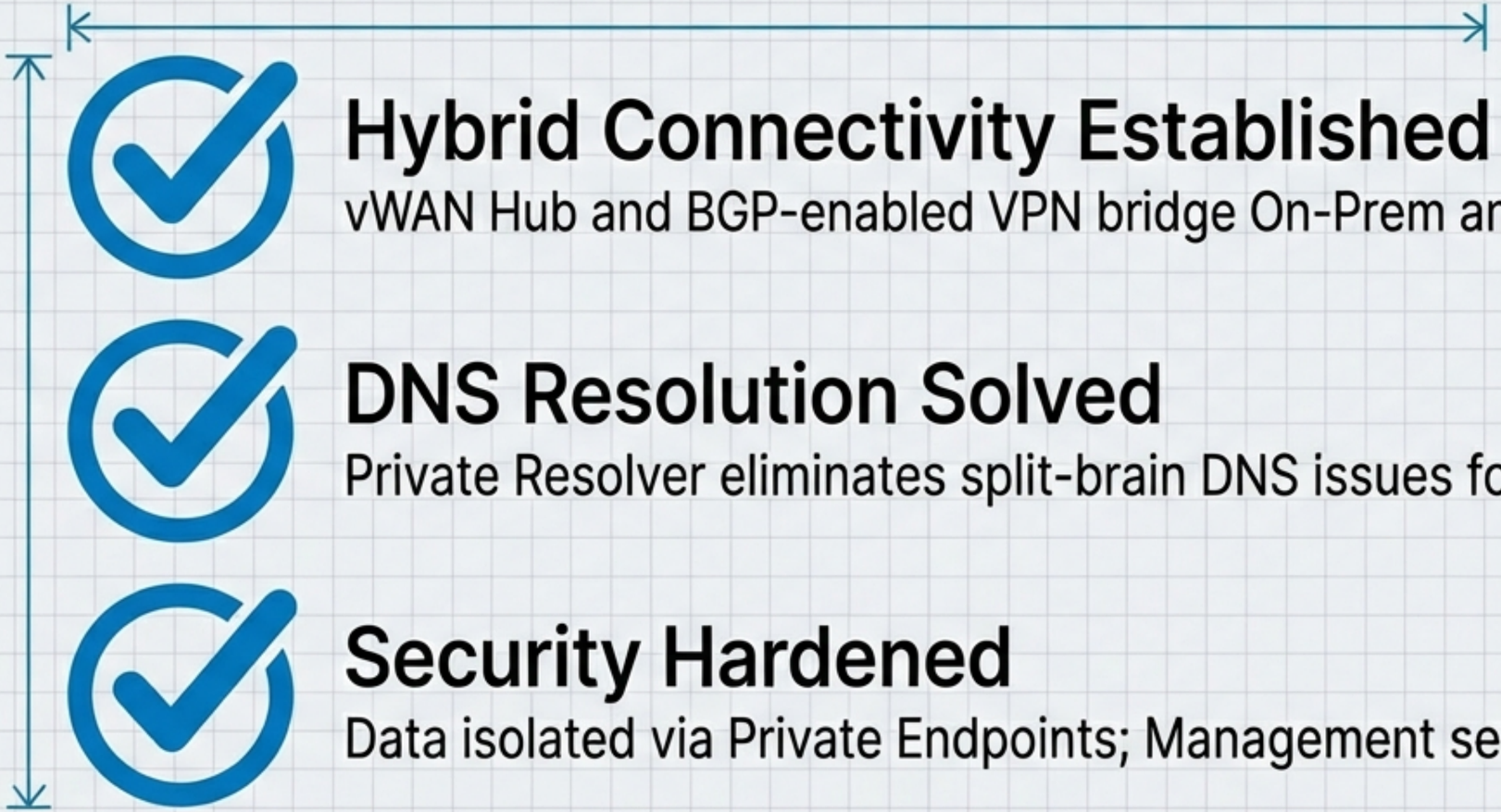
Applied to Interface: testvm896

Priority	Name	Direction	Access	Protocol	Source/Dest
100	AllowAnyCustomAnyInbound	Inbound	✅ Allow (Green)	Any (*)	Any / Any
100	AllowAnyCustomAnyOutbound	Outbound	✅ Allow (Green)	Any (*)	Any / Any

Current Configuration: Wide Open (Allow Any). Production recommendation: Restrict to application ports.

Deployment Summary: Production-Ready Backbone

Technical Blueprint / Engineering Precision



Hybrid Connectivity Established

vWAN Hub and BGP-enabled VPN bridge On-Prem and Azure.

DNS Resolution Solved

Private Resolver eliminates split-brain DNS issues for Private Links.

Security Hardened

Data isolated via Private Endpoints; Management secured via Bastion.

This architecture provides a validated pattern for secure, hybrid cloud networking.