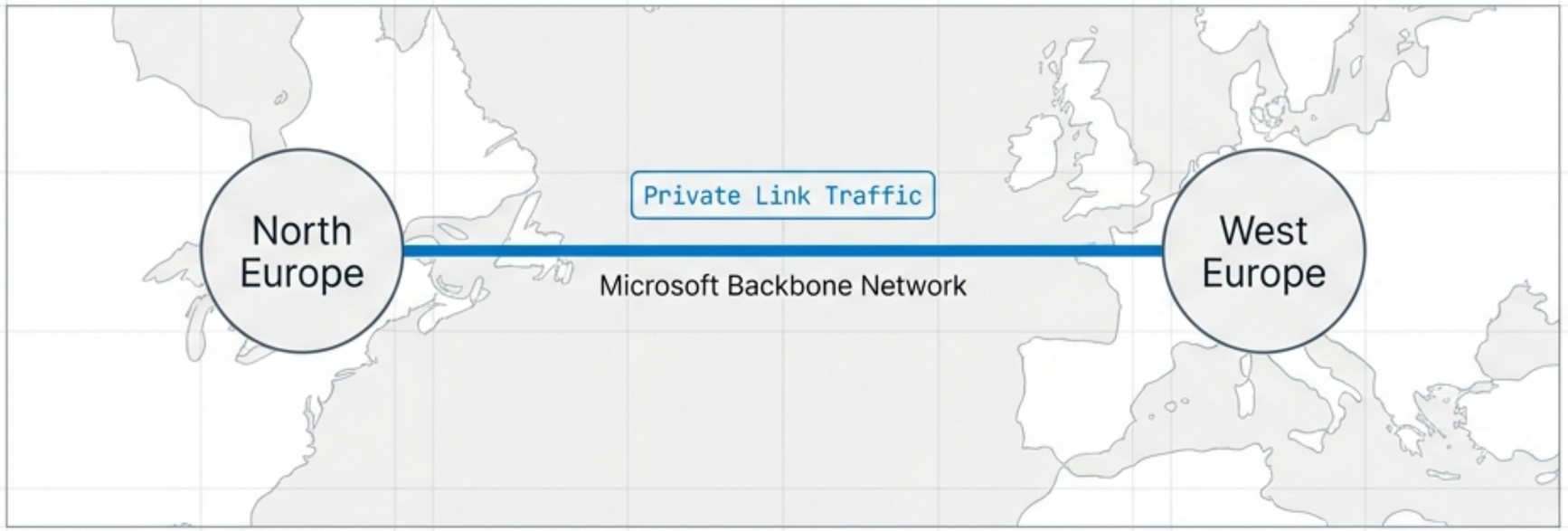
Azure Hybrid Networking & Private Service Projection

A reference architecture for consuming isolated, load-balanced services via Azure Private Link.



Architecture Type:
Hub-and-Spoke with Cross-Region Private Link

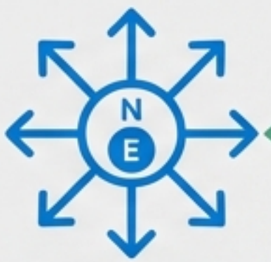
Core Components:
VPN Gateway (Hybrid), Standard Load Balancer, Private Link Service, Private Endpoint

Deployment Method:
Azure ARM Templates (JSON)

Dual-Environment Topology

The architecture is divided into two distinct logical and physical zones. Traffic does not traverse the public internet for service consumption; instead, it utilizes the Azure backbone.

The Consumer Hub

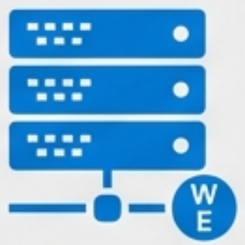


North Europe

Region: North Europe
Network Name: ‘vnet-hub’
Role: Hybrid connectivity entry point and service consumer
Key IP Space: ‘172.16.0.0/16’

Azure Backbone Connection
Direct Peering (No Public Internet)

The Provider Service



West Europe

Region: West Europe
Network Name: ‘testvm-vnet’
Role: Isolated, load-balanced application hosting
Key IP Space: ‘10.88.0.0/16’

The Consumer Hub: Network Foundation

vnet-hub (North Europe)

GatewaySubnet
172.16.1.0/27
Tag: Reserved for VPN Gateway

VMs
172.16.2.0/24
Tag: Workload hosting

PE-subnet
172.16.3.0/24
Tag: Dedicated for Private Endpoints

default
172.16.0.0/24

Configuration Note

Custom DNS server configured at '10.0.60.240'.

Indicates integration with existing enterprise identity or name resolution infrastructure.

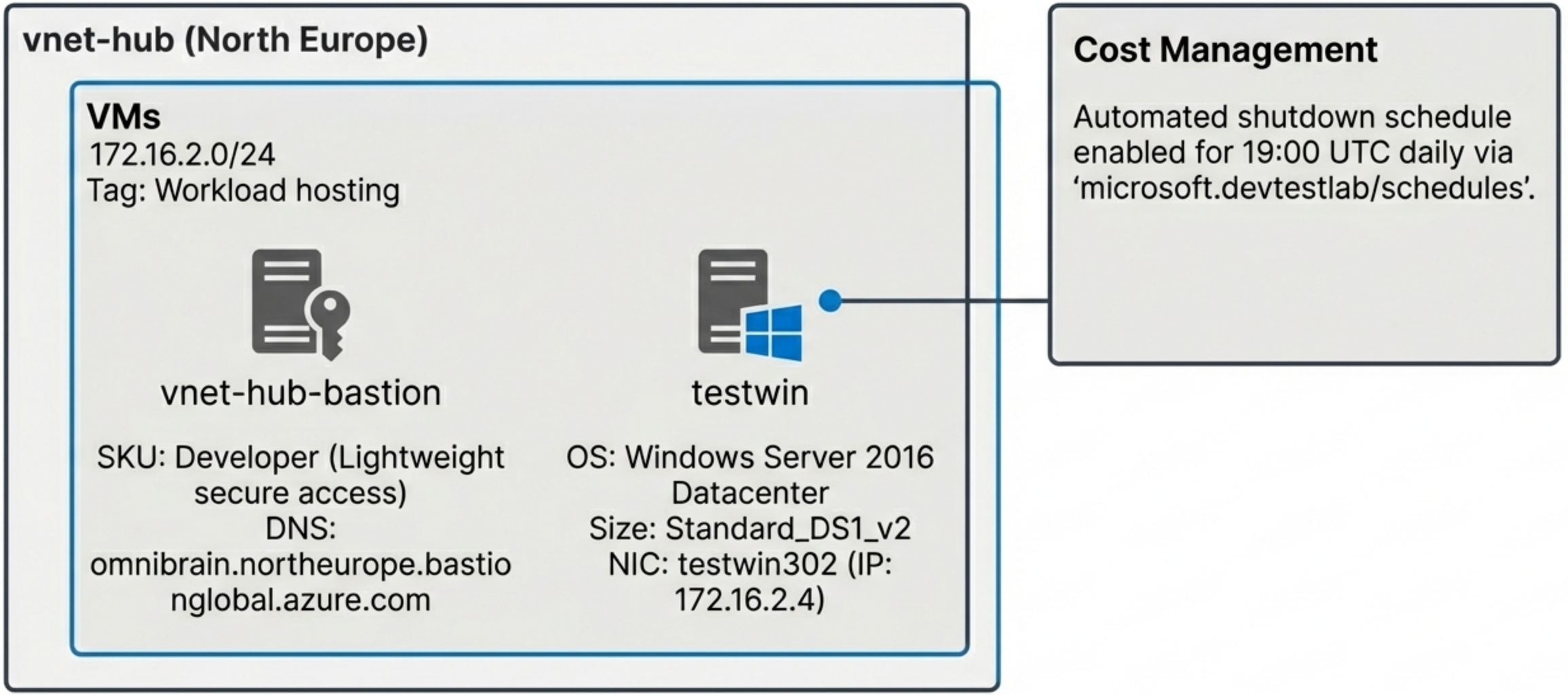
Hybrid Connectivity Bridge

The North Europe Hub extends the on-premises datacenter into Azure via a secure IPsec tunnel.

Local Network Gateway ‘LNGW’
IP: 37.228.233.173
Address Spaces: 192.168.0.0/24, 10.0.0.0/8

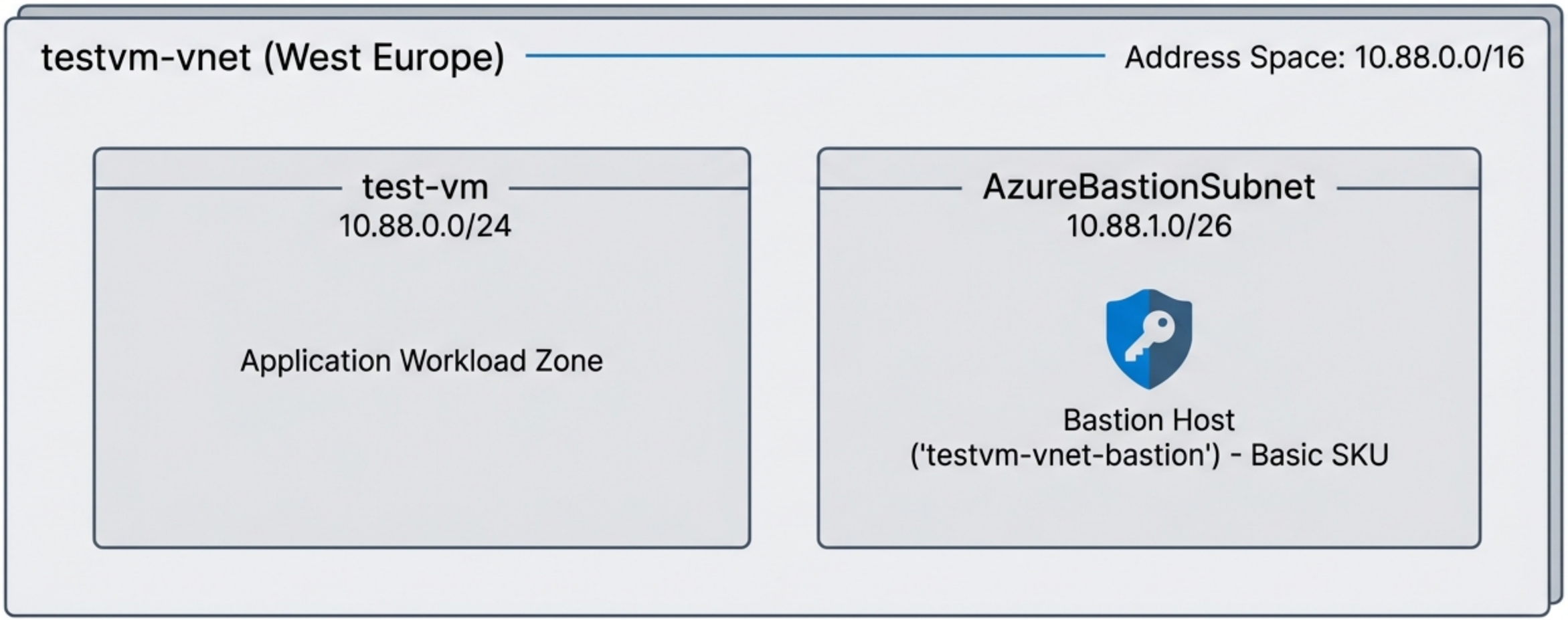
Resource: ‘vpn-gw’
SKU: VpnGw2AZ
Type: RouteBased, Generation 2, Active-Standby

Secure Management & Consumer Workloads

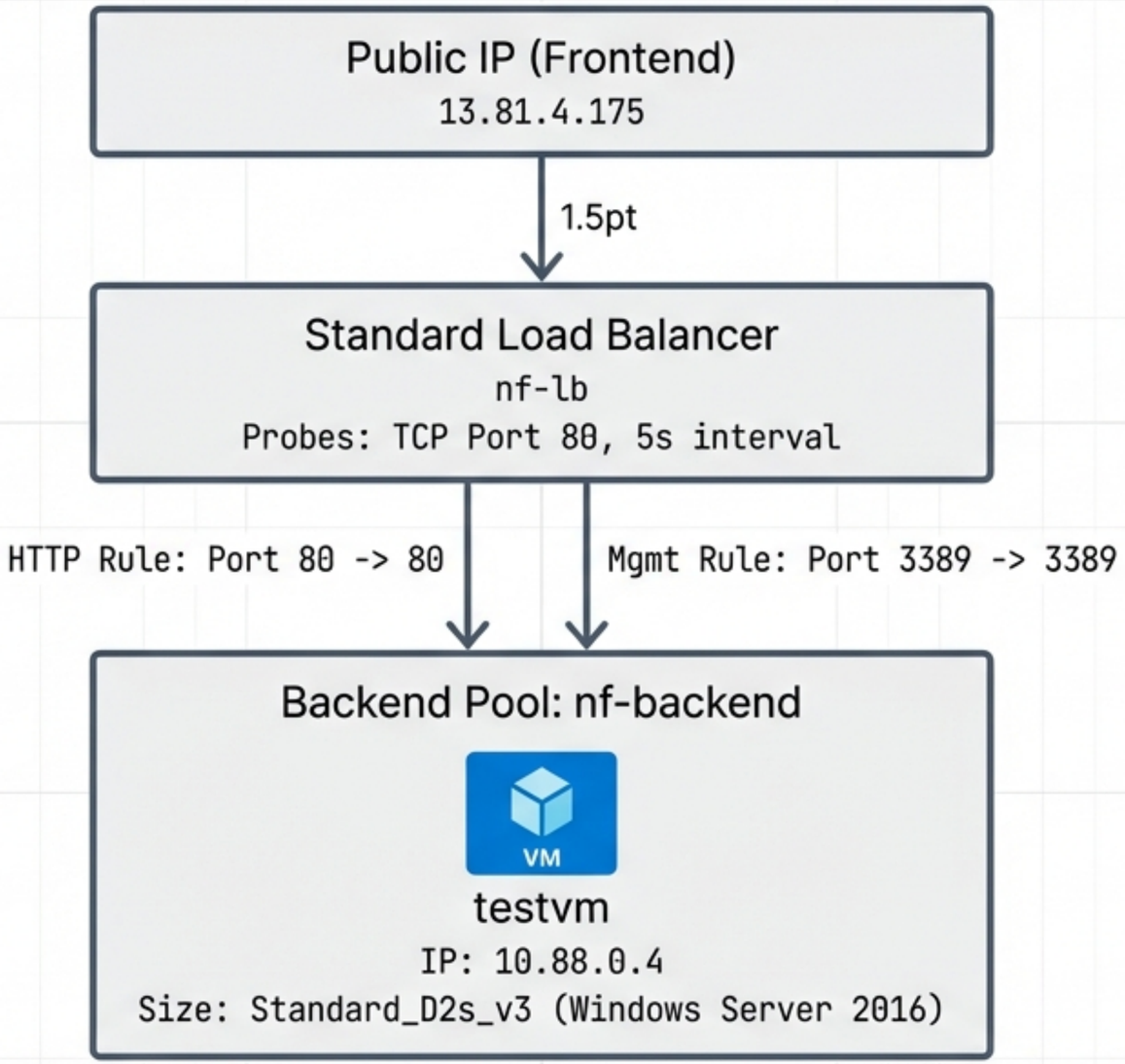


The Provider Environment: Service Isolation

Located in West Europe, the Provider network ('testvm-vnet') is designed as a self-contained unit, independent of the Hub's IP schema.

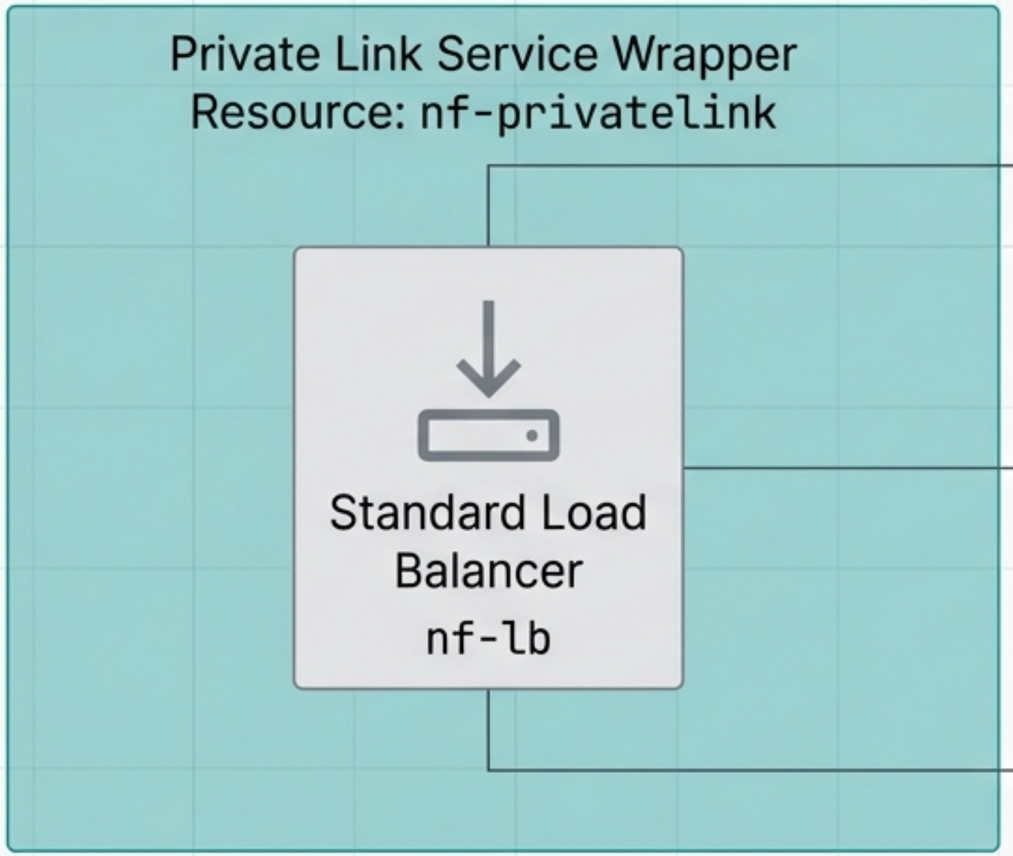


Traffic Distribution & Load Balancing



Projecting the Service: Private Link Service

The “privateLinkServices” resource abstracts the load balancer, allowing it to be consumed privately across regions and subscriptions.



Location: `West Europe`

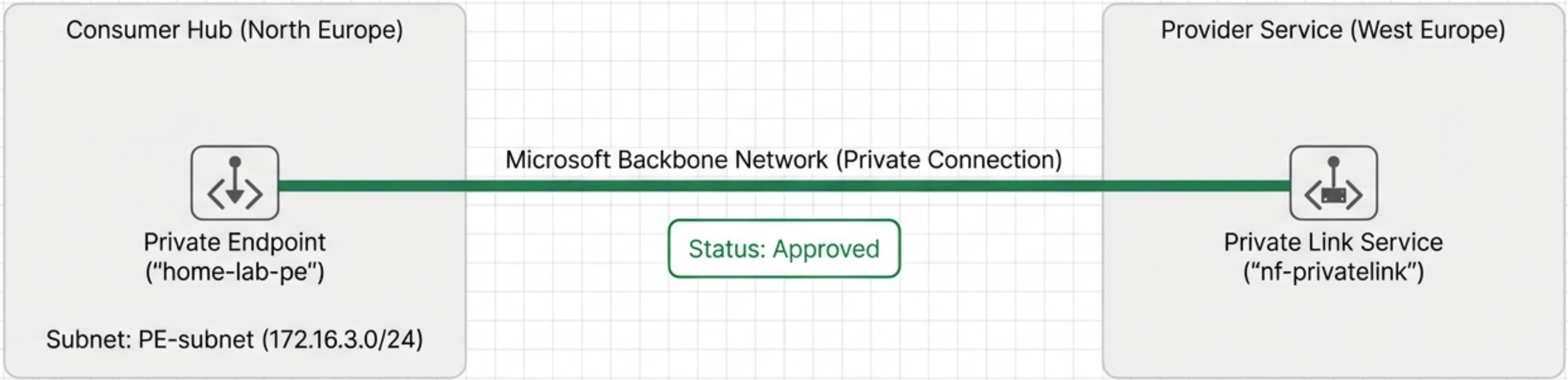
Frontend Association:
Linked directly to `'nf-lb'` frontend

IP Configuration:
Dynamically allocated from `'test-vm'` subnet

Access Control:
- Visibility: Restricted to subscription `'e11e6f4a...'`
- Auto-Approval: Enabled for subscription `'e11e6f4a...'`

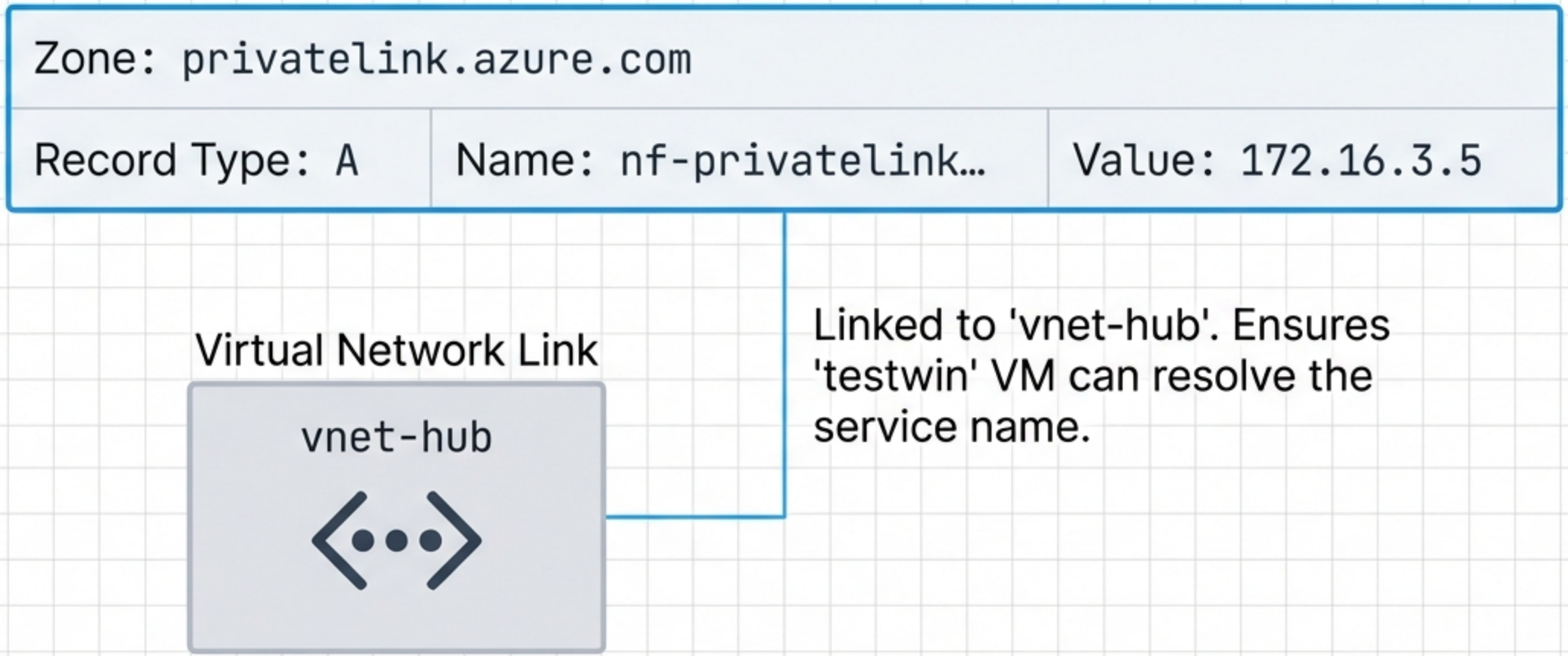
The Integration: Private Endpoint

The Hub consumes the remote West Europe service as if it were a local resource within the North Europe VNet.



Private DNS & Name Resolution

A Private DNS Zone creates an authoritative internal record, mapping the service name to the private IP address of the endpoint.



Security Posture & Access Rules

Security is managed via Network Security Groups (NSGs) applied at the subnet and interface level.

Current Configuration (Lab Mode)

NSG Names: `'nsg-open'`, `'nf-nsg-open'`

Rule: **`AllowAnyCustomAnyInbound`** (Priority 100)

Rule: **`AllowAnyCustomAnyOutbound`** (Priority 100)

Protocol: `*` (All Traffic Allowed)

Production Best Practice

Restrict Source IPs to trusted ranges.

Limit Ports to 80 (HTTP) and 443 (HTTPS) only.

Deny all other inbound traffic.

Resource Bill of Materials

Networking	Connectivity	Compute
2x Virtual Networks (‘vnet-hub’, ‘testvm-vnet’)	1x Private Link Service (‘nf-privatelink’)	2x Virtual Machines (Windows Server 2016)
1x VPN Gateway (‘VpnGw2AZ’)	1x Private Endpoint (‘home-lab-pe’)	2x Bastion Hosts (Developer & Basic SKUs)
1x Standard Load Balancer (‘nf-lb’)		

Architectural Summary

This ARM template deployment successfully demonstrates a Private Service Projection pattern.

Key Takeaways:

- **Traffic Privacy**: Data between the Consumer Hub and Provider Service remains entirely on the Microsoft Backbone Network.
- **Address Overlap Prevention**: The Provider network (`'10.88.x.x'`) is completely abstracted; the Consumer only sees a local IP (`'172.16.3.5'`).
- **Cross-Region**: Seamless connectivity between North Europe and West Europe without public peering.
- **Hybrid Ready**: The VPN Gateway ensures on-premises users can access the private service via the Hub.