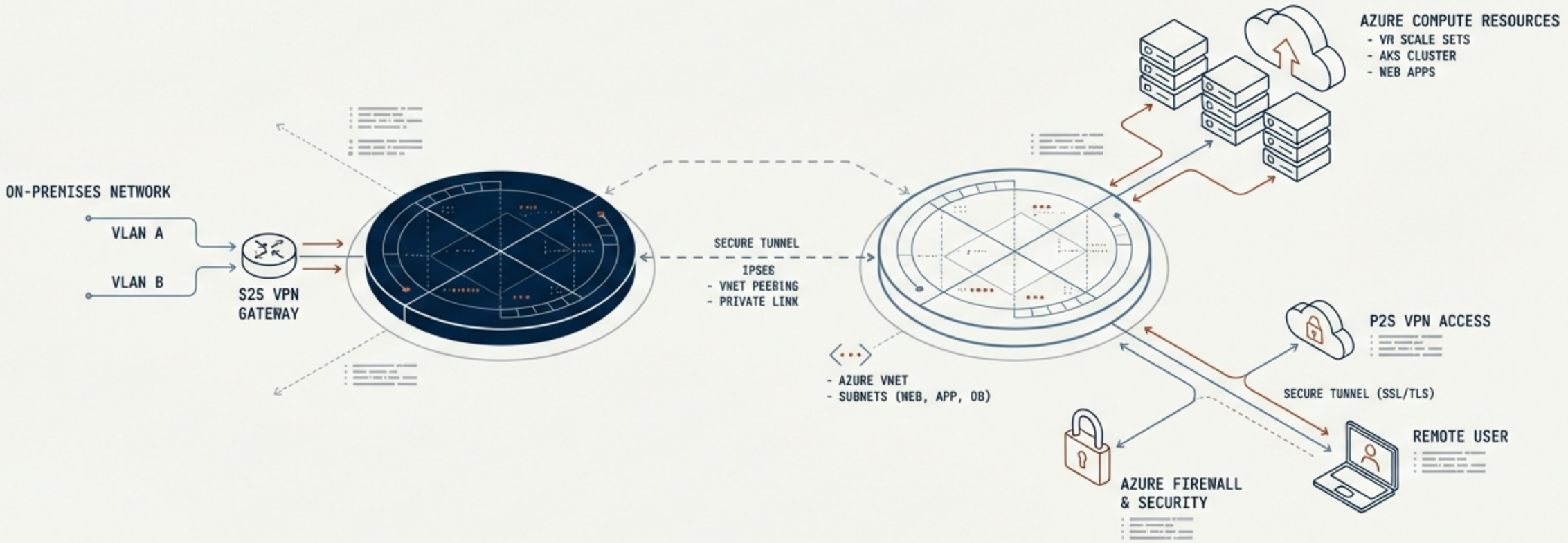
Azure Hybrid Connectivity & Compute Architecture

Deployment Configuration for Site-to-Site VPN, Point-to-Site Access, and Secure Compute



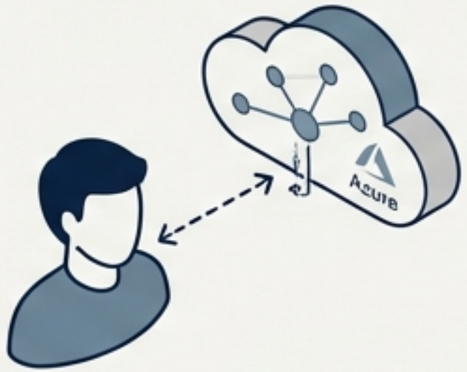
Architecture designed by **Nick Fennell** | Deployment Region: **West Europe** | Status: **Configuration Ready**

Architectural Deliverables & Capabilities

This template automates the provisioning of a secure, hybrid extension of the on-premises network into the Azure West Europe region.

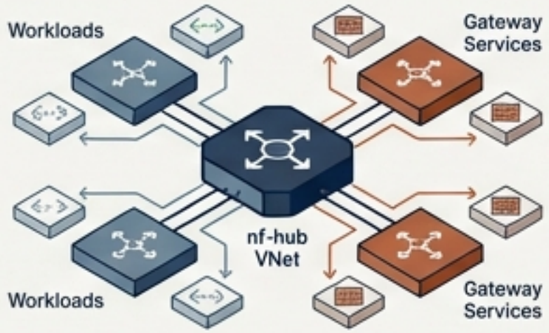
Hybrid Connectivity

Establishes a BGP-enabled IPsec tunnel between on-premises infrastructure and Azure.



Remote User Access

Provisions an OpenVPN-based Point-to-Site (P2S) gateway for individual client connectivity.



Hub Network Topology

Deploys the nf-hub Virtual Network with dedicated segmentation for workloads and gateway services.

Secure Compute

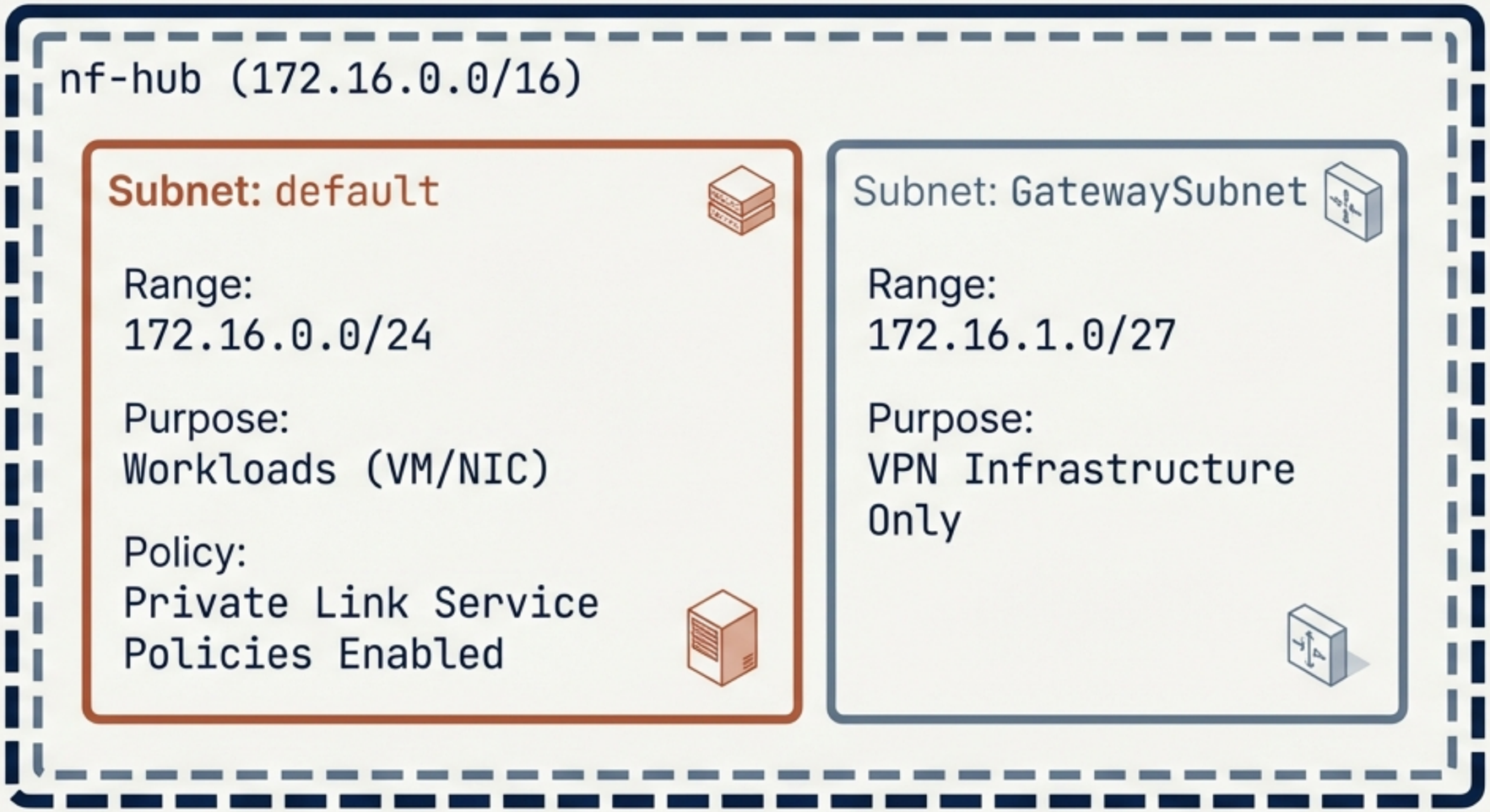
Instantiates a Trusted Launch Ubuntu 24.04 LTS Virtual Machine protected by Network Security Groups.

The Infrastructure Foundation: Virtual Network Topology

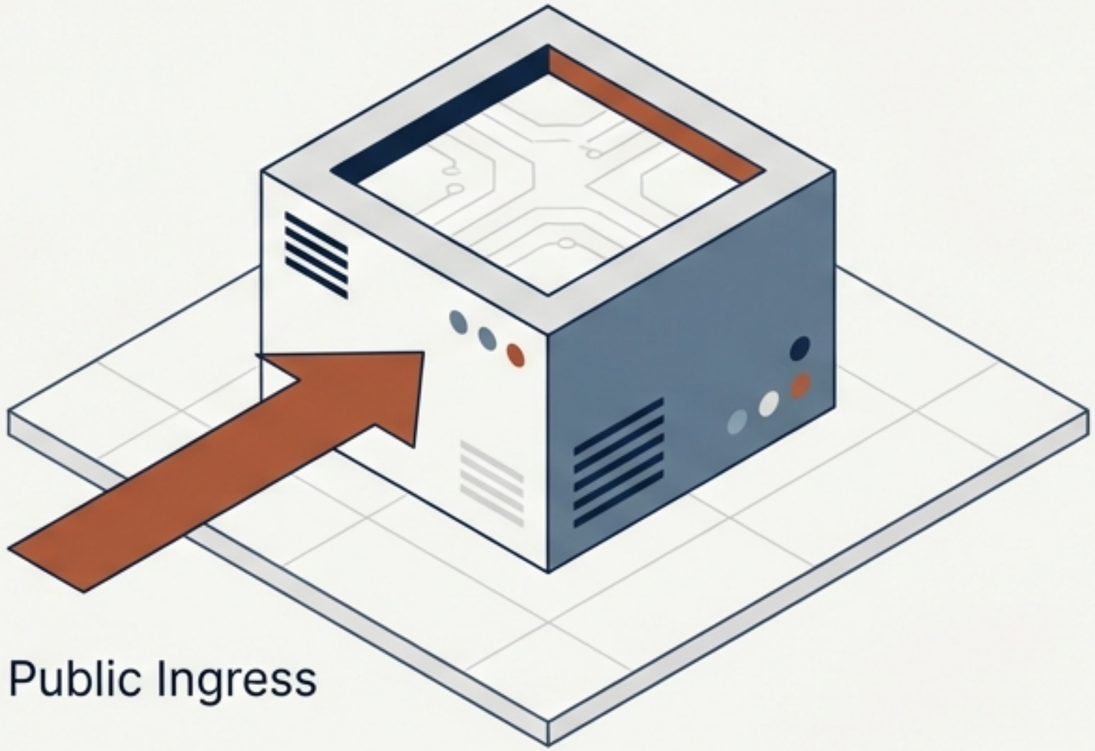
Resource Name:
nf-hub

Region:
West Europe

Total Address Space:
172.16.0.0/16



Azure Ingress: Virtual Network Gateway Configuration



Public Ingress

Resource Name	`ng-vpngw`
SKU	`VpnGw1 (Standard Tier)`
Routing Type	`RouteBased (Dynamic)`
Gateway Type	`VPN`

Public Identity Configuration

Resource: `nf-gwip`
IP Address: `52.166.77.218 (Static)`
DDoS Protection: **Inherited from Virtual Network**

Defining the On-Premises Boundary

The Local Network Gateway (nf-lng) acts as the logical anchor for the physical datacenter.

Data Card

Data Card

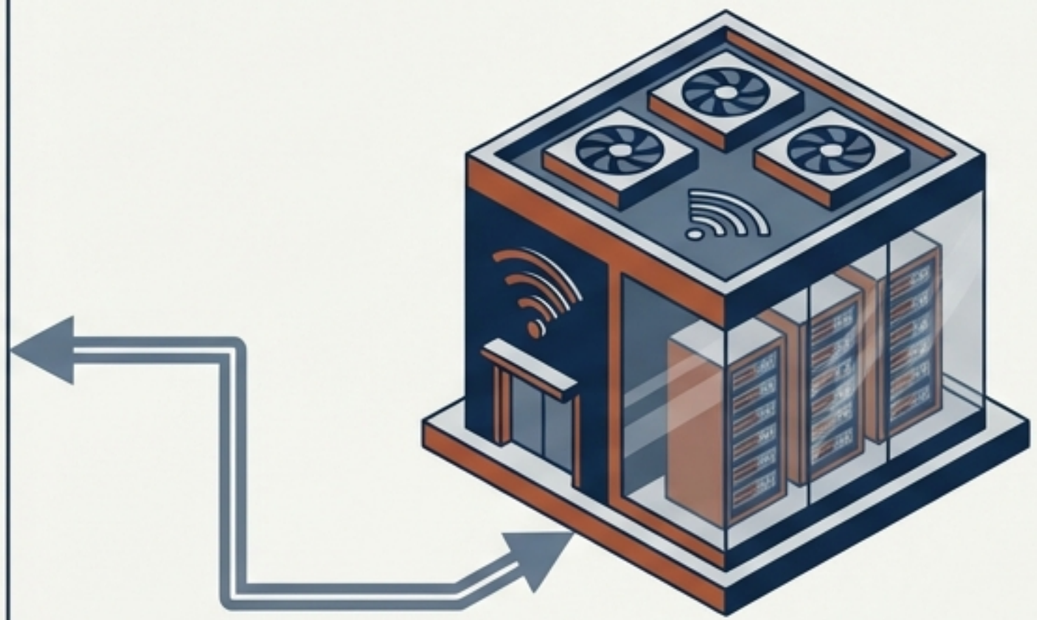
Resource Name: nf-lng
Gateway Public IP: 37.228.231.33

Routed Address Spaces (Traffic Destinations)

- 10.0.0.0/8 (Corporate Network)
- 192.168.0.0/24 (Branch/Legacy Network)

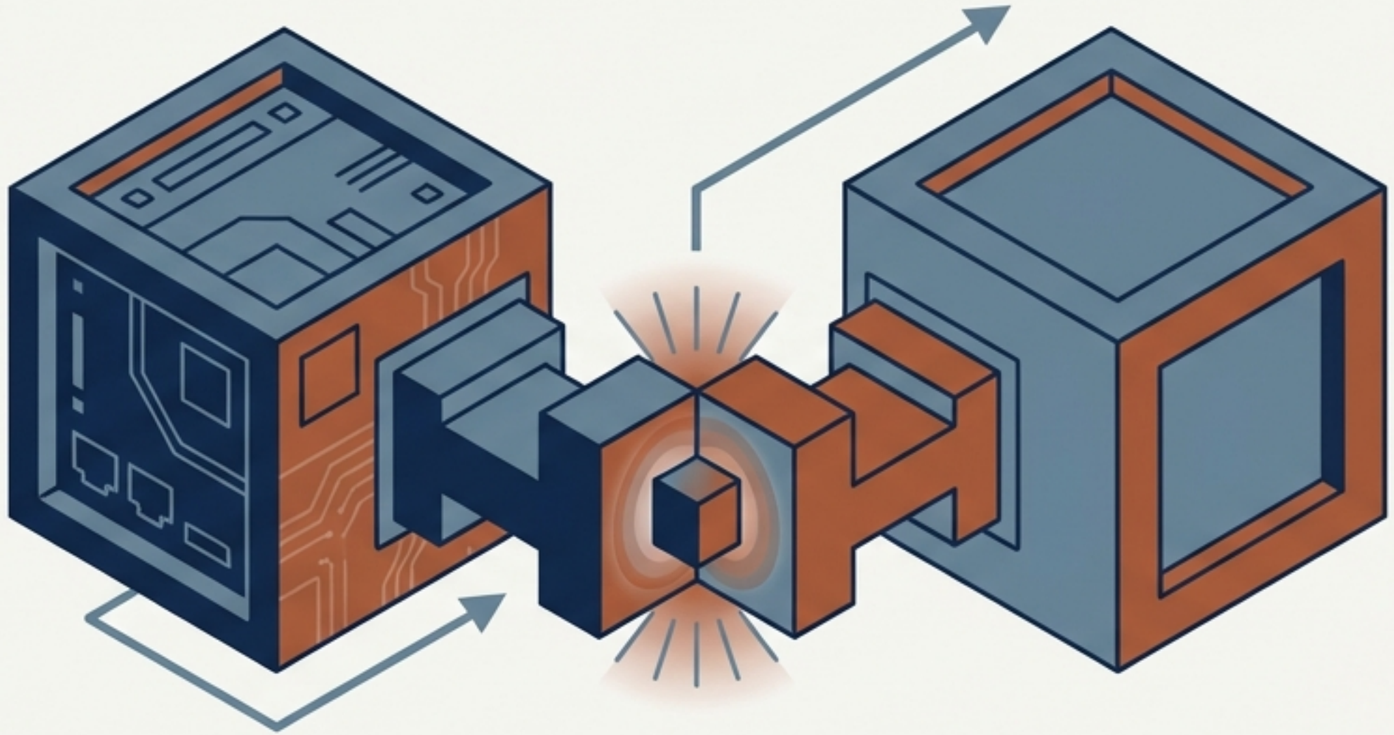
BGP Identity

ASN: 65010
Peering Address: 10.0.0.1



The Bridge: Site-to-Site Connection Logic

Azure Gateway
(ng-vpngw)



Local Gateway
(nf-lng)

Connection Specifics

Resource: `S2S`
Type: `IPsec / IKEv2`
Mode: `Default`

Operational Settings

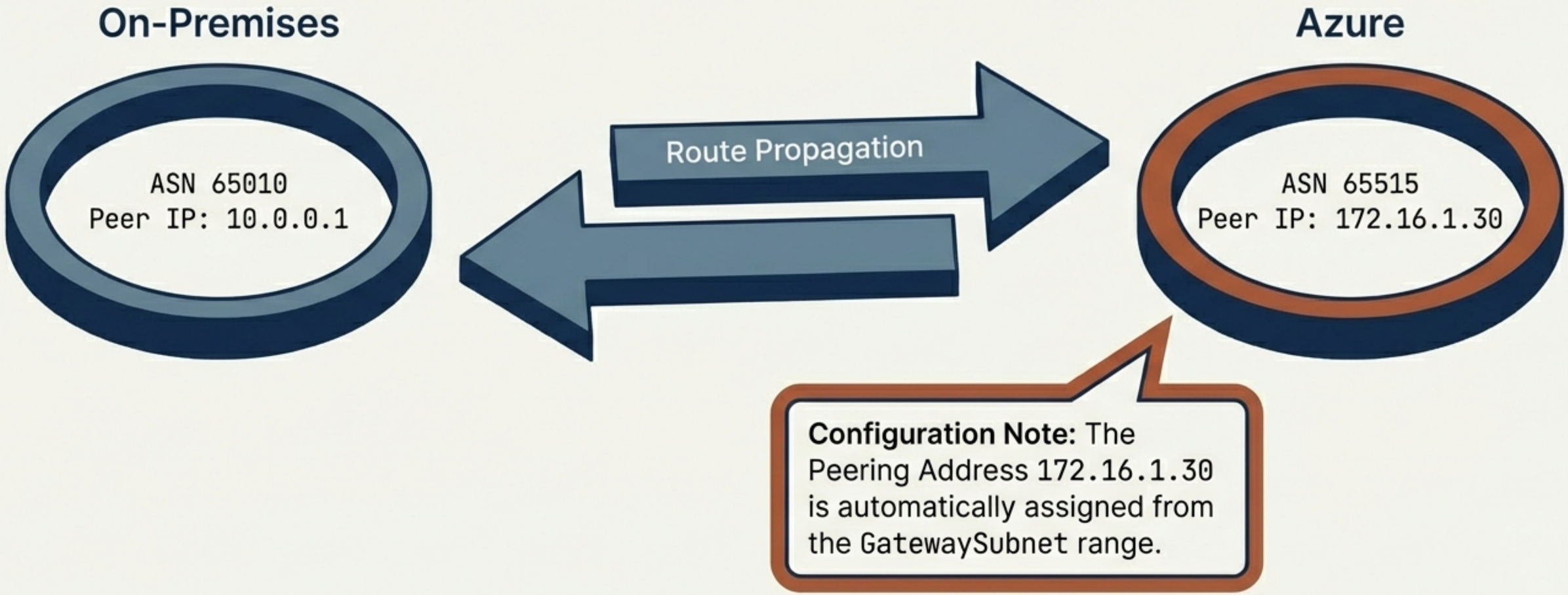
DPD Timeout: `45 seconds`
BGP: `Enabled`

Traffic Logic

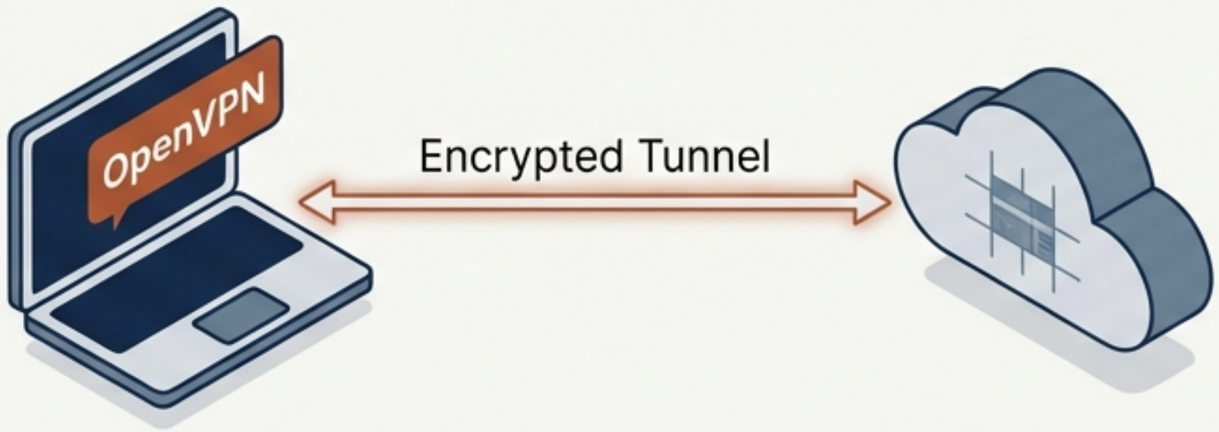
Traffic Selectors: `Disabled`
Routing: `Dynamic via BGP`

Dynamic Routing Strategy (BGP)

Automatic route exchange eliminates manual table updates.



Remote User Access: Point-to-Site (P2S)



Protocol Stack

Tunnel Type:	`OpenVPN`
Authentication:	`Certificate-based`

Network Configuration

Client Address Pool: `10.1.1.0/24`

(Clients receive IPs from this range)

Certificate Authority Chain

Root Name: `ROOT`

Issuer CN: `lab01-DC01-CA`

Chain: `local -> lab01 -> lab01-DC01-CA`

Compute Workload Specification

Spec Sheet

Virtual Machine Identity

Resource:	nf-vm1
OS:	Ubuntu 24.04 LTS (Noble Numbat)
Publisher:	Canonical
SKU:	server

Hardware Profile

Size:	Standard_DS1_v2
Hibernation:	Disabled

Storage Configuration

Disk Type:	Managed OS Disk
Caching:	ReadWrite
Naming Pattern:	nf-vm1_OsDisk_1_[guid]

Access Control

Admin User:	azureuser
Auth Method:	Password Enabled

Compute Security Profile: **Trusted Launch**

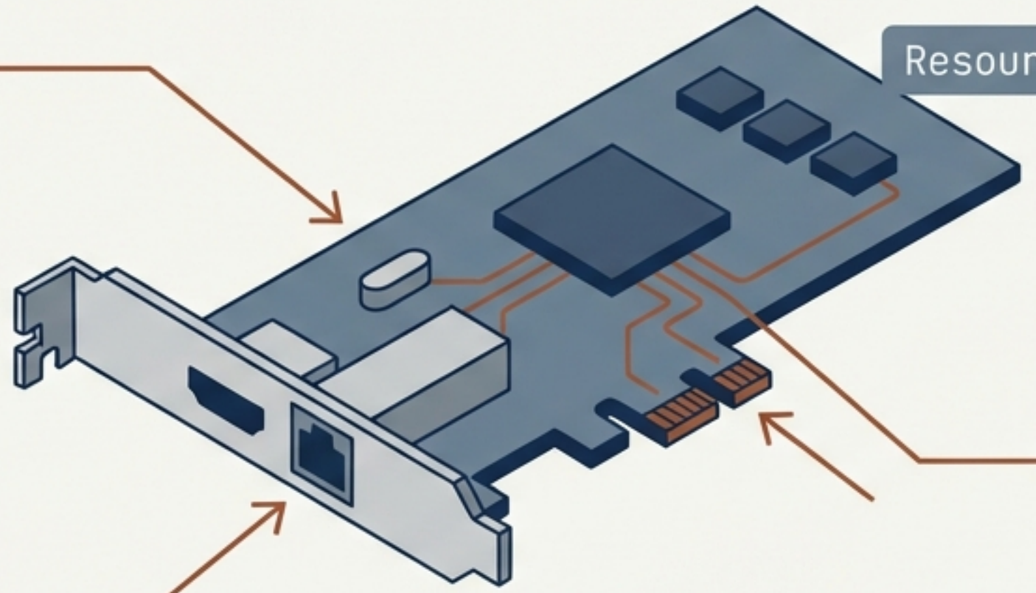
Gen2 protection against bootkits and firmware-level attacks

Diagnostics: Boot Diagnostics Enabled
(Serial Console & Screenshot Capture)

Network Interface Configuration

IP Configuration

Private IP: `172.16.0.4`
Allocation: `Dynamic`
Subnet: `default`



Performance

Accelerated Networking: `ENABLED`
IP Forwarding: `Disabled`

Associations

Attached VM: `nf-vm1`
Network Security Group: `nf-vm1-nsg`

Perimeter Security: Network Security Group

Resource: nf-vm1-nsg | Scope: nf-vm1555 Interface

Priority	Name	Port	Protocol	Source	Action
300	SSH	22	TCP	Any (*)	Allow

Security Insight

Warning: The current configuration allows SSH from Any Source (*). For production hardening, restrict Source Address Prefix to VPN Client Pool (10.1.1.0/24) or On-Premises Range.

Deployment Parameters & Inputs

Parameter Key	Default Value
`virtualNetworks_nf_hub_name`	**nf-hub**
`virtualMachines_nf_vm1_name`	**nf-vm1**
`connections_S2S_name`	**S2S**
`localNetworkGateways_nf_lng_name`	**nf-lng**
`publicIPAddresses_nf_gwip_name`	**nf-gwip**
`networkSecurityGroups_nf_vm1_nsg_name`	**nf-vm1-nsg**

The template relies on these defaults for rapid testing but supports full naming customization at runtime.

Governance & Operational Metadata

July 22, 2025

Deployment Initiated

Resources:

- Public IP
- VNet
- Local Network Gateway

July 23, 2025

Compute Provisioning

Resources:

- VM
- NIC
- NSG
- VPN Gateway

July 24, 2025

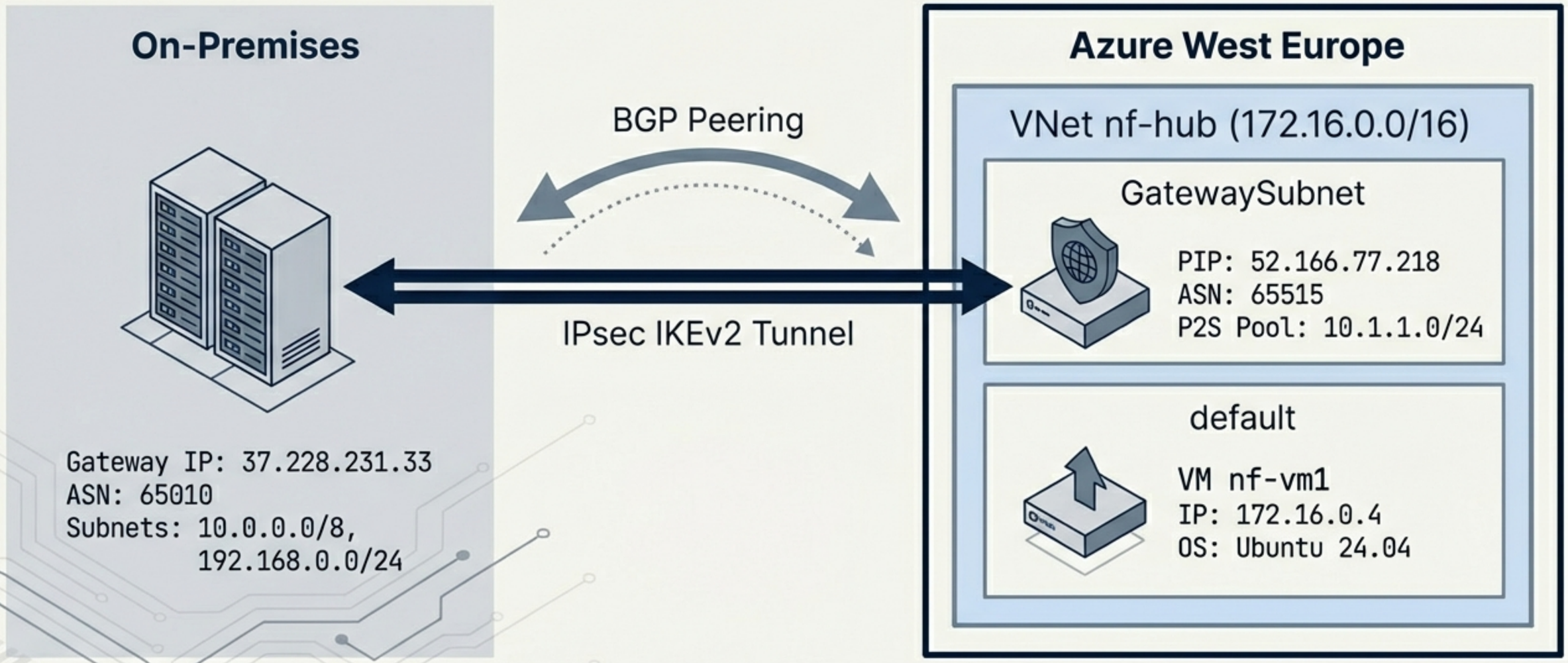
Connectivity Finalized

Resources:

- S2S Connection

Creator Tag: Nick Fennell
API Versions: Network (2024-07-01), Compute (2024-11-01)

Full Architecture Topology



Architecture Status: VALIDATED