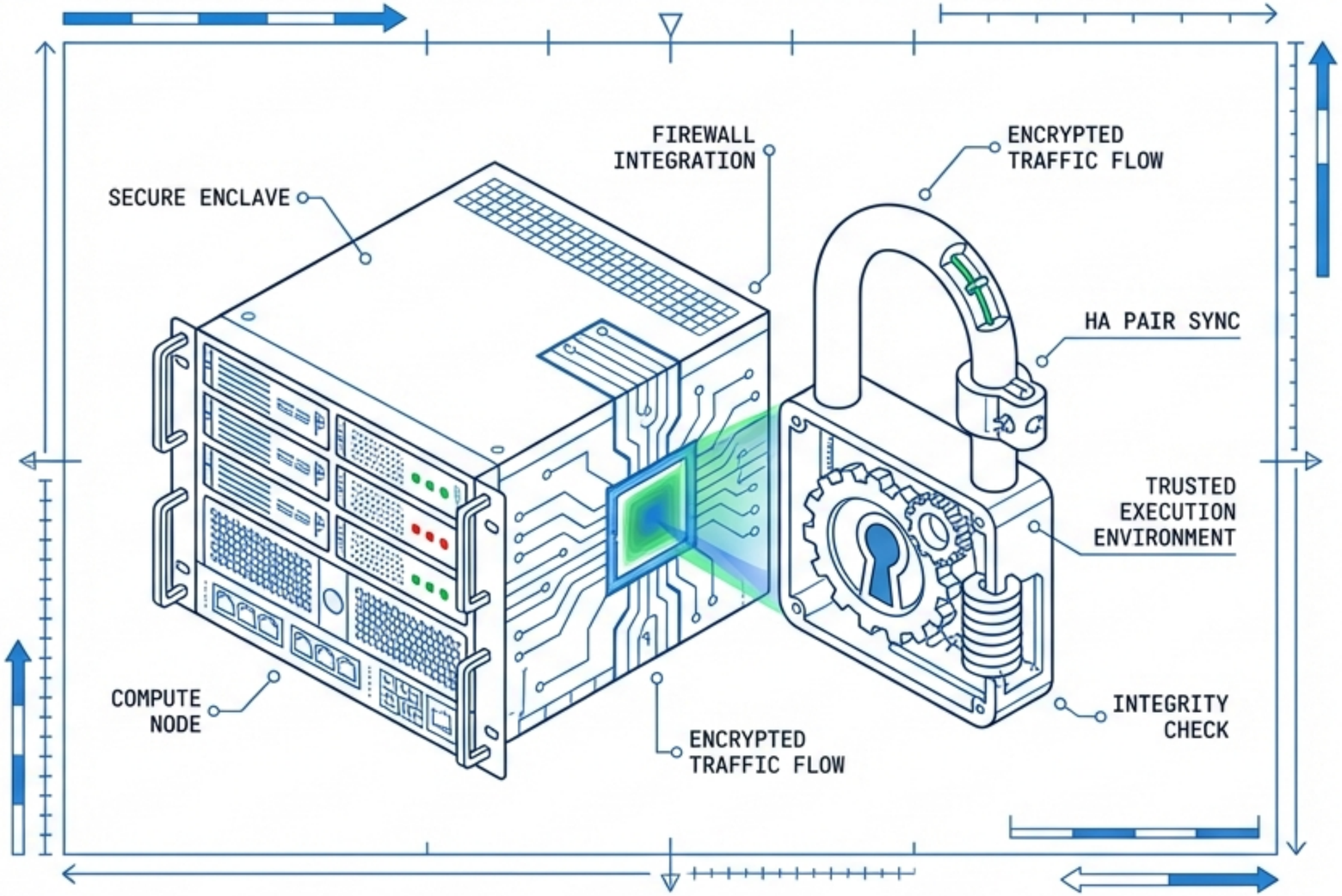
# Azure High-Availability Firewall Architecture

Technical Analysis of the Palo Alto VM-Series ARM Deployment




DEPLOYMENT TYPE:
ARM Template / JSON

```
{
  "type": "Microsoft.Network/virtualNetworks",
  "name": "vnet-hub", ...
}
```

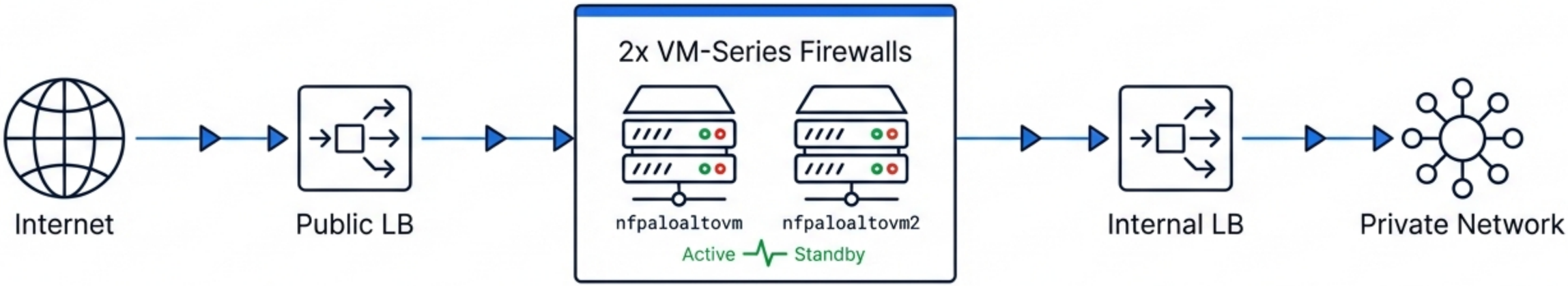
WORKLOAD:
Palo Alto Networks VM-Series Flex (BYOL)

Supports Active/Passive & Active/Active configurations. License required.

TOPOLOGY:
Hub-and-Spoke Ingress/Egress

# DEPLOYMENT SCOPE & CAPABILITIES

The ARM templates define a resilient security perimeter utilizing a clustered Virtual Machine approach.




## HIGH AVAILABILITY

Two distinct VM nodes (nfpaloaltovm, nfpaloaltovm2) wrapped in an Availability Set.

## TRAFFIC MANAGEMENT

Dual Load Balancers managing both public ingress and private internal routing.

## LICENSING MODEL

VM-Series Flex (BYOL) on Linux.

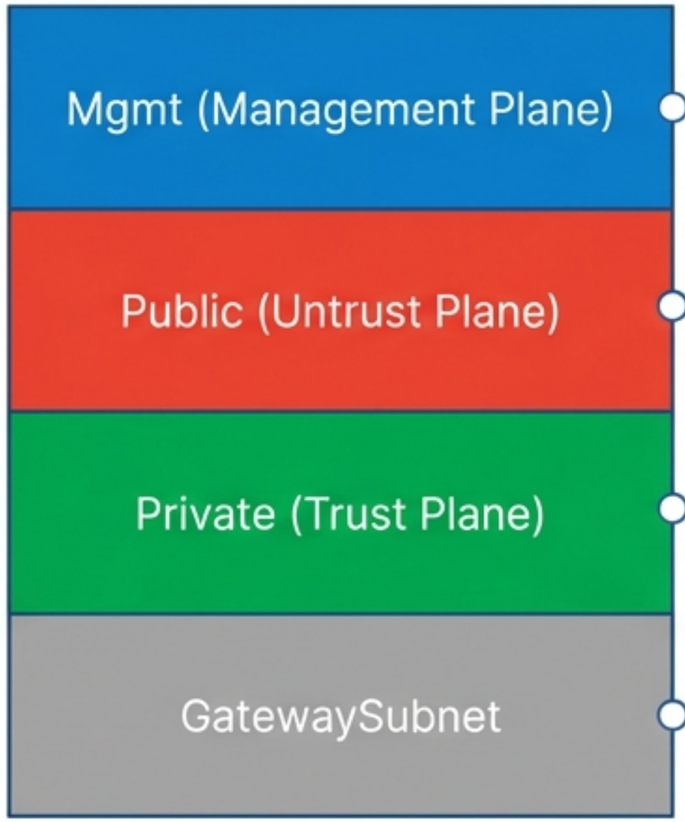
## SOFTWARE VERSION

PAN-OS 11.2.5

# THE NETWORK FOUNDATION: VNET & SEGMENTATION

VNET Name: fwVNET

Address Space:
172.18.0.0/16




**172.18.0.0/24** – Dedicated for out-of-band administrative access.

**172.18.1.0/24** – Inbound traffic from the internet.

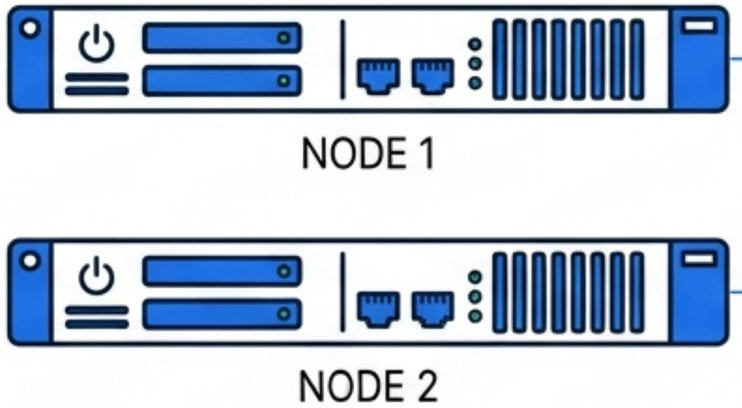
**172.18.2.0/24** – Internal traffic inspection.

**172.18.3.0/27** – Reserved for VPN/ExpressRoute connectivity.

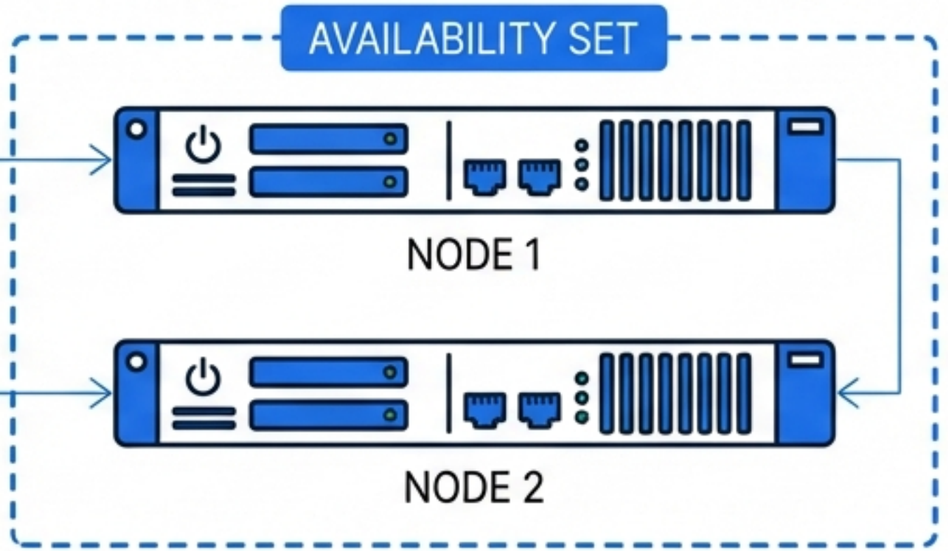
**Context**: The strict separation of subnets enables the isolation of data planes, a critical security best practice found in the `virtualNetworks` resource definitions.

# COMPUTE RESOURCES & REDUNDANCY

## THE NODES




## RESILIENCE STRATEGY



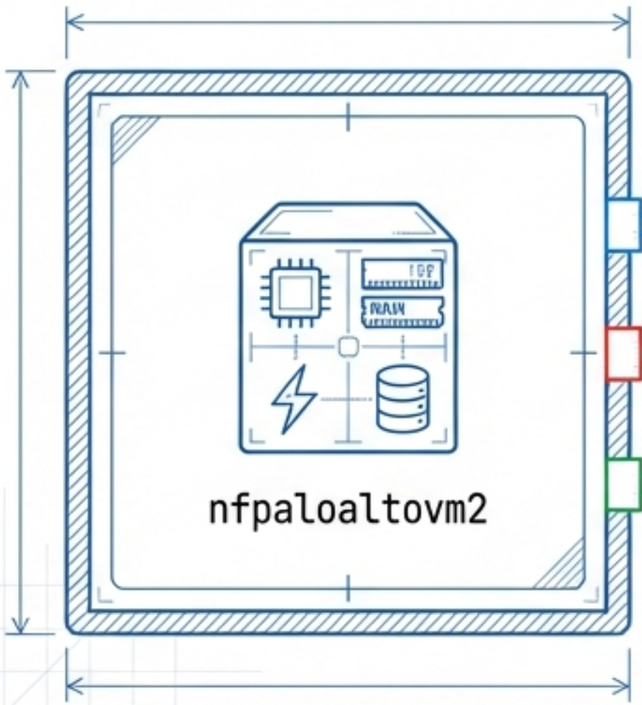

### SPECIFICATIONS

- Name: **nfpaloaltovm** & **nfpaloaltovm2**
- VM SKU: **Standard_D8_v4** (High Compute) / **Standard_B4ls_v2**
- OS: Linux (Palo Alto Networks Publisher)

### RESILIENCE PARAMETERS

- Resource: **newavailabilityset...**
- Fault Domains: 2 (Physical Power/Cooling Isolation)
- Update Domains: 5 (Sequential Patching Logic)
- Target SLA: **99.95%**

# THE THREE-INTERFACE TOPOLOGY




**Interface:** eth0 (Management)
**IP:** 172.18.0.5
**Function:** Control Plane Access
**Resource:** nfpaloaltovm2-nfpaloaltovm2-eth0

**Interface:** eth1 (Public/Untrust)
**IP:** 172.18.1.5
**Function:** Data Plane Ingress / Public LB Backend
**Resource:** nfpaloaltovm2-nfpaloaltovm2-eth1

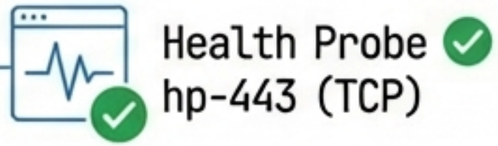
**Interface:** eth2 (Private/Trust)
**IP:** 172.18.2.5
**Function:** Internal Routing / Internal LB Backend
**Resource:** nfpaloaltovm2-nfpaloaltovm2-eth2

# INGRESS STRATEGY: PUBLIC LOAD BALANCER

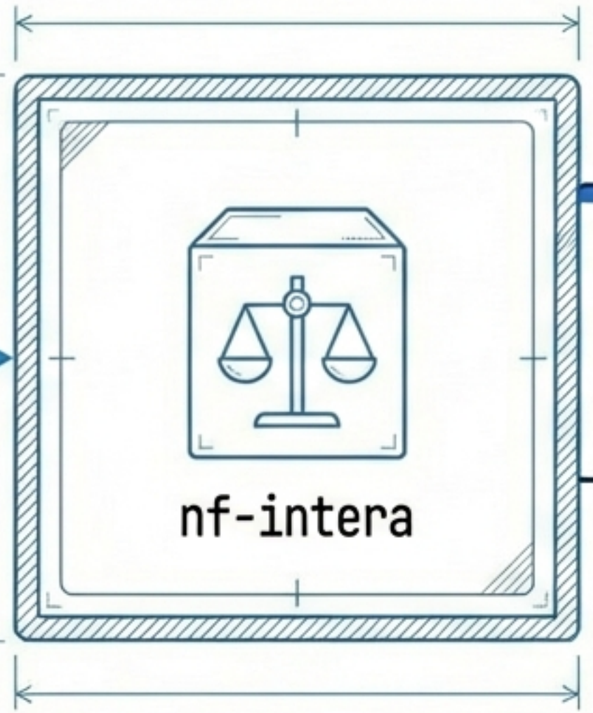
Resource: nf-elb | Frontend IP: 51.124.173.156 | Tier: Standard Regional

LOAD BALANCING RULES

| PROTOCOL | PORT | USAGE | FLOATING IP |
|---|---|---|---|
| TCP | 80 | HTTP Ingress | Enabled |
| TCP | 443 | HTTPS Ingress | Disabled |
| TCP | 22 | SSH Management | Disabled |
| UDP | 500 | VPN IKE | Disabled |
| UDP | 4500 | VPN NAT-T | Disabled |



# INTERNAL TRAFFIC ROUTING & DISTRIBUTION




Private Frontend IP:
172.18.2.6

Subnet: Private
(172.18.2.0/24)

Internal Workloads

Internal LB (nf-intera)

Backend Pool: nf-internal-be

VM1
eth2

VM2
eth2

Health Probe: hp-443 checks internal interface health.
Configuration: HA Ports (All Ports) / TCP 443 specifically defined.

# AZURE-LEVEL SECURITY GROUPS (NSGs)

## DATA PLANE STRATEGY (eth1, eth2)

Passthrough Configuration

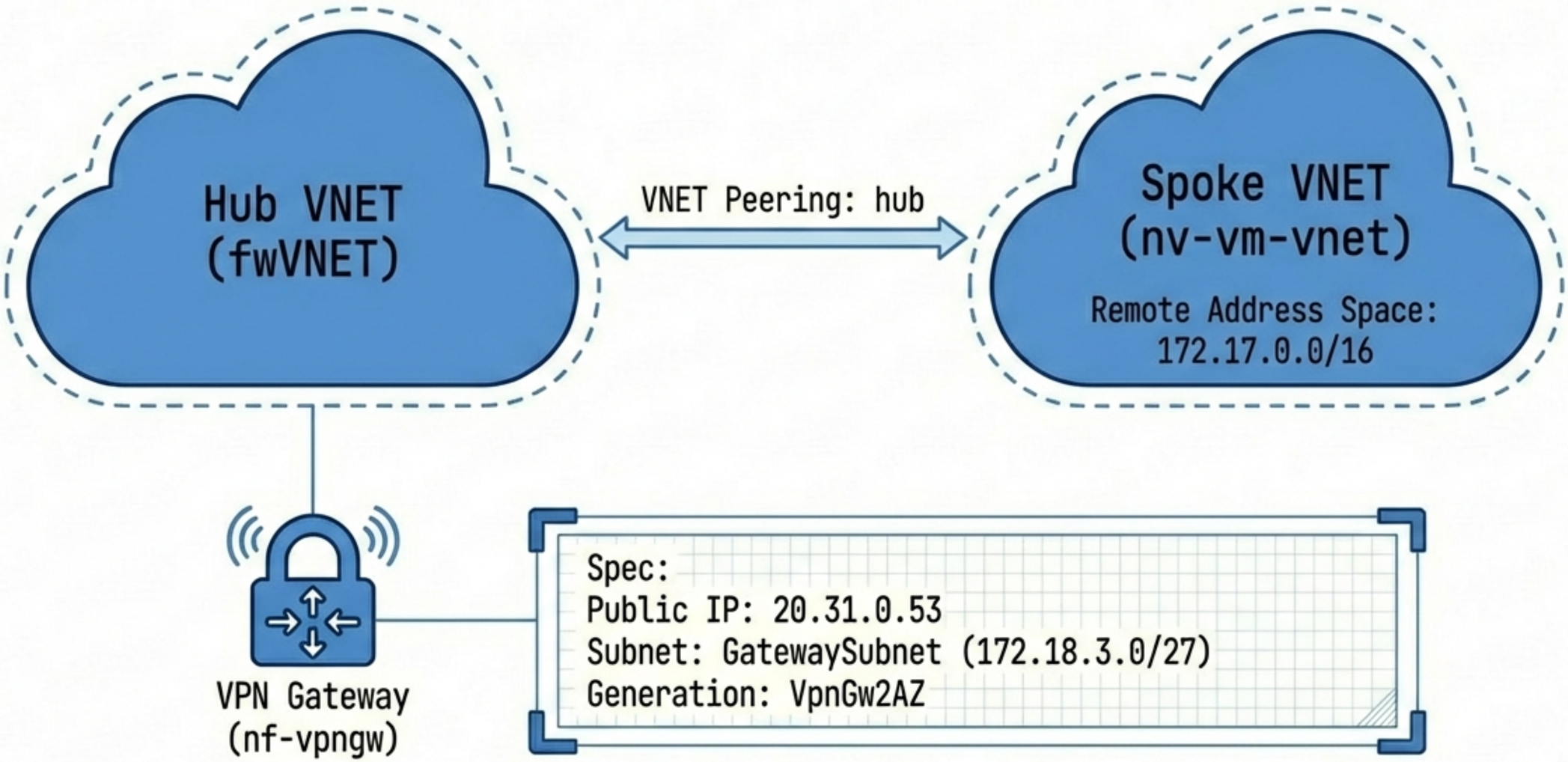
Spec:
NSG Name: Allow-All
Policy: Inbound/Outbound Protocol *
Rationale: Avoids double-filtering; delegates inspection logic to the Firewall.

## MANAGEMENT PLANE STRATEGY (eth0)

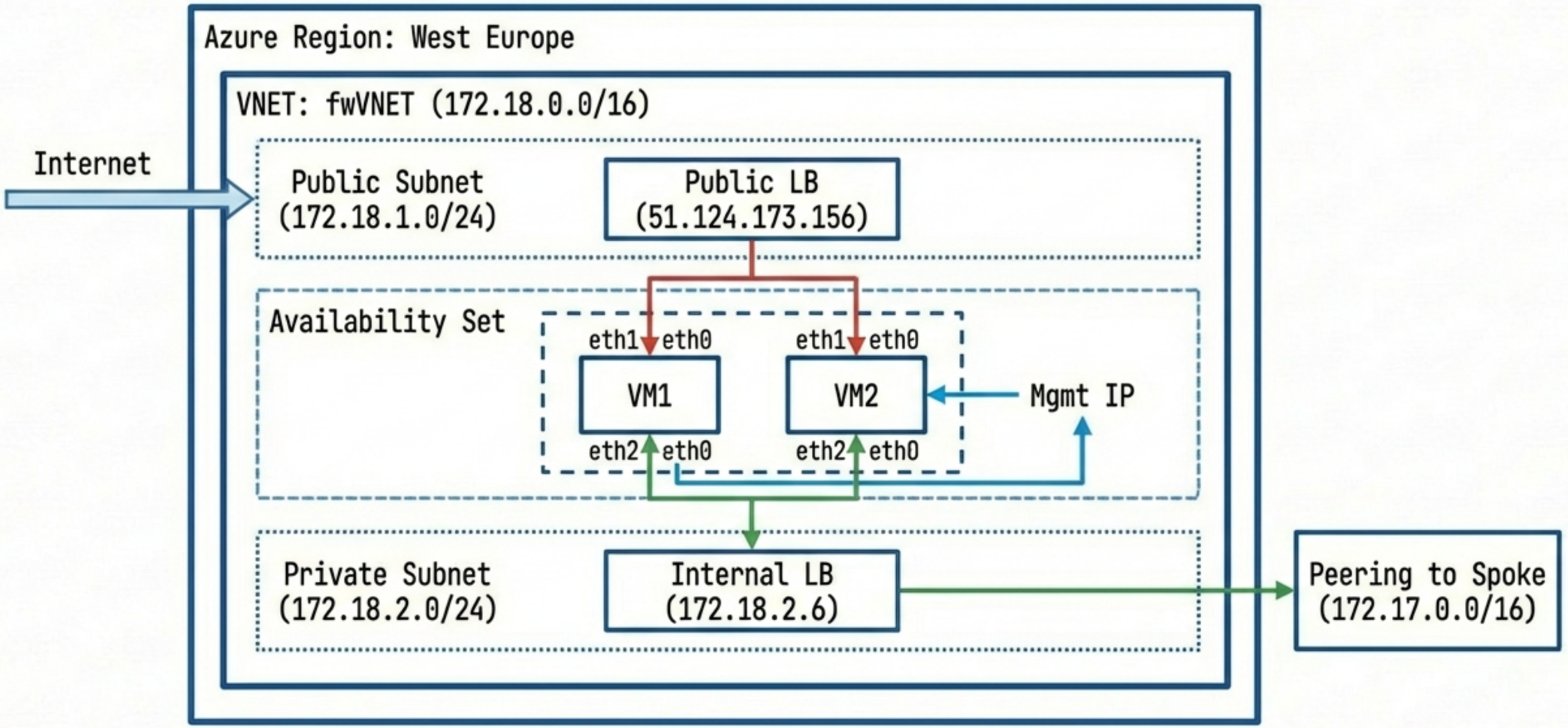
Hardened Shell

Spec:
NSG Name: DefaultNSG
Rule 100: Allow-Outside-From-IP (0.0.0.0/0)
Rule 101: Allow-Intra (172.18.0.0/16)
Rule 200: Default-Deny (Implicit)

# CONNECTIVITY & TOPOLOGY INTEGRATION



# THE COMPLETE ARCHITECTURAL BLUEPRINT



# DEPLOYMENT PARAMETERS & NAMING CONVENTIONS

Key identifiers and configuration variables extracted from the ARM template parameters.

| PARAMETER | CONFIGURED VALUE |
| --- | --- |
| Resource Group | nf-rg2 |
| VM Names | nfpaloaltovm, nfpaloaltovm2 |
| Public IP (Firewall Node 1) | 51.105.220.116 |
| Public IP (Firewall Node 2) | 104.45.72.74 |
| Disk Size | 60GB (Premium LRS) |
| Admin User | azureuser1 |
| Deployment Tag | panNGFWfn5lbng2qbuhc |