

# Azure Virtual networks (Vnet)

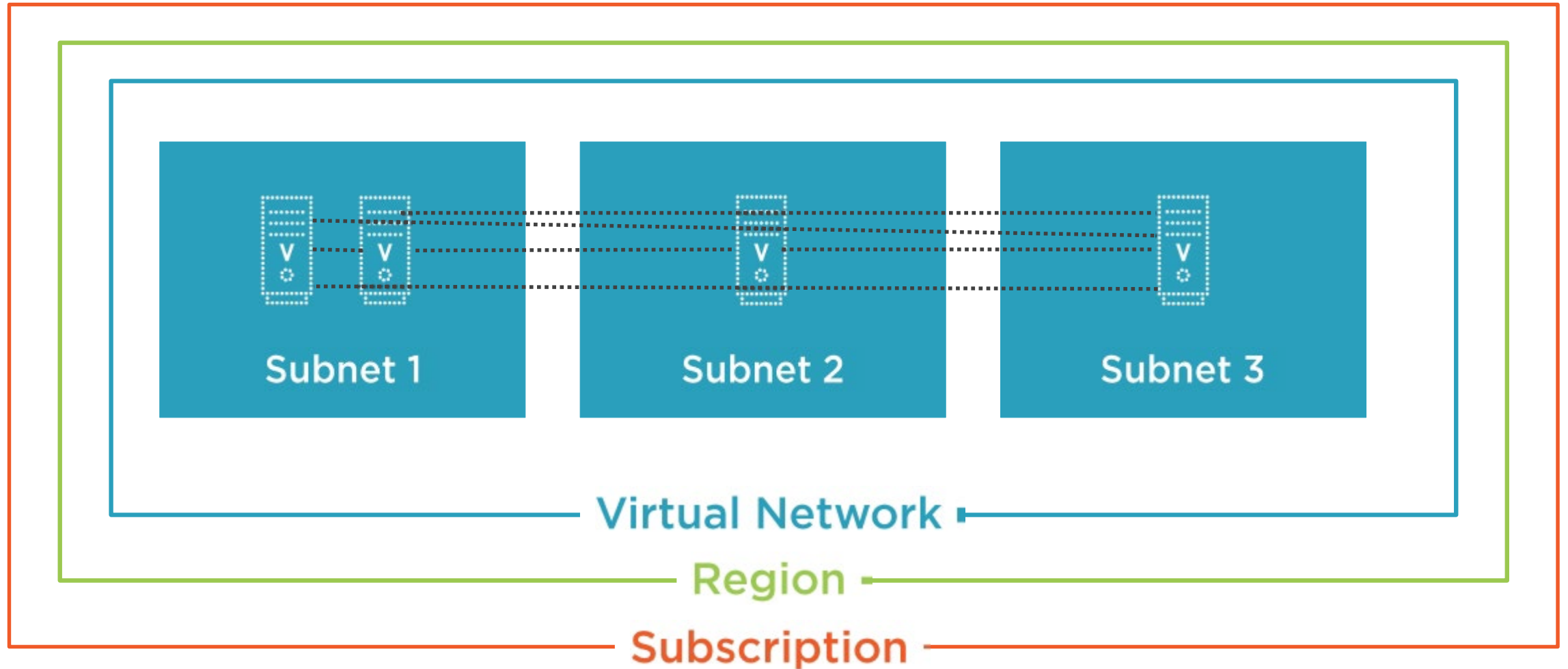
## What is a VNet?

- An Azure Virtual Network (VNet) is a representation of your own network—in the cloud.
- It is a logically isolated segment of the Azure cloud that is dedicated to your subscription.

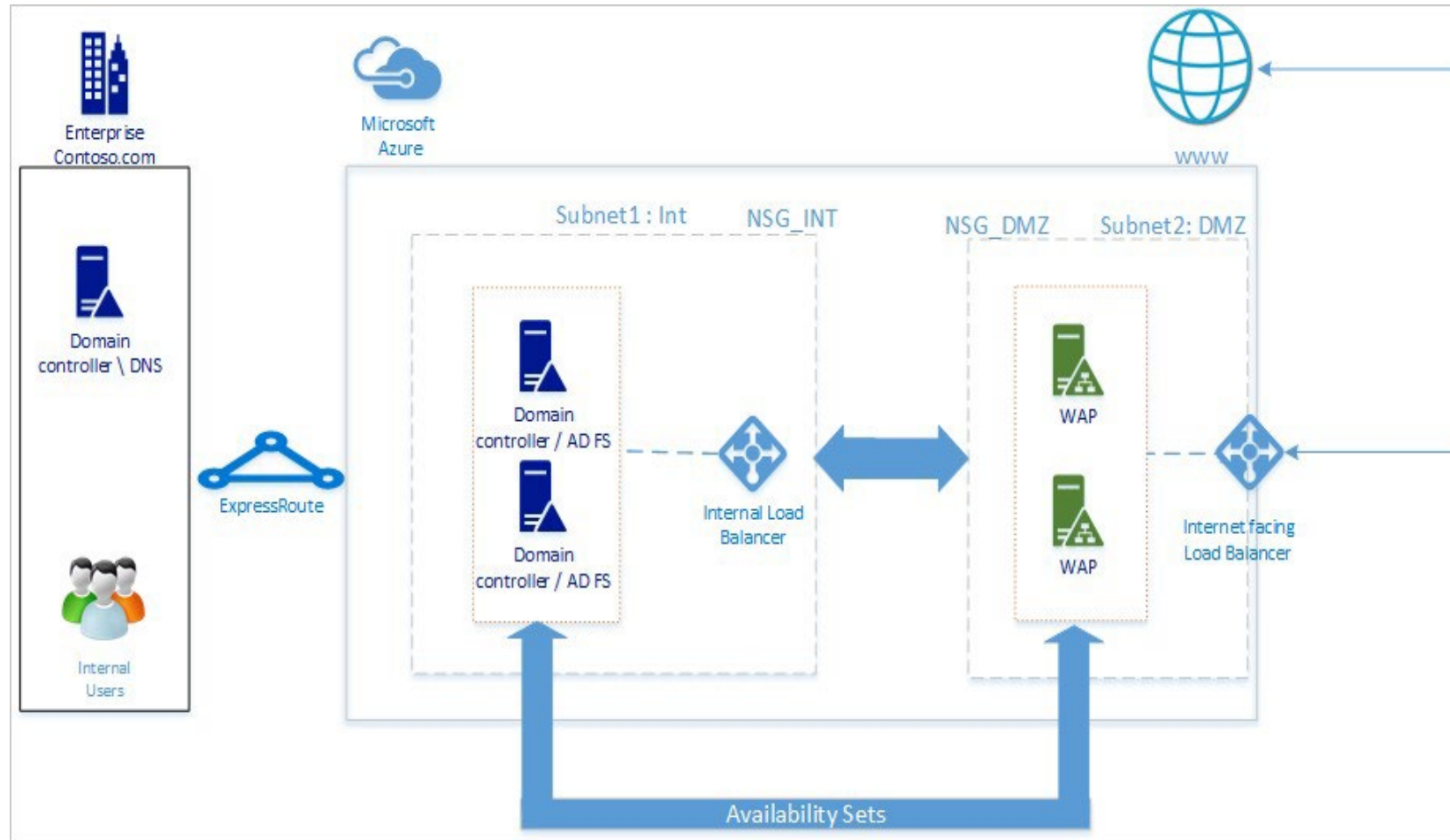
## Key Benefits

- Enables secure communication between Azure resources (e.g., VMs, databases, containers).
- Functions as a private network, not exposed to the public internet unless you explicitly configure access.
- Supports features like subnets, network security groups (NSGs), routing, and peering for advanced configurations.

# Vnet diagrams



# Vnet diagrams



# Vnet Capabilities

## Isolation

- Each Virtual Network (VNet) is logically isolated from other VNets—even within the same region or subscription.
- No cross-VNet communication occurs unless you explicitly configure it (e.g., VNet Peering or VPN Gateway).

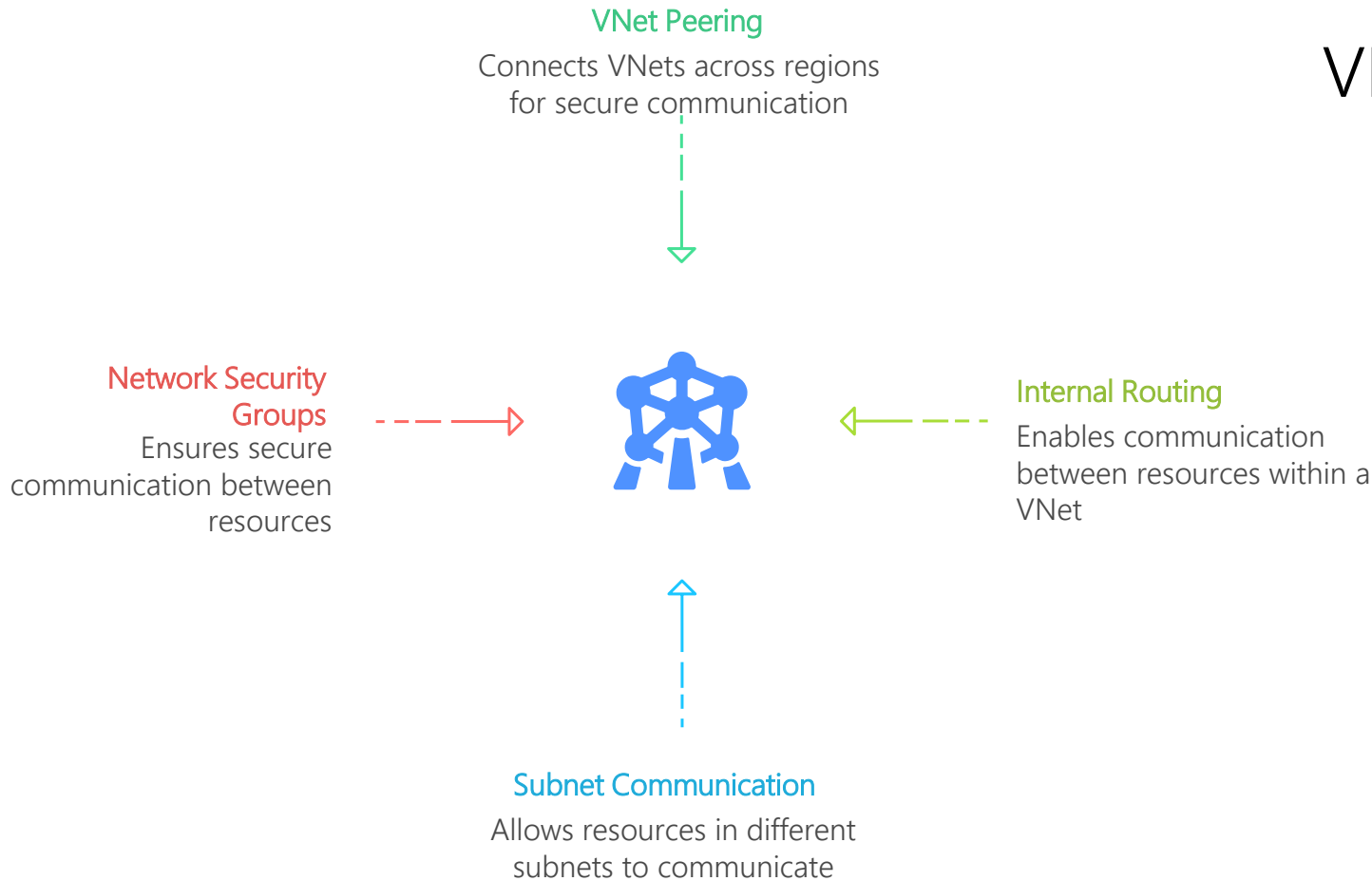
## Customizability

- Define your own IP address ranges (CIDRs), subnets, and networking rules.
- Create separate VNets for Dev, Test, and Prod—even reusing the same CIDR blocks if isolated by region or subscription.
- Connect VNets with different CIDRs to enable secure, controlled communication between environments.

## Name Resolution

- Azure VNets support internal DNS resolution using Azure-provided DNS servers.
- **Optionally, you can configure:** Custom DNS Servers, DNS Forwarding, Private DNS Zones for enhanced flexibility.

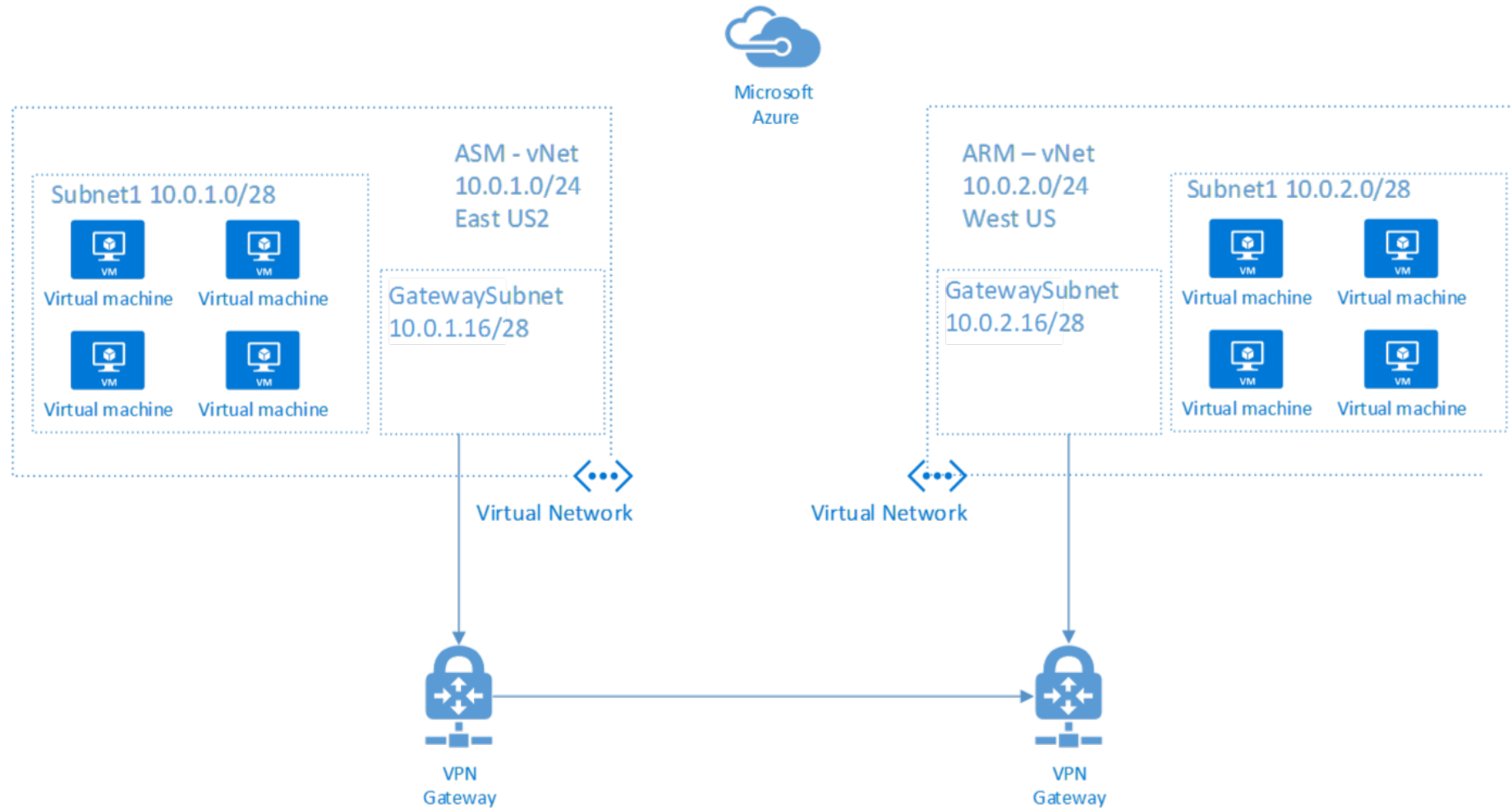
# Vnet Capabilities



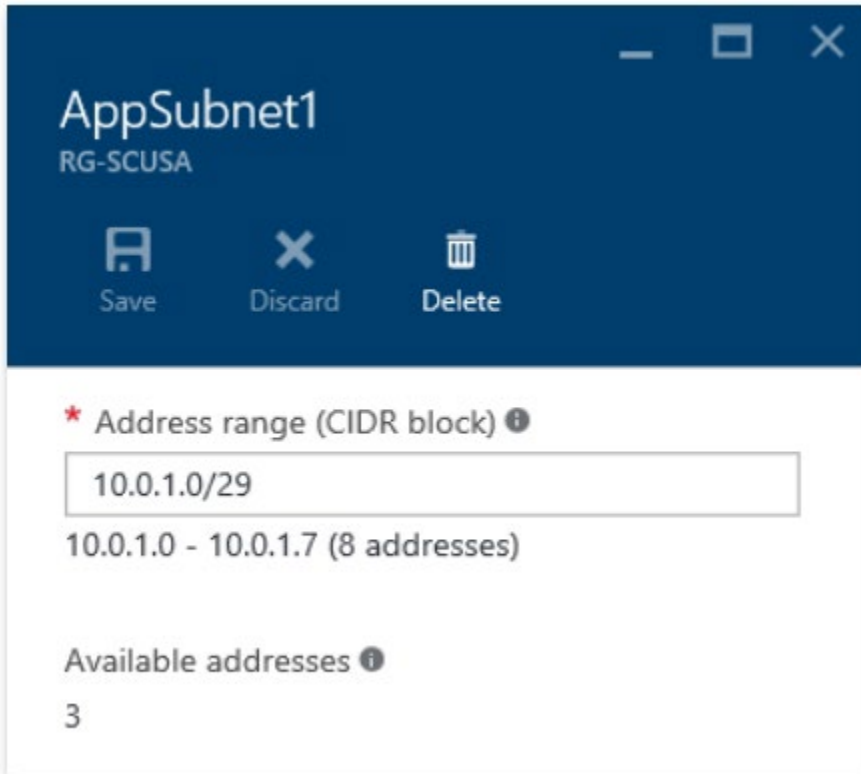
## VNet connectivity

- VNets can be connected to each other.
- Any resource can communicate with any other resource even on different Subnets.
- App server can connect to database server on different Subnet

# Vnet diagrams



# Vnet Reserved IPs



AppSubnet1  
RG-SCUSA

Save Discard Delete

\* Address range (CIDR block) ⓘ

10.0.1.0/29

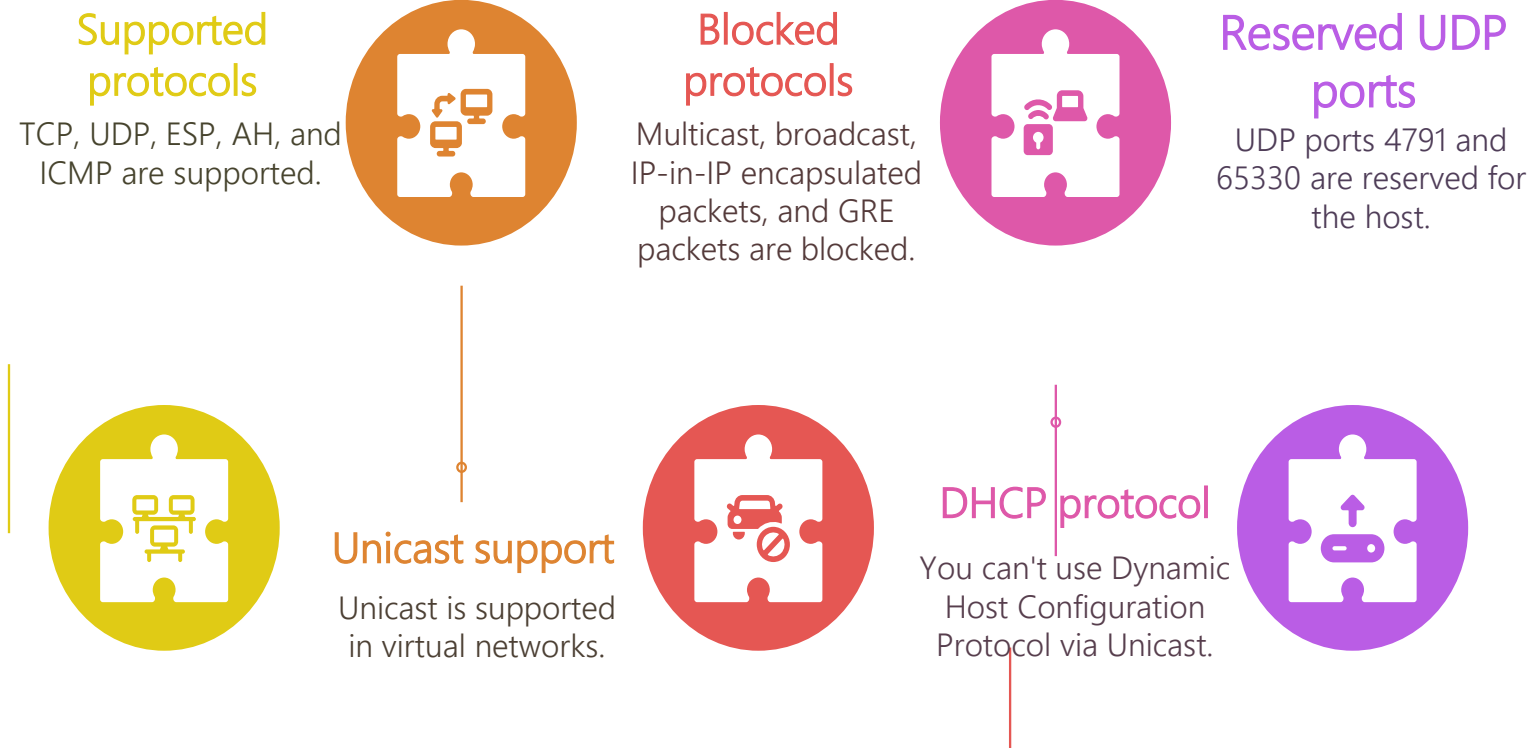
10.0.1.0 - 10.0.1.7 (8 addresses)

Available addresses ⓘ

3

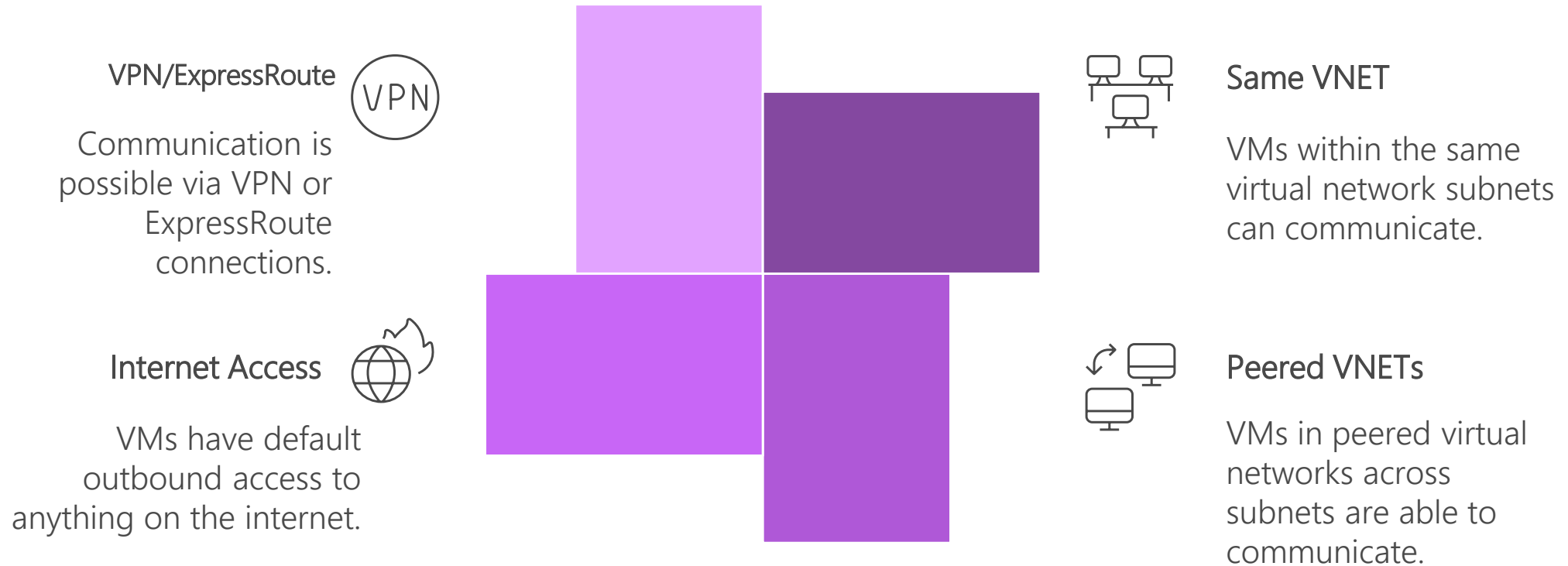
- Certain IPs reserved for Azure's internal use
- First and last reserved per protocol for host ID and broadcast
- The first 3 IP addresses are reserved

# Vnet protocol support and limitations





# Traffic flow in a VNet



# Traffic flow in a VNet



## **Not all resources should talk to each other**

By default, all subnets within a VNet can communicate — but this may violate security or compliance policies.

## **Enforce subnet-level boundaries**

Multi-tier applications (e.g., web ↔ app ↔ database) often require **only neighbor tiers to communicate**, not full mesh access.

## **Limit public internet access**

Outbound internet traffic should be **restricted or routed through a controlled egress point** like a NAT Gateway or Azure Firewall.

## **Control specific traffic types and ports**

Use **Network Security Groups (NSGs)** to allow only the **required protocols and port ranges** between subnets or resources.

# Network security groups



## **NSGs act as rule containers**

Create **custom security rules** and group them in a **Network Security Group (NSG)**.

## **Assign NSGs to Subnets, NICs, or Both**

**NSGs can be applied at:**

- The **subnet level** (affects all VMs in the subnet)
- The **network interface (NIC)** level (affects that specific VM)
- Or both — **combined enforcement applies**

## **Subnet NSGs are not perimeter firewalls**

Rules are evaluated **at the NIC level**, even when applied to a subnet. Every NIC enforces the rules as if they were local.

## **Rule evaluation order**

- **Inbound traffic:** Subnet NSG → then NIC NSG
- **Outbound traffic:** NIC NSG → then Subnet NSG
  - **Both must allow** the traffic for it to pass.

# NSG Rules

## 5 Tuple

### 1. Source

IP address, CIDR range, Service Tag (e.g., Internet, VirtualNetwork), or Application Security Group (ASG)

### 2. Source Port

A specific port (e.g., 80), range (1000–2000), or \* for all ports

### 3. Destination

IP, CIDR, Service Tag, or ASG — just like Source

### 4. Destination Port

Exact port, range, or wildcard

### 5. Protocol

TCP, UDP, ICMP, ESP, AH, or \* to match all

# NSG Rule Scope with CIDR & Tags

5 Tuple

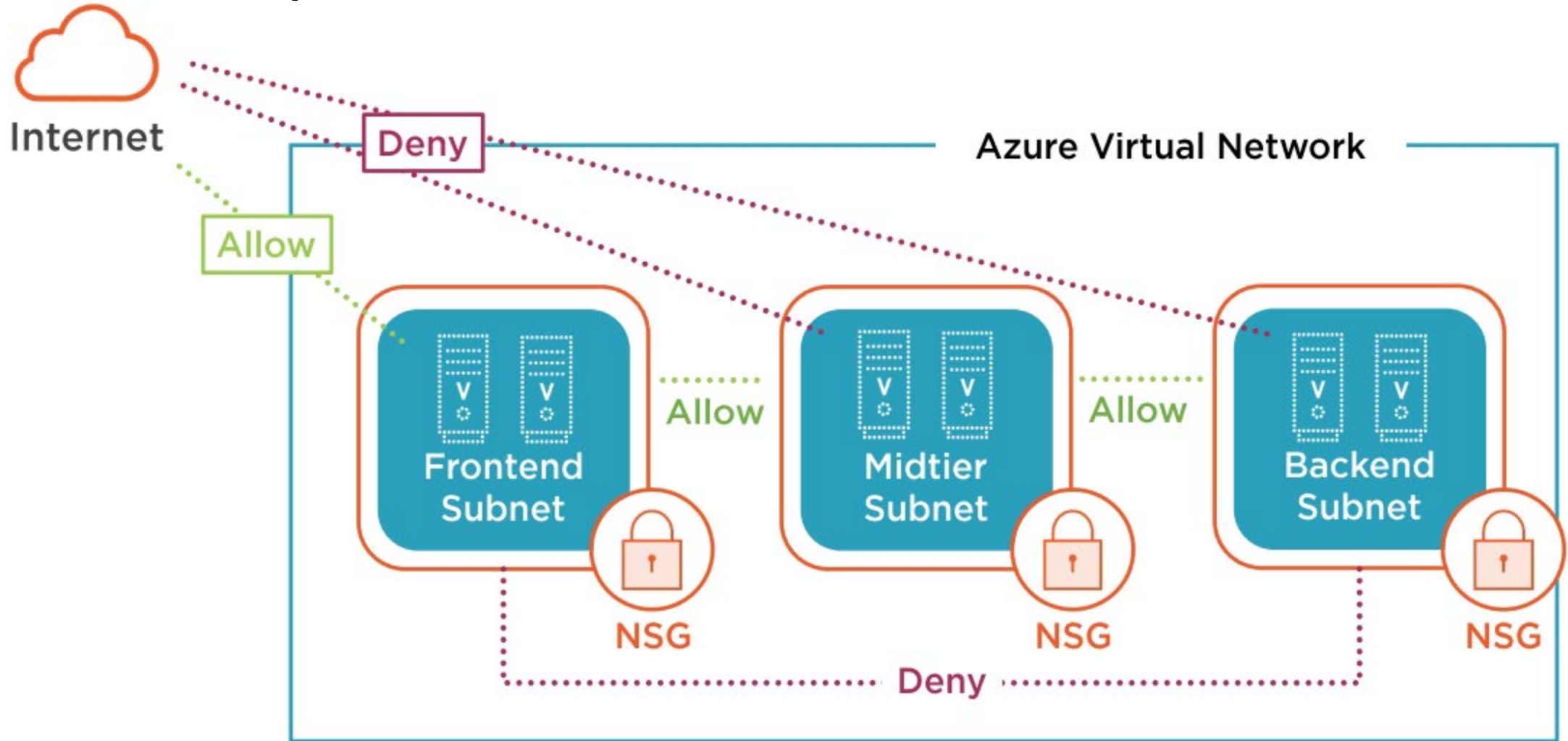
## Source/Destination can be defined using:

- IP Addresses (e.g., 10.0.0.4)
- CIDR Blocks (e.g., 10.0.0.0/24)
- Service Tags (Predefined Labels)

## Common Azure Service Tags

Tag	Description
VirtualNetwork	Matches all addresses within the same VNet (incl. Subnets)
AzureLoadBalancer	Refers to Azure's Internal Load Balancer Infrastructure
Internet	Represents all External IPs (outside the VNet address space)

# NSG Example



# NSG Example

- Rules are combined in a NSG
- Based on the priority flexible configurations are possible
- Lower priority number means higher priority

Description	Priority	Source Address	Source Port	Destination Address	Destination Port	Action
ILB	1010	AZURE_LOADBALANCER	*	*	10000	Allow
Inbound RDP	2005	VIRTUAL_NETWORK	*	*	3389	Allow
Deny all inbound	4000	*	*	*	*	Deny

# Application security groups



## Simplify NSG Management in Dynamic Environments

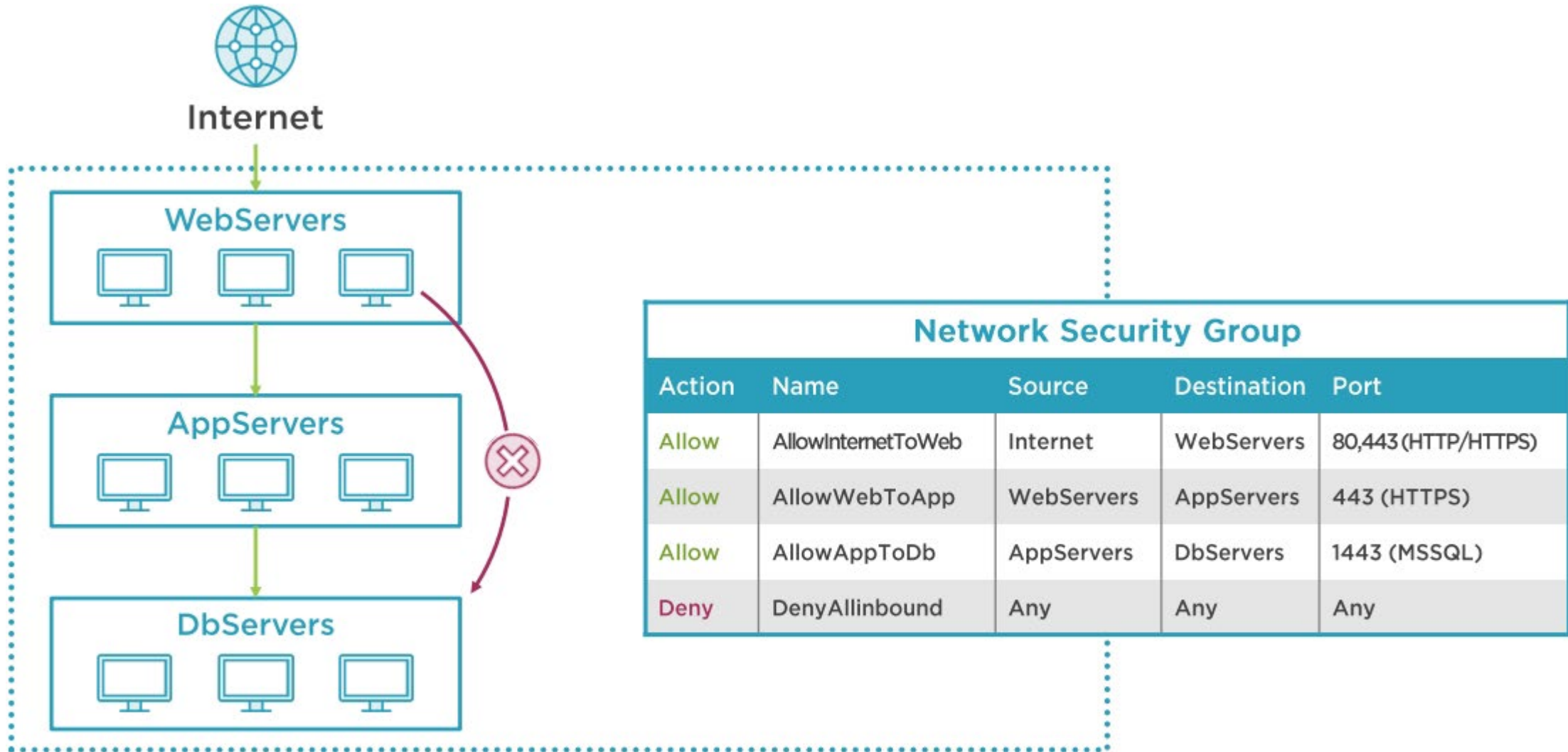
- NSGs traditionally rely on IP address ranges, which can be hard to manage as environments grow.
- Application Security Groups (ASGs) let you group VMs logically by role:

**Example groups:** Web, App, Database

- Each VM NIC can be assigned to one or more ASGs.
- You can reference ASGs in NSG rules instead of IPs or CIDRs.
- ASGs work alongside NSG features like service tags and priority rules.



# ASG Example



# Pop quiz:

**Scenario:**

VNet-EastUS (10.1.0.0/24) is peered with VNet-WestEurope (10.2.0.0/24). You want only DB servers in WestEurope to talk to App servers in EastUS—nothing else should cross the peering.

**What is the simplest and most secure way to enforce this?**

- A. Deploy Azure Firewall in EastUS to filter peered traffic
- B. Use “Block traffic to remote VNet” on WestEurope peering + NSG allow only DB subnet
- C. Apply NSG on EastUS subnet allowing only 10.2.0.0/24 → 10.1.0.0/24
- D. Use User Defined Route to drop all remote VNet IP ranges except the DB subnet

# Pop quiz:

**Scenario:**

VNet-EastUS (10.1.0.0/24) is peered with VNet-WestEurope (10.2.0.0/24). You want only DB servers in WestEurope to talk to App servers in EastUS—nothing else should cross the peering.

**What is the simplest and most secure way to enforce this?**

- A. Deploy Azure Firewall in EastUS to filter peered traffic
- B. Use “Block traffic to remote VNet” on WestEurope peering + NSG allow only DB subnet
- C. Apply NSG on EastUS subnet allowing only 10.2.0.0/24 → 10.1.0.0/24
- D. Use User Defined Route to drop all remote VNet IP ranges except the DB subnet