

# Microsoft Azure Network Engineer: Design and Implement Core Networking Infrastructure

---

## Design and Implement Private IP Addressing for VNets



**Tim Warner**

Author Evangelist, Pluralsight

@TechTrainerTim   TechTrainerTim.com



# Overview



**Plan and deploy virtual networks (VNets) on Azure**

**Consider the need for subnet delegation**



# Relevant Exam AZ-700 Skills

## **Exam AZ-700: Designing and Implementing Microsoft Azure Networking Solutions – Skills Measured**

### **Design and Implement Core Networking Infrastructure (20–25%)**

Design and implement private IP addressing for VNets

- create a VNet
- plan and configure subnetting for services, including VNet gateways, private endpoints, firewalls, application gateways, and VNet-integrated platform services
- plan and configure subnet delegation



# Exercise Files

Timothy  
timothywarner316@gmail.com

## Troubleshooting with Microsoft Azure Network Watcher

by Tim Warner

Microsoft now gives you packet-level access to your Windows Server and Linux virtual machines (VMs) running in Azure. You'll learn how to use Network Watcher to troubleshoot network security groups (NSGs), perform packet captures, and much more.

[Resume Course](#) [Bookmark](#) [Add to Channel](#)

Table of contents

Description

Transcript

**Exercise files**

Discussion

Learning Check

Recommended

These exercise files are intended to provide you with the assets you need to create a video-based hands-on experience. With the exercise files, you can follow along with the author and re-create the same solution on your computer. We find this to be even more effective than written lab exercises.

[Download exercise files](#)

### Course author

**Tim Warner**

Timothy Warner is a Microsoft Most Valuable Professional (MVP) in Cloud and Datacenter Management who is based in Nashville, TN.

### Course info

Level	Intermediate
Rating	★★★★★
My rating	★★★★★
Duration	2h 12m
Released	31 Oct 2017

### Share course

[f](#) [t](#) [g+](#) [in](#)



# Exercise Files

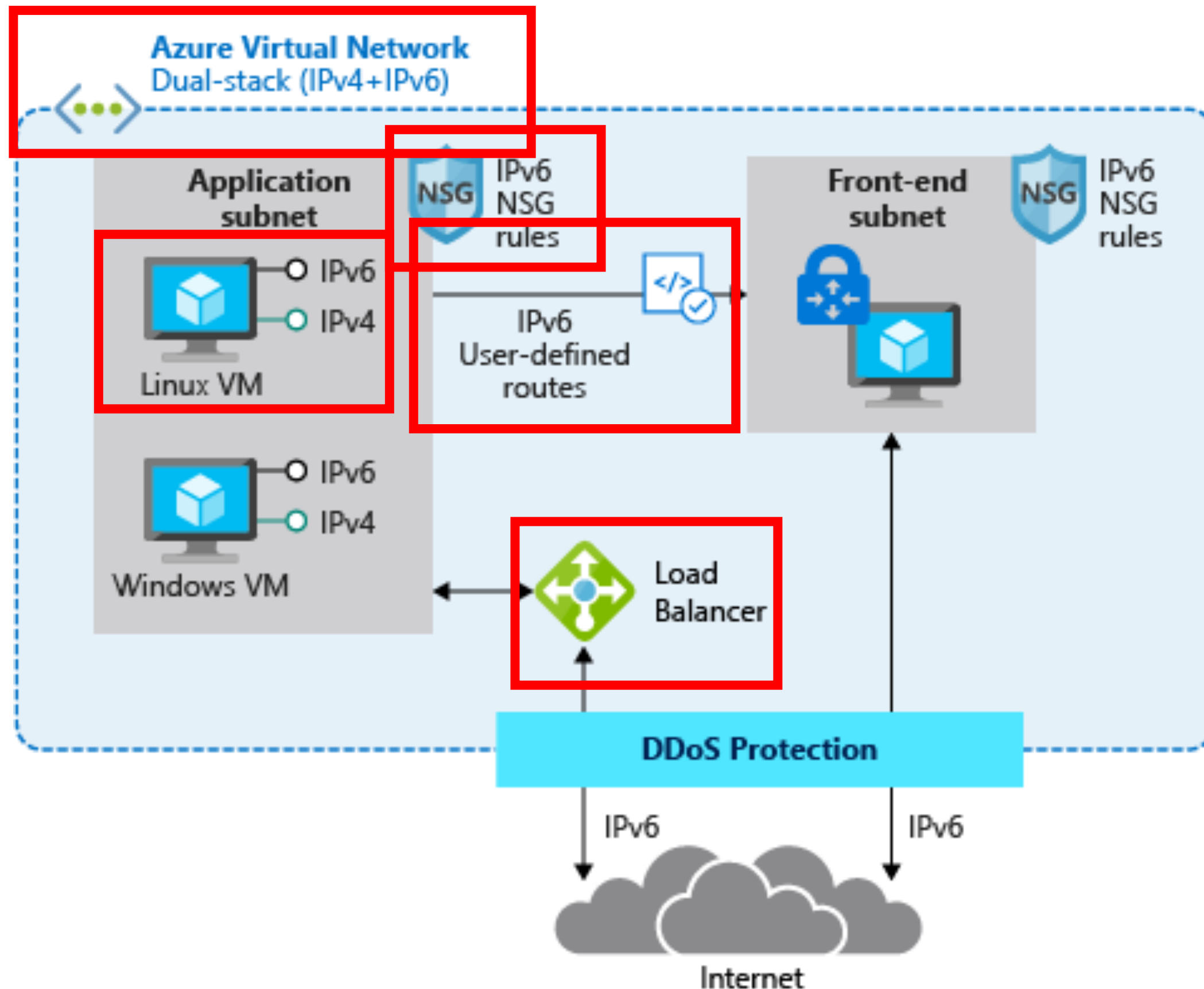
The screenshot displays a Windows desktop environment with three overlapping windows:

- File Explorer:** Located on the left, it shows the path `C:\Users\Tim\Downloads\azure`. The file list contains folders named 02, 03, 04, 05, and 06. Folder 02 is selected. The status bar at the bottom indicates "0 / 5 object(s) selected".
- Code Editor:** The central window is titled `microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt`. It displays a list of 22 numbered links related to Azure AD PIM documentation. The links are as follows:
  - 1 Module 4: Organize and Perform Azure AD PIM Access Reviews
  - 2
  - 3 Microsoft Azure
  - 4 <https://azure.microsoft.com/en-us/>
  - 5
  - 6 Azure Documentation
  - 7 <https://docs.microsoft.com/en-us/azure/>
  - 8
  - 9 Azure AD Privileged Identity Management (PIM) documentation | Microsoft Docs
  - 10 <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/>
  - 11
  - 12 Identity Governance - Azure Active Directory | Microsoft Docs
  - 13 <https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview>
  - 14
  - 15 Create an access review of Azure resource roles in PIM - Azure Active Directory | Microsoft Docs
  - 16 <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-start-access-review>
  - 17
  - 18 Review access to Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
  - 19 <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-perform-security-review>
  - 20
  - 21 View audit history for Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
  - 22 <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-use-audit-log>
- File Details Window:** A small window on the right shows details for a file in the `02\demos\` folder. It includes a table with the following data:

	Size	Pack
	1 298	
	359	



# A Word About IPv6



No IPv6 on AZ-\* exams

No VPN Gateway support

No AKS container support

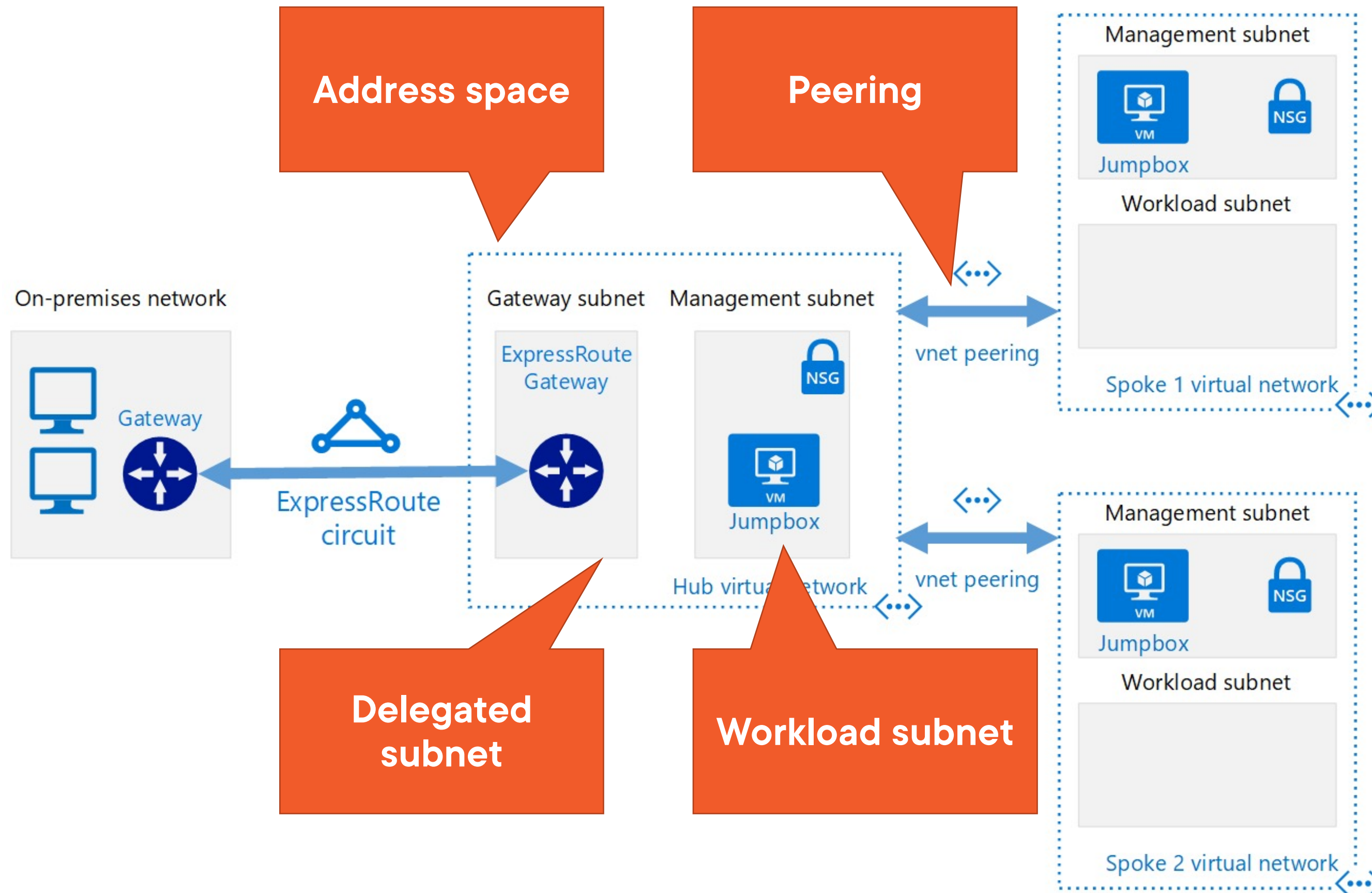
# Plan Virtual Networks on Azure

---





# Azure Virtual Network Components

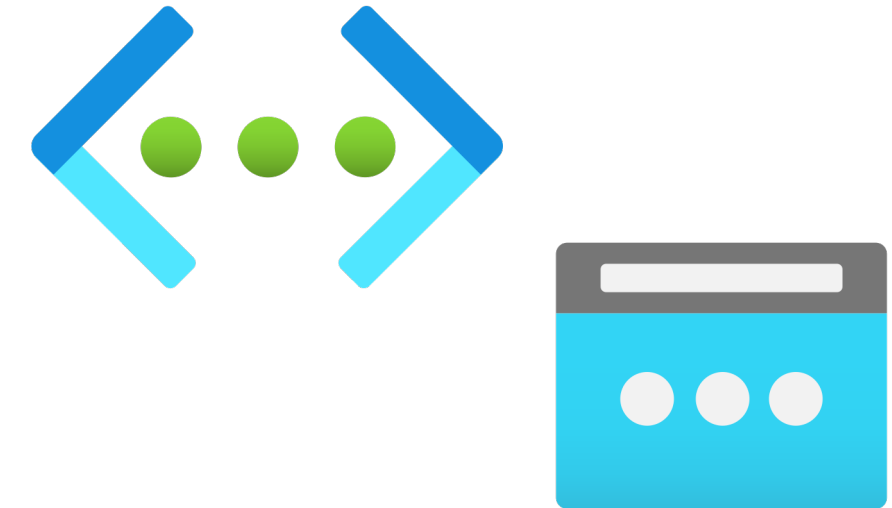




# Planning for Private IPv4 Addresses

## RFC 1918 ranges

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)



## Restricted ranges

- 224.0.0.0/4 (Multicast)
- 255.255.255.255/32 (Broadcast)
- 127.0.0.0/8 (Loopback)
- 169.254.0.0/16 (Link-local)
- 168.63.129.16/32 (Internal DNS)

## Restricted subnet IPs

- x.x.x.0: Network address
- x.x.x.1: Reserved by Azure for the default gateway
- x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space
- x.x.x.255: Network broadcast address

**Subnets can range in size from /8 to /29**

Azure Wire  
Server  
168.63.129.16



**Virtual public IP address (VIP)**

**VM Agent heartbeat**

**Azure Load Balancer health probes**

**Azure-provided DHCP**

**Azure-provided DNS**

**Azure-provided routing**

# Azure VM Outbound Internet Connectivity

## NAT Gateway

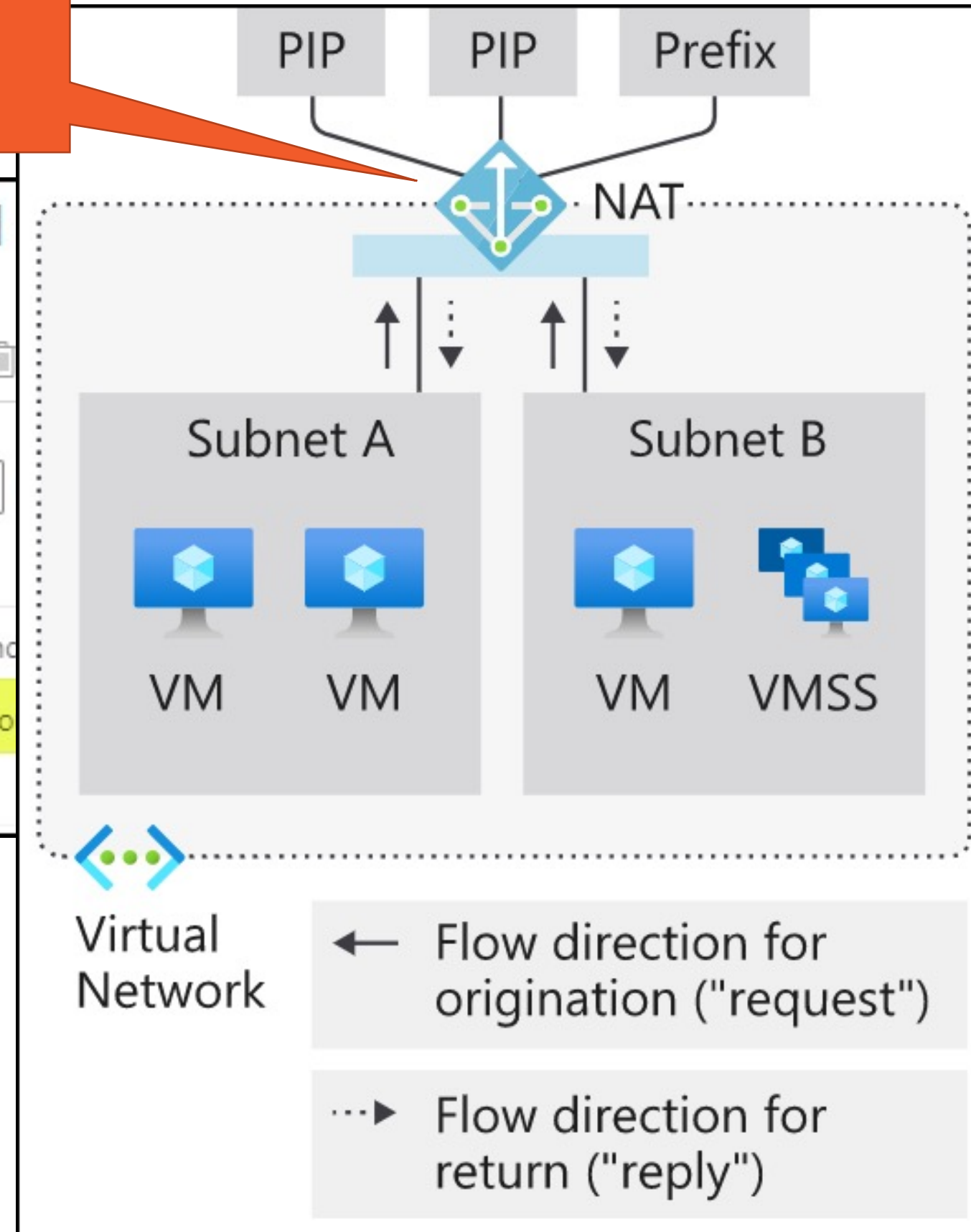
timvm01nsg720 | Outbound

Network security group

+ Add Hide default rules Refresh

Filter by name

Priority ↑↓	Name ↑↓
<input type="checkbox"/> 65000	AllowVnetOutBound
<input checked="" type="checkbox"/> 65001	AllowInternetOutBo
<input type="checkbox"/> 65500	DenyAllOutBound



Filter by name

Action == all

Destination ↑↓	Action ↑↓
VirtualNetwork	✓ Allow
Internet	✓ Allow
Any	✗ Deny



# Planning for Name Resolution

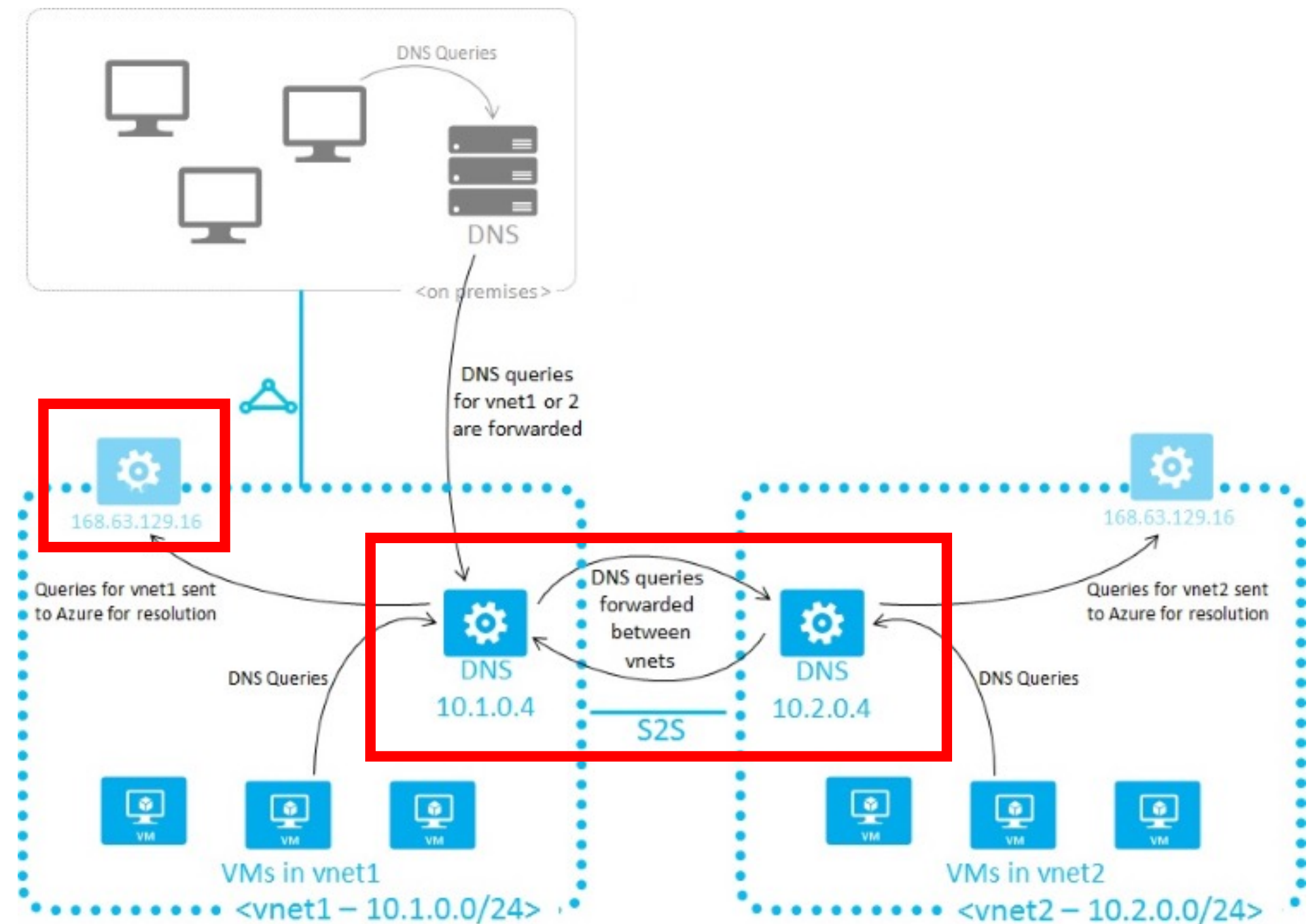
Azure-provided DNS is limited to the VNet scope and uses the Wire Server

Single-label hostnames (like WINS)

\*.cloudapp.net public DNS name (you can add your own)

Add your own DNS server IPs at the VNet and/or vNIC scope

Alternative: private Azure DNS zone

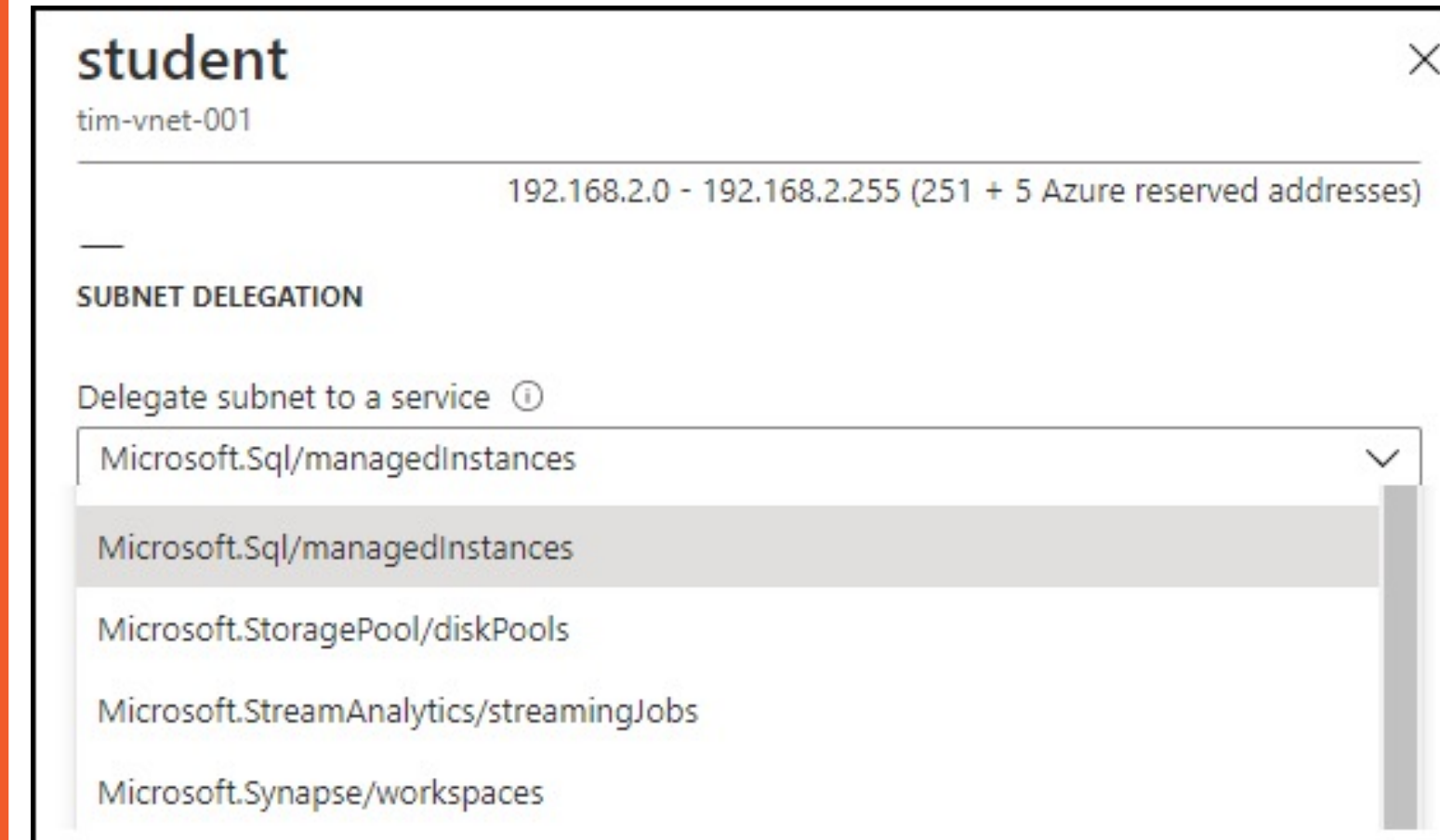


# Subnet Delegation

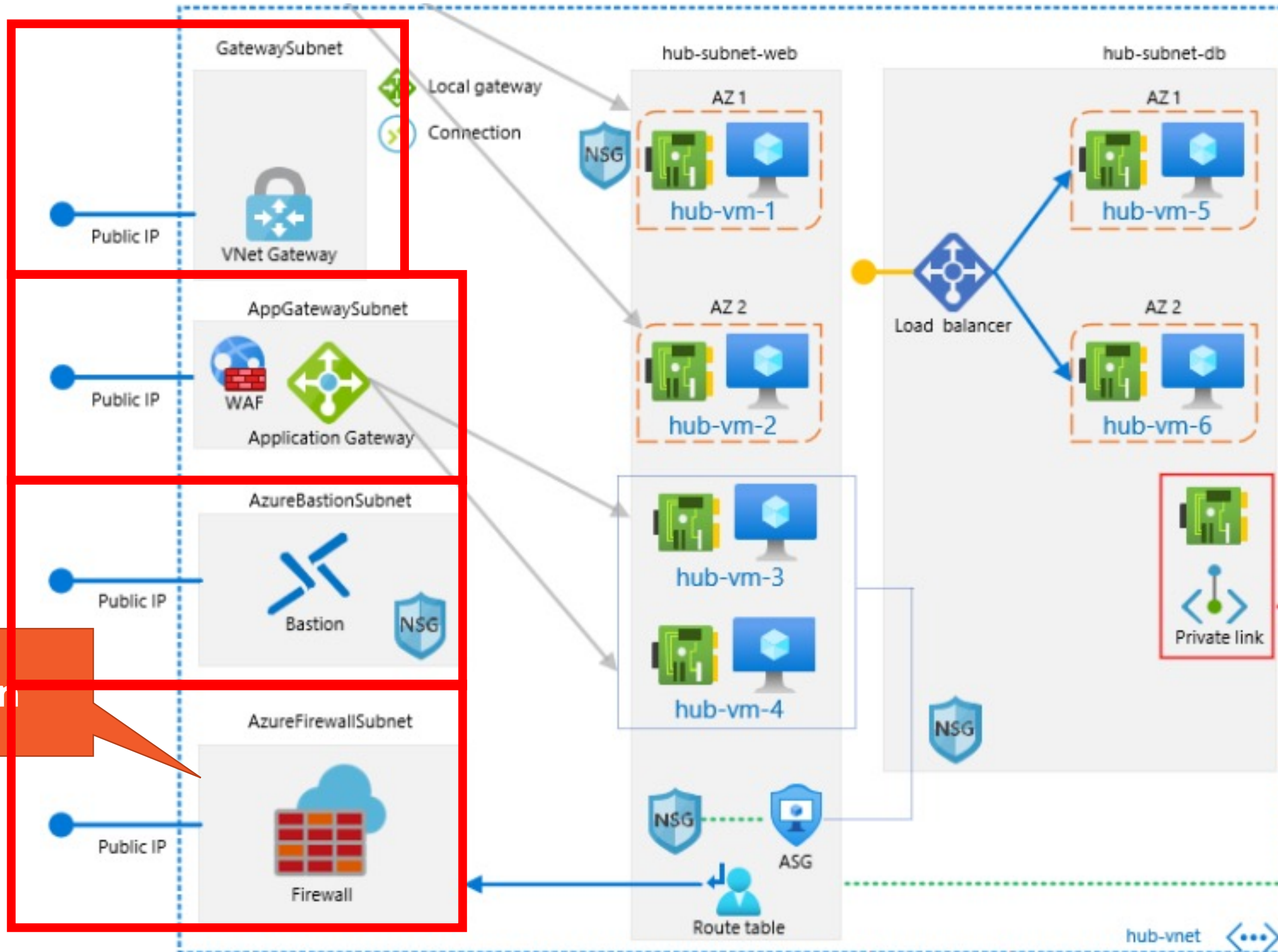
**Designate a subnet for a particular Azure PaaS service**

**Allows PaaS service to establish basic network configuration rules**

**Some Azure network virtual appliances (NVAs) have reserved subnet labels**

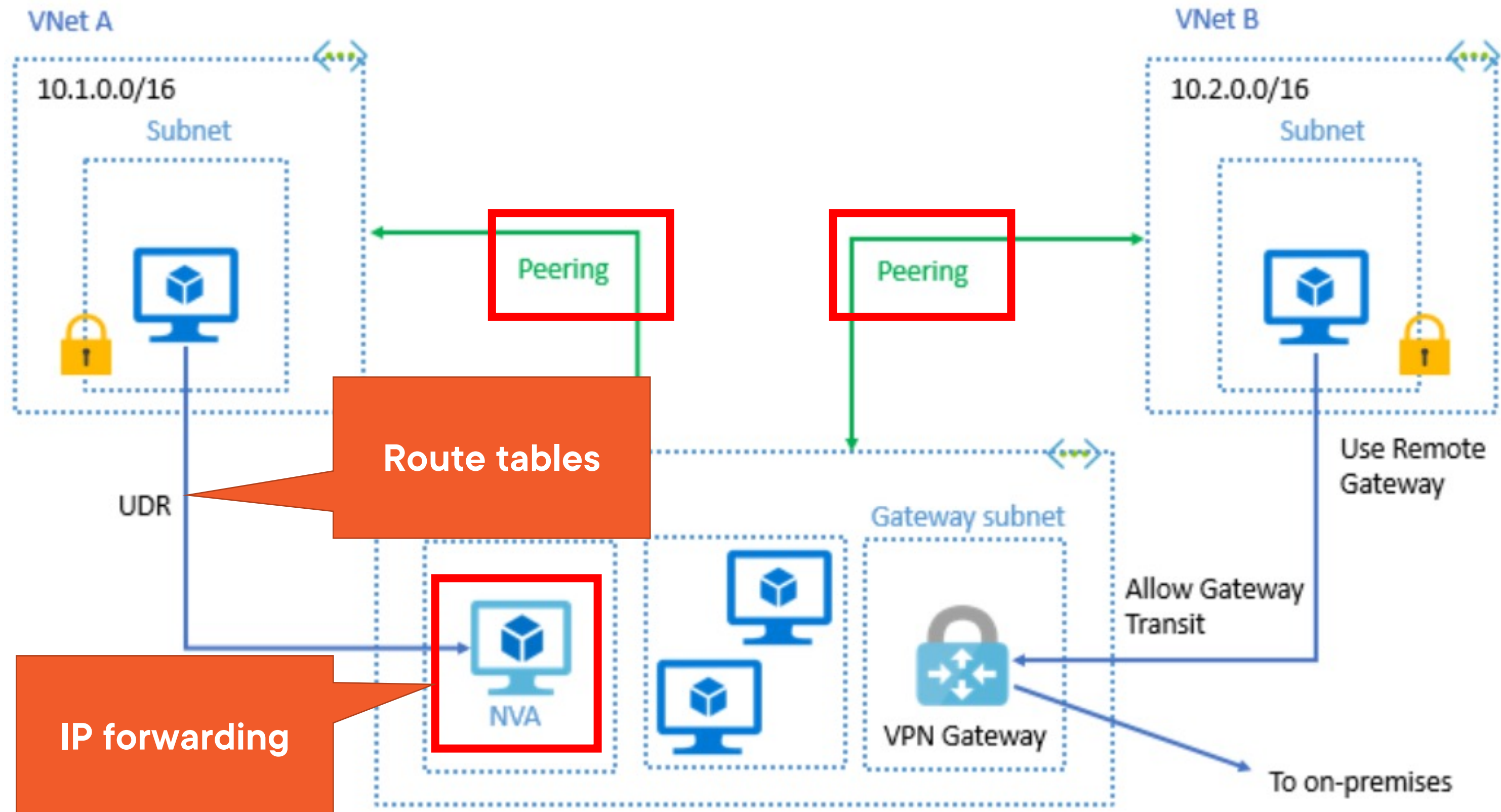


# Subnet Delegation Examples

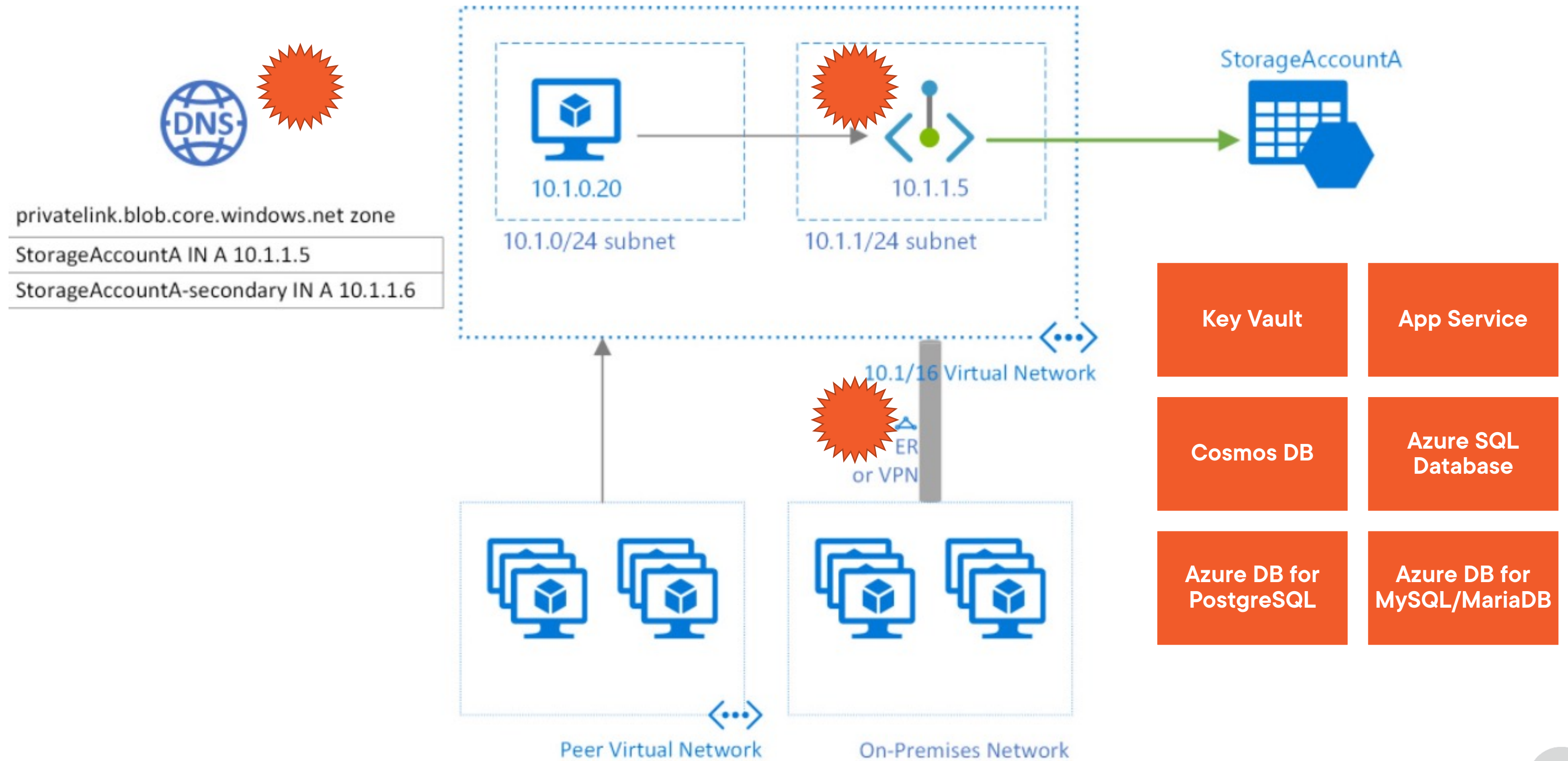




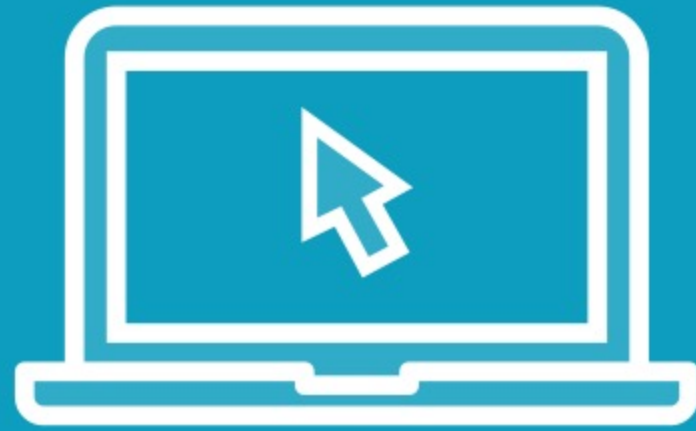
# Hub-and-Spoke Topology



# Private Endpoints



# Demo



# 1

**Configure TCP/IP on VM NIC**

**Name resolution**

**NAT gateway?**





# Deploy Virtual Networks on Azure

---



# Azure VNet Deployment Methods

**Portal**

**PowerShell/CLI**

**Bicep/ARM  
template**

**REST API**

**Azure SDKs**

**Terraform**



# Demo



# 2

**Create one VNet in the portal**

**Create another one with ARM template**

- Quickly generate the Bicep





## Summary



**Ensure all your VM TCP/IP configuration happens at the Azure control plane**

- Except for software firewall, etc.

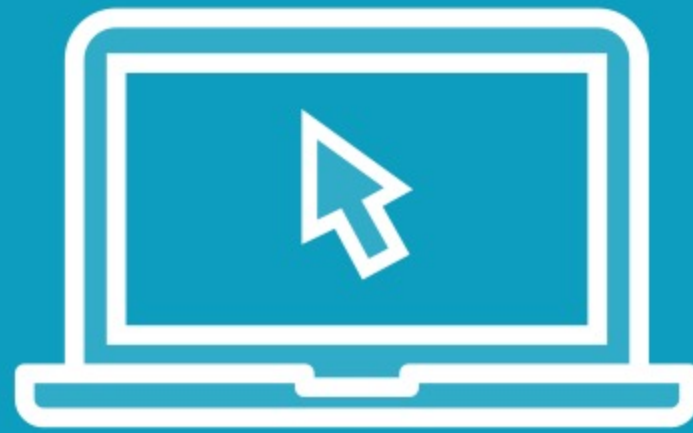
**Consider governing your VNets with Azure Blueprints**

**"How can I join my Azure VMs to our local Active Directory domain?"**

**Next module: *Design and Implement Name Resolution***



# Demo



# 1

## Configure TCP/IP on VM NIC

### Name resolution

- Do custom servers 192.x and wire server
- Verify Internet resolution works

### NAT gateway

- Test ipaddress.com before and after



# Demo



# 2

**Create one VNet in the portal**

**Create another one with ARM template**

- Quickly generate the Bicep

