Design and Implement Azure Virtual Network NAT

Tim Warner

Principal Author Evangelist, Pluralsight

@TechTrainerTim   TechTrainerTim.com

Overview

Planning for Azure Virtual Network NAT

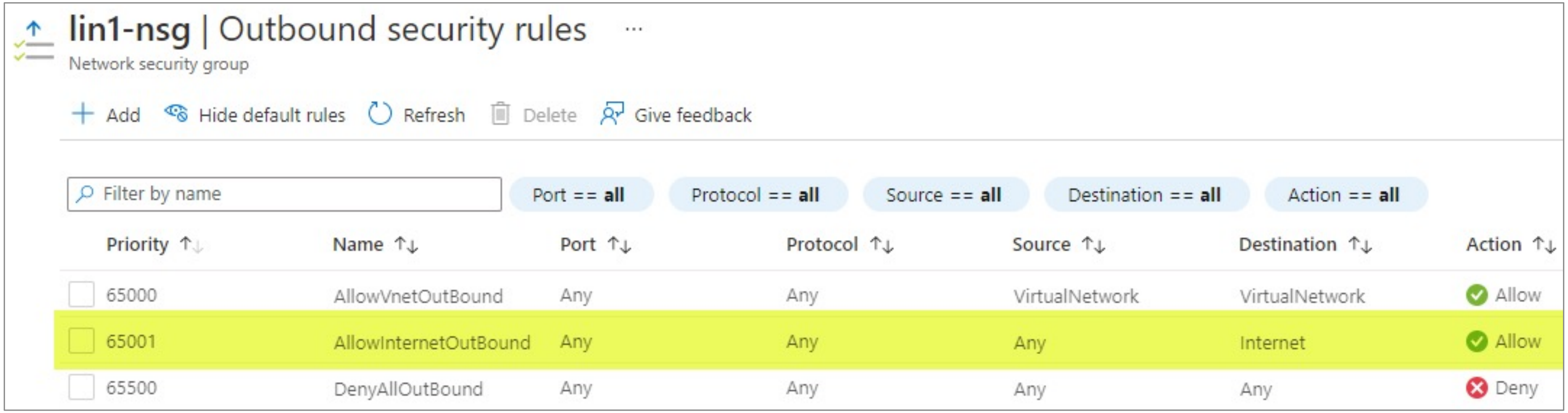
- When to choose

Implementing Azure Virtual Network NAT

- Allocating IP addresses and prefixes
- Associating with subnet(s)

Planning for Azure Virtual Network NAT

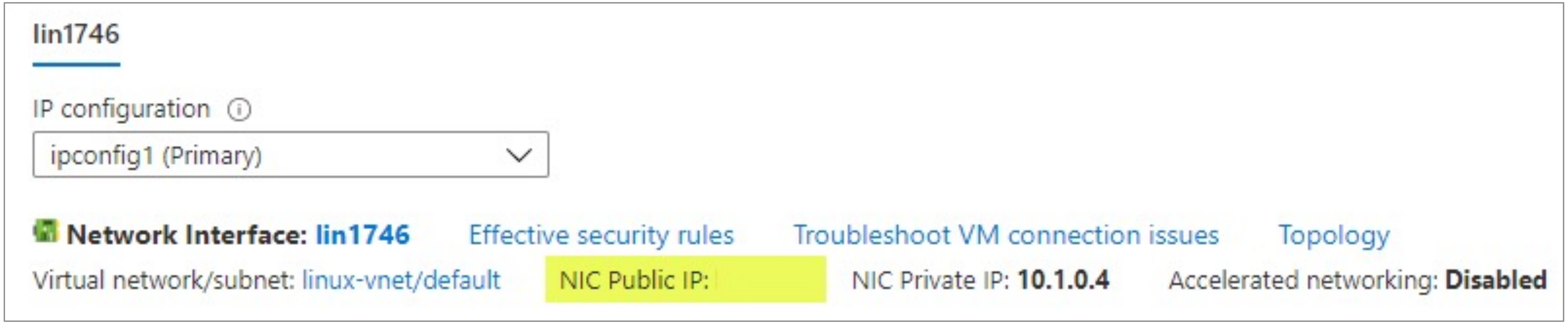
Default Outbound Access IP Mechanism



lin1-nsg | Outbound security rules ···

Network security group

	Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
□	65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
□	65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
□	65500	DenyAllOutBound	Any	Any	Any	Any	☒ Deny



lin1746

IP configuration ⓘ

ipconfig1 (Primary)

Network Interface: lin1746 Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: linux-vnet/default NIC Public IP: NIC Private IP: **10.1.0.4** Accelerated networking: **Disabled**

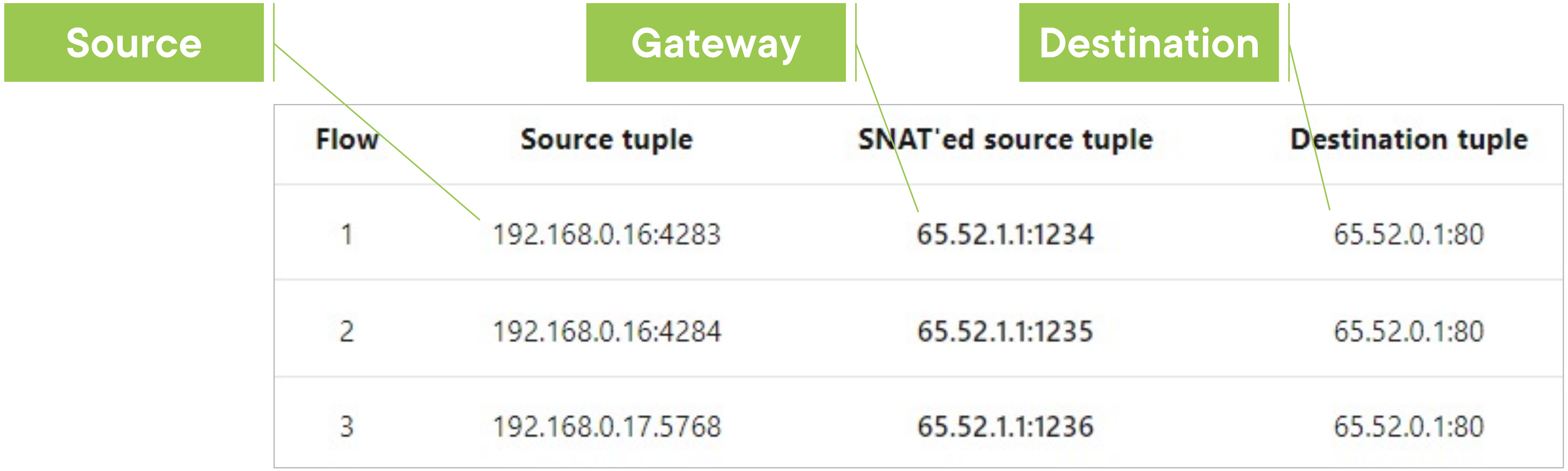
timw.info/27e

Source Network Address Translation (SNAT)

Allows private network traffic outbound access to the Internet through a shared public IP address. Also gives the private endpoint a predictable public IP address for connectivity and monitoring purposes

Port Address Translation (PAT)

NAT extension that allows multiple private endpoints to “share” a single IP address



Source

Gateway

Destination

Flow	Source tuple	SNAT'ed source tuple	Destination tuple
1	192.168.0.16:4283	65.52.1.1:1234	65.52.0.1:80
2	192.168.0.16:4284	65.52.1.1:1235	65.52.0.1:80
3	192.168.0.17.5768	65.52.1.1:1236	65.52.0.1:80

timw.info/8h0

Azure Virtual Network NAT

Resilient, fully managed Source Network Address Translation (SNAT) gateway

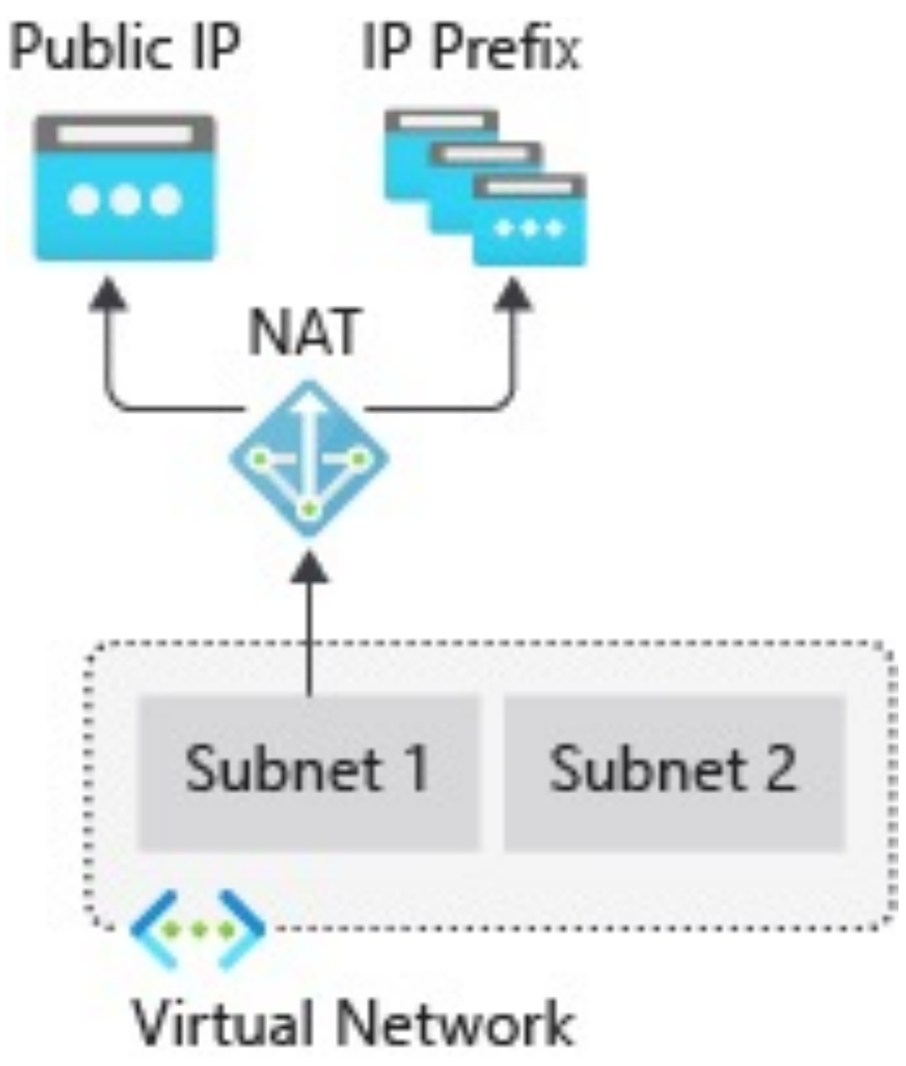
Simplifies outbound Internet connectivity for your Azure

VMs

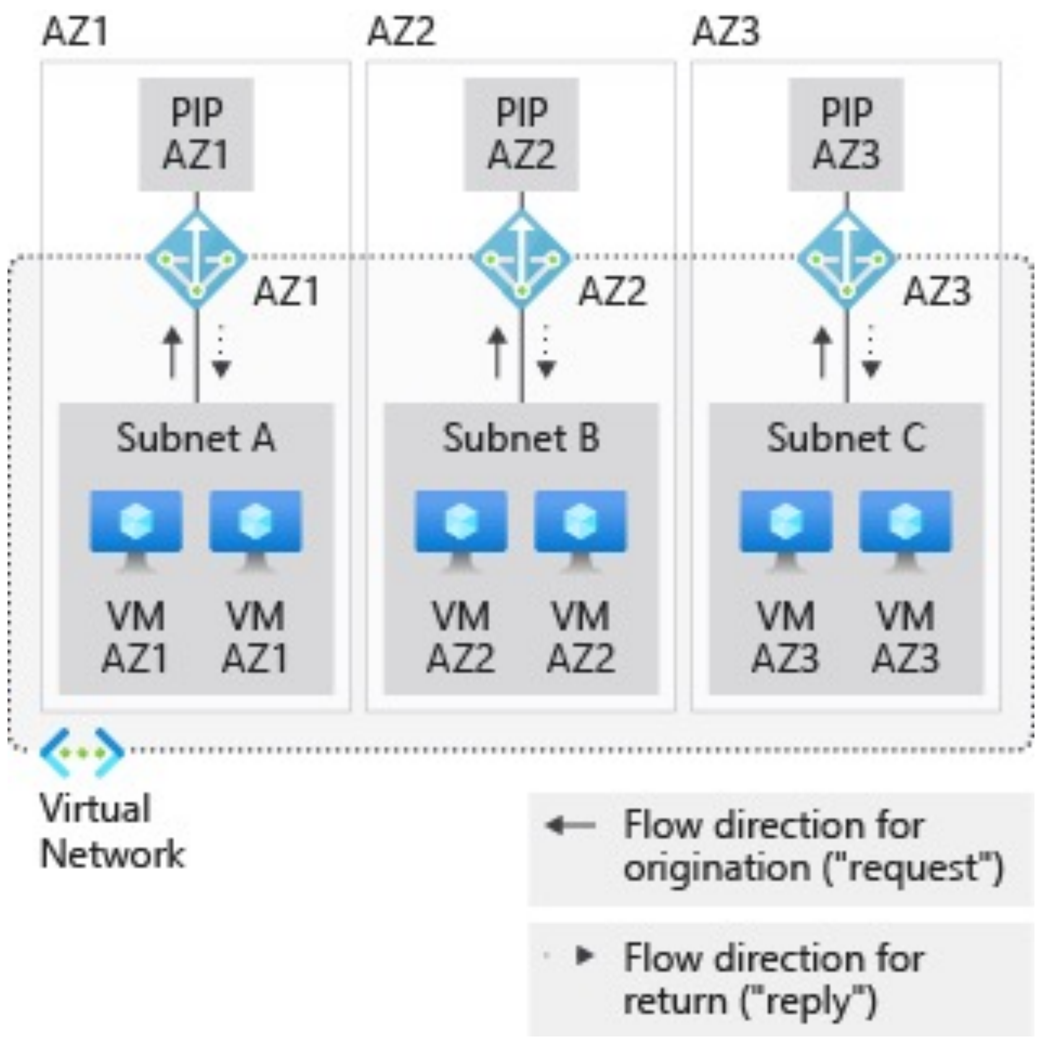
Regional or zone isolation

- Linked to the subnet

Azure Virtual Network NAT Architecture



Regional deployment



Zonal deployment

timw.info/4i7

Outbound Public IP Addresses

Public IP address

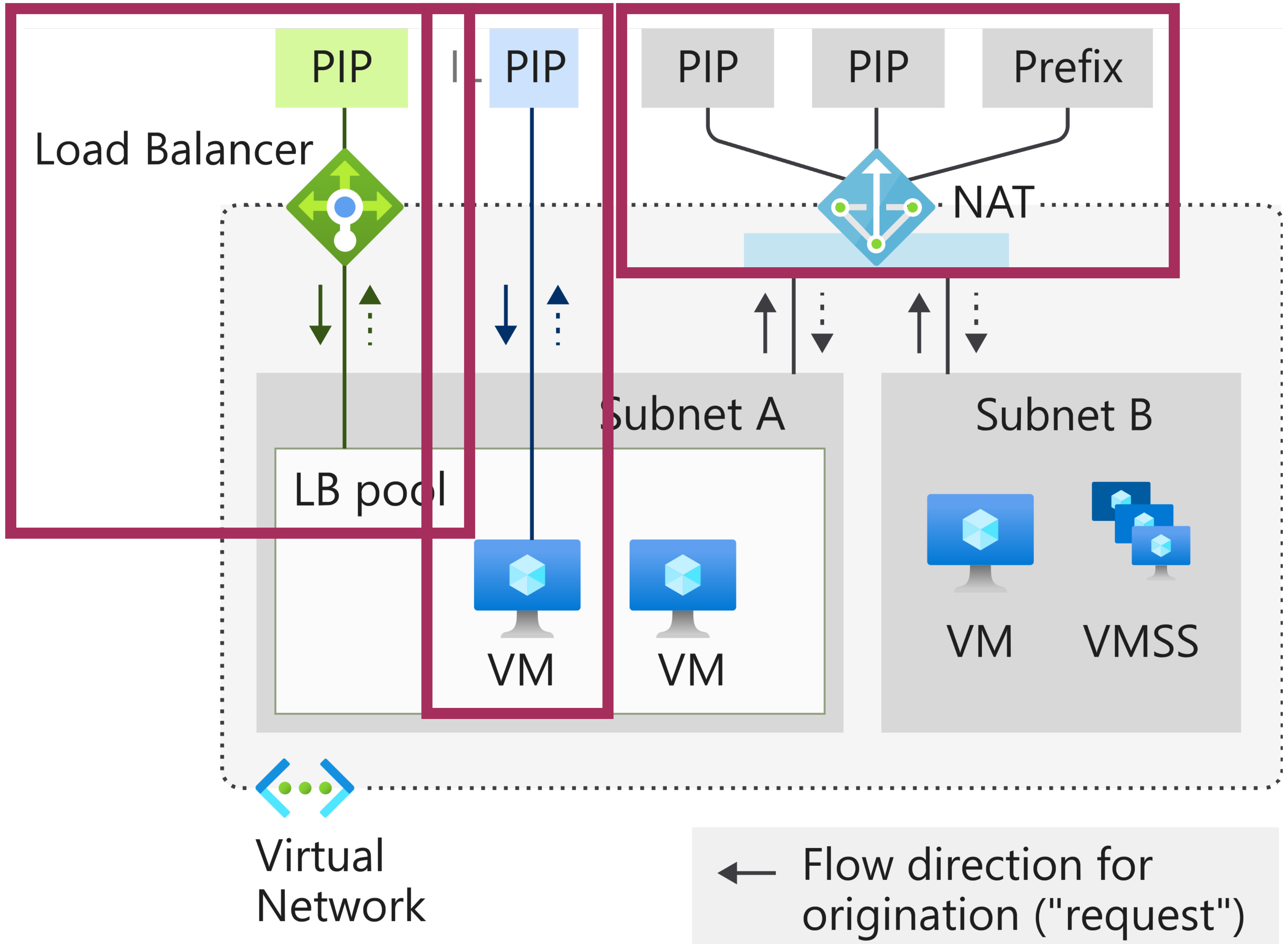
- Maximum 16 addresses (including prefix)
- Standard SKU
- Each address provides 64,000 SNAT ports

Public IP prefix

- Maximum 16 addresses (including individual IPs)
- Contiguous IP address range
- Can be shared across NAT gateways

Traffic Flows

Inbound



Outbound

← Flow direction for origination ("request")

⋯▸ Flow direction for return ("reply")

timw.info/62d

Implementing Azure Virtual Network NAT

Deploy a NAT Gateway (Bicep)

```
param vnetName string = 'myVnet'
param subNetName string = 'mySubnet'
param vnetAddressSpace string = '192.168.0.0/16'
param vnetSubnetPrefix string = '192.168.0.0/24'
param natGatewayName string = 'myNATgateway'
param publicIpDNS string = 'gw-${uniqueString(resourceGroup().id)}'
param location string = resourceGroup().location

var publicIpName = '${natGatewayName}-ip'
```

Deploy a NAT Gateway (Bicep)

```
resource publicIp 'Microsoft.Network/publicIPAddresses@2020-06-01' = {
  name: publicIpName
  location: location
  sku: {
    name: 'Standard'
  }
  properties: {
    publicIPAddressVersion: 'IPv4'
    publicIPAllocationMethod: 'Static'
    idleTimeoutInMinutes: 4
    dnsSettings: {
      domainNameLabel: publicIpDNS
    }
  }
}
```

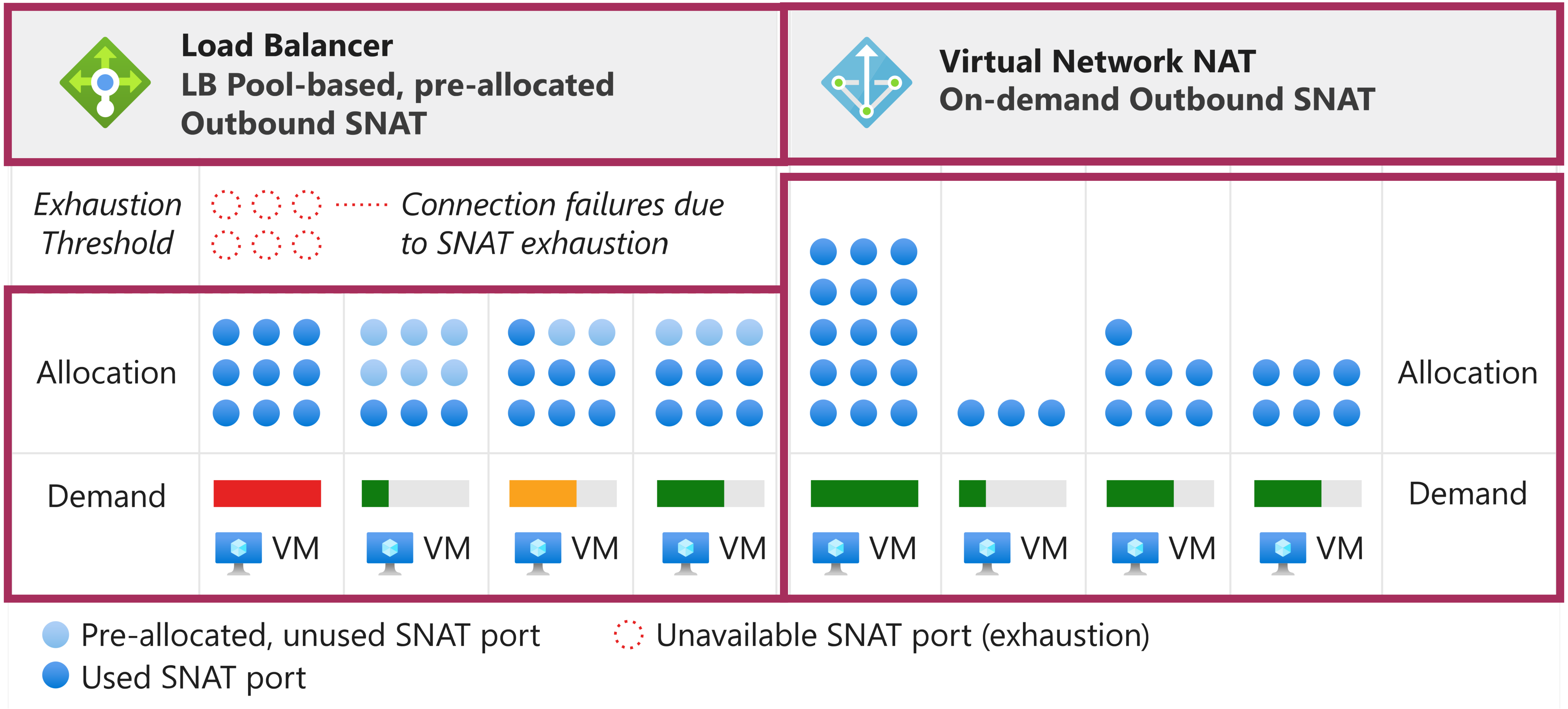
Deploy a NAT Gateway (Bicep)

```
 resource natGateway 'Microsoft.Network/natGateways@2020-06-01' = {
  name: natGatewayName
  location: location
  sku: {
    name: 'Standard'
  }
  properties: {
    idleTimeoutInMinutes: 4
    publicIpAddresses: [
      {
        id: publicIp.id
      }
    ]
  }
}
```

Deploy a NAT Gateway (Bicep)

```
resource vnet 'Microsoft.Network/virtualNetworks@2020-06-01' = {
  name: vnetName
  location: location
  properties: {
    addressSpace: {
      addressPrefixes: [
        vnetAddressSpace
      ]
    }
    subnets: [
      {
        name: subNetName
        properties: {
          addressPrefix: vnetSubnetPrefix
          natGateway: {
            id: natGateway.id
          }
          privateEndpointNetworkPolicies: 'Enabled'
          privateLinkServiceNetworkPolicies: 'Enabled'
        }
```

Combating SNAT Port Exhaustion



Load Balancer
LB Pool-based, pre-allocated Outbound SNAT

Virtual Network NAT
On-demand Outbound SNAT

Exhaustion Threshold

Connection failures due to SNAT exhaustion

Allocation

Demand

VM VM VM VM VM VM VM VM

● Pre-allocated, unused SNAT port

● Used SNAT port

○ Unavailable SNAT port (exhaustion)

timw.info/34i

Demo

1

Work with default outbound access

Deploy NAT gateway

Test VM access

Monitor

Summary

Azure Virtual Network NAT gives you a convenient alternative to Azure Load Balancer as a SNAT solution

Please be careful assigning public IP addresses directly to Azure VMs

- Microsoft publishes their service tag ranges every month

Thanks so much!

Courses: *timw.info/ps*

Twitter: *@TechTrainerTim*