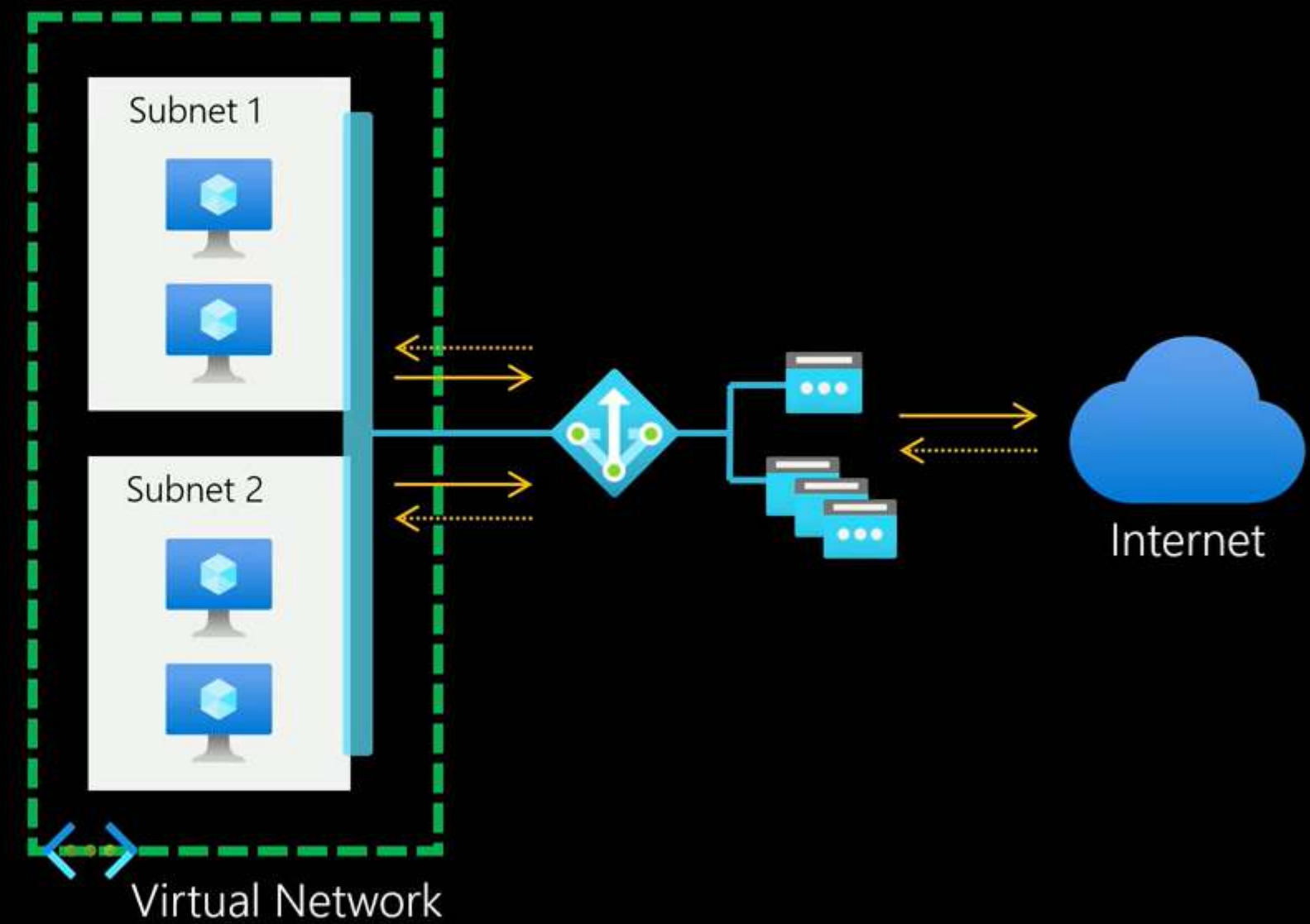# Azure NAT Gateway

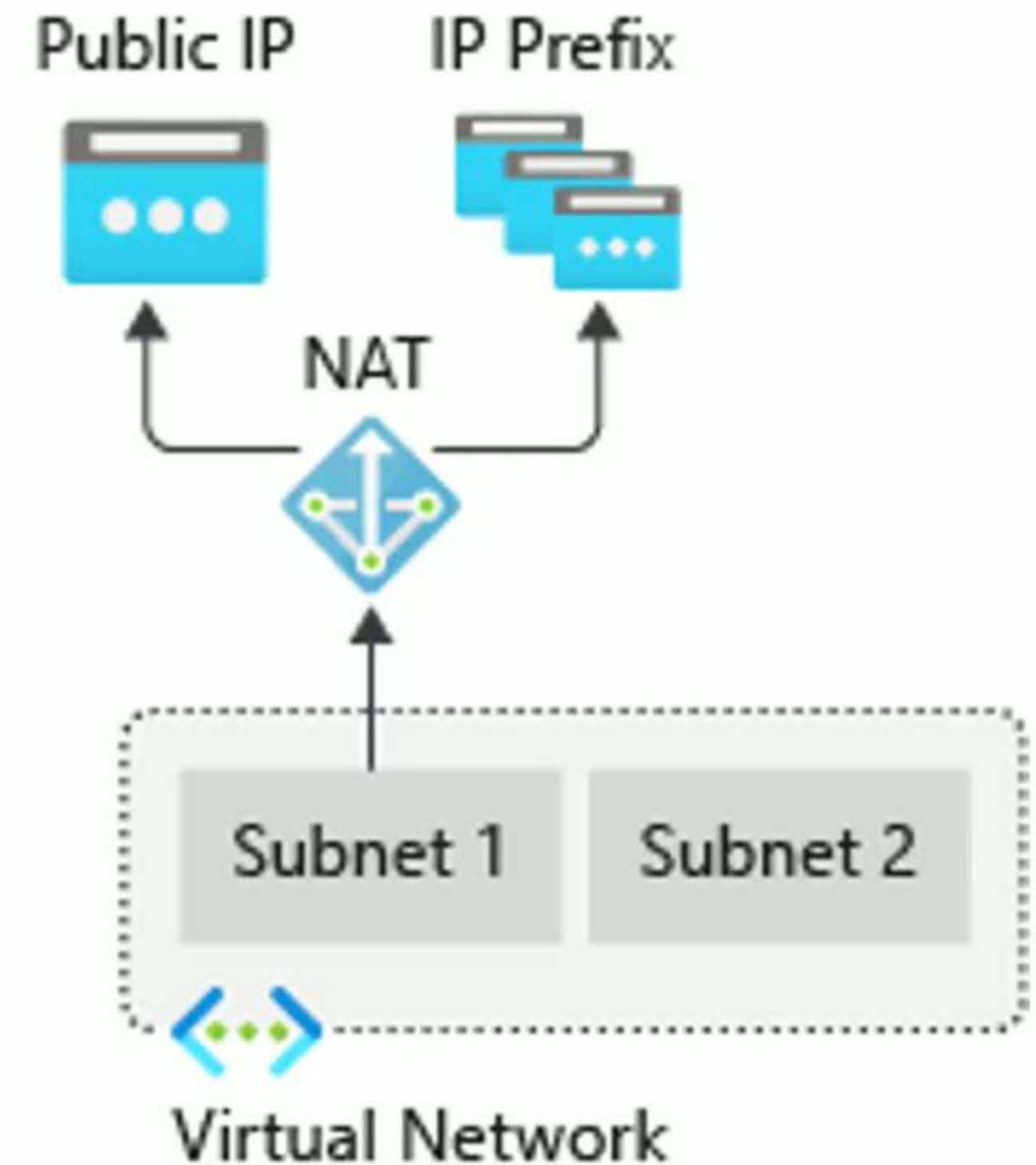# Azure NAT Gateway

Network Address Translation (NAT) service.
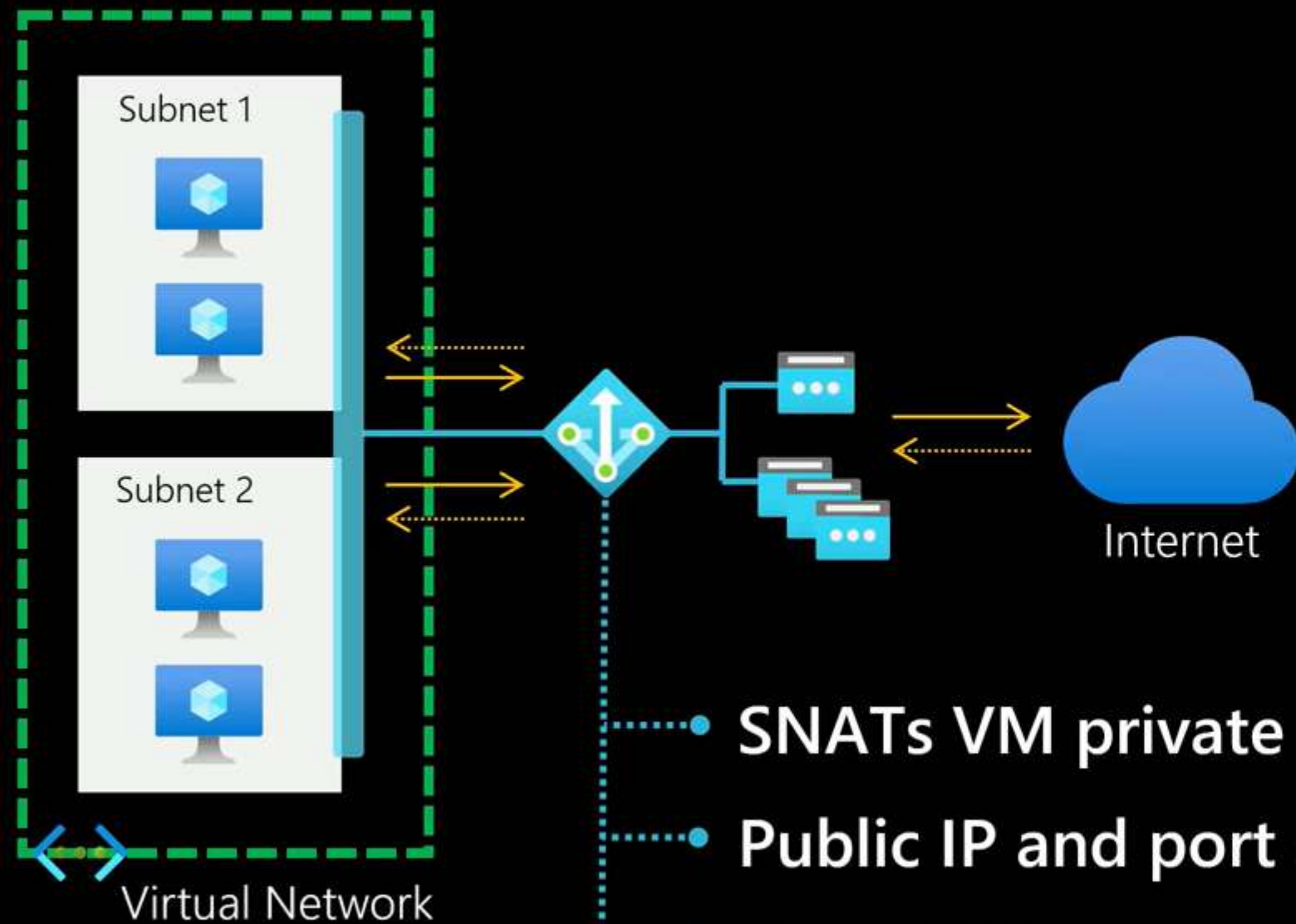
Let all instances in a private subnet connect outbound to the internet while remaining fully private.

Unsolicited inbound connections from the internet aren't permitted through a NAT gateway.

Provides dynamic SNAT port functionality to automatically scale outbound connectivity and reduce the risk of SNAT port exhaustion.

Public IP   IP Prefix

NAT

Subnet 1   Subnet 2

Virtual Network

Azure NAT Gateway SNAT

Subnet 1

Subnet 2

Virtual Network

Internet

- SNATs VM private IP and port to public IP and port
- Public IP and port selected at random to connect outbound
- Many VMs can use same NAT gateway IP to connect outbound

SNAT scaled with NAT Gateway by assigning up to 16 public IPs.

Load Balancer SNAT

Public Load Balancer frontend IPs could provide outbound connectivity to the internet.

This configuration uses source network address translation (SNAT).

SNAT translates virtual machine's private IP into the load balancer's public IP address.
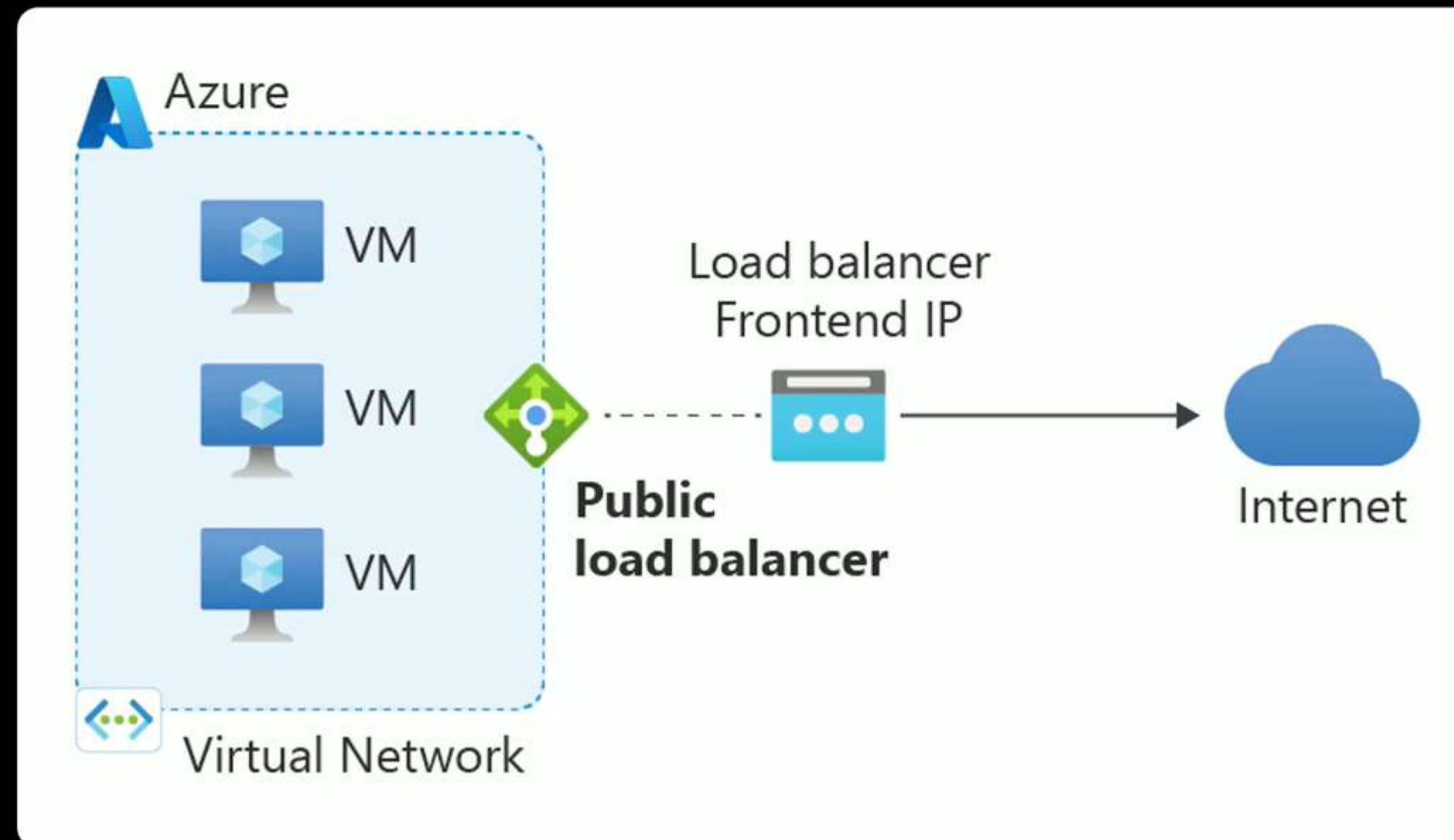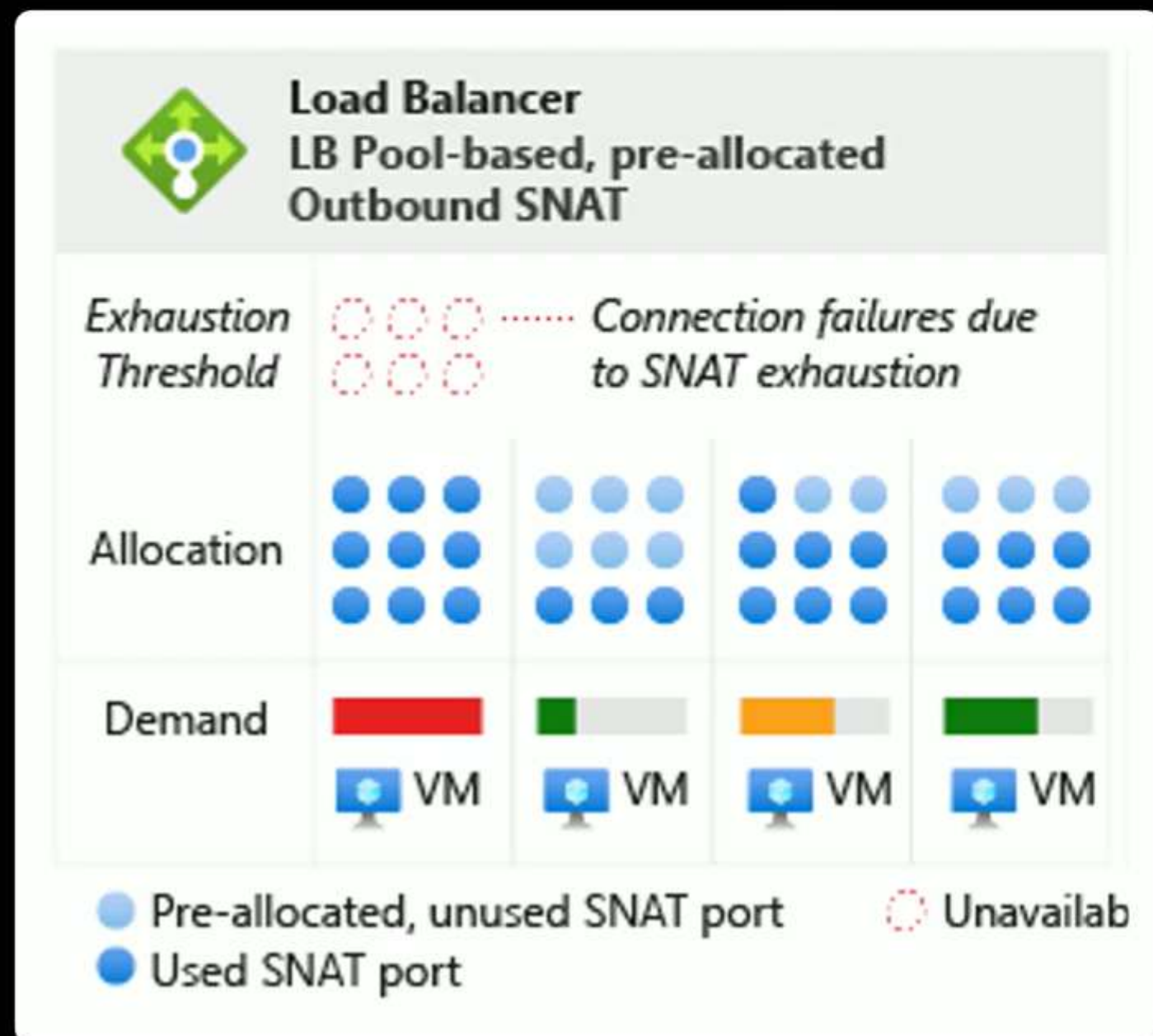
Load Balancer SNAT port exhaustion issue

With LB, each VM use a fixed number (up to 1024) pre-allocated SNAT ports.

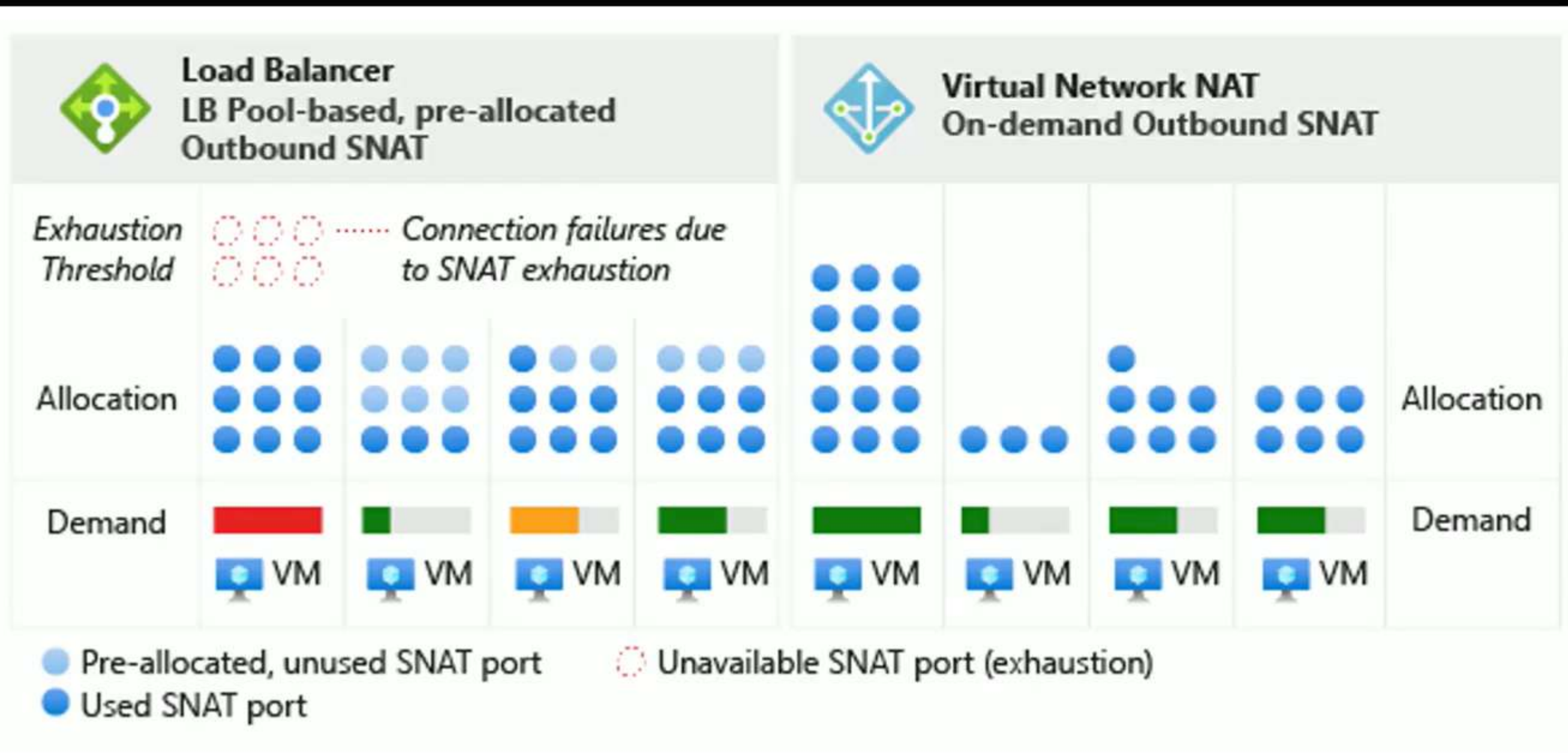If a VM need more, it will run into port exhaustion and connection will be dropped.

Meanwhile, other VMs might have available SNAT ports!

Load Balancer SNAT port exhaustion issue

With **NAT Gateway**, pre-allocation of SNAT ports isn't required, which means SNAT ports aren't left unused by VMs not actively needing them.

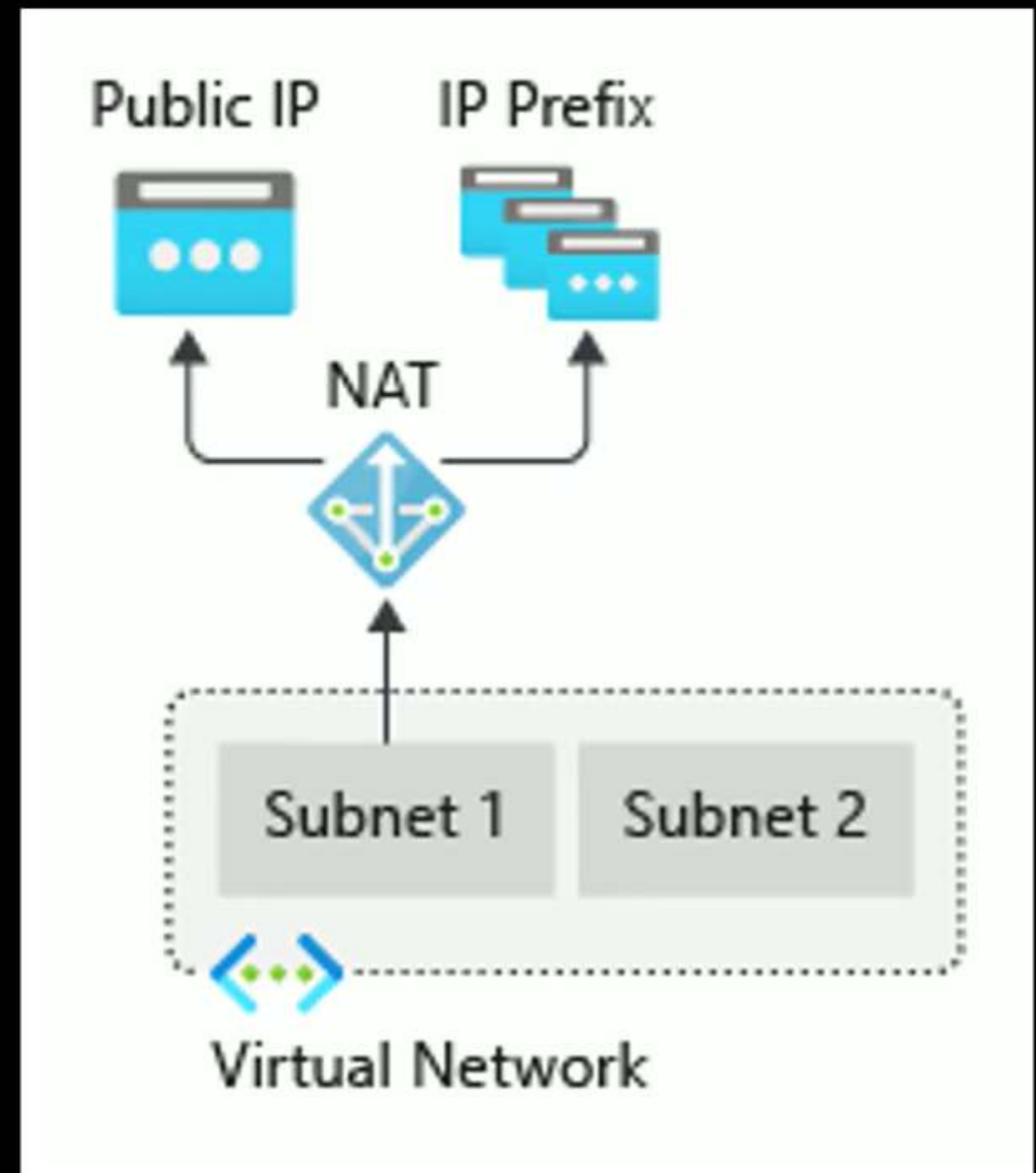# Azure NAT Gateway configuration

A Subnet can be attached only to a single NAT gateway.

Can't span multiple virtual networks.

Can use up to 16 IP addresses.

Multiple subnets within the same VNET can either use

different NAT gateways or the same NAT gateway.

Supports IP Prefix.
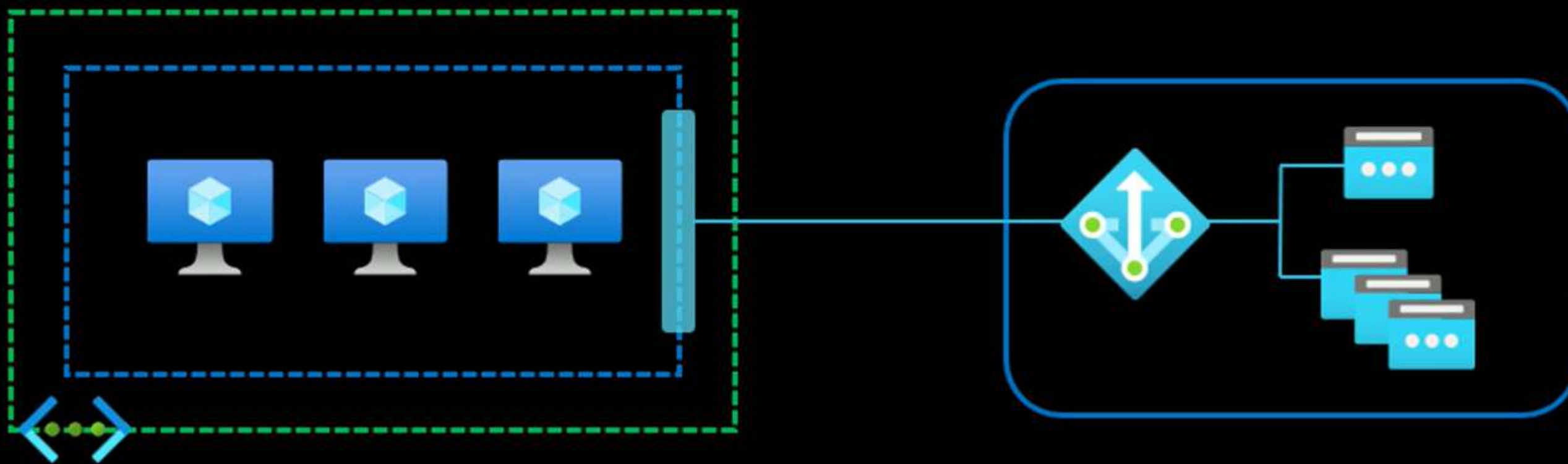
Azure NAT Gateway pricing

	Rate
Resource Hours	**$0.045** per hour $32 per month
Data Processed	**$0.045** per GB $45 per TB

azure.microsoft.com/en-us/pricing/details/azure-nat-gateway
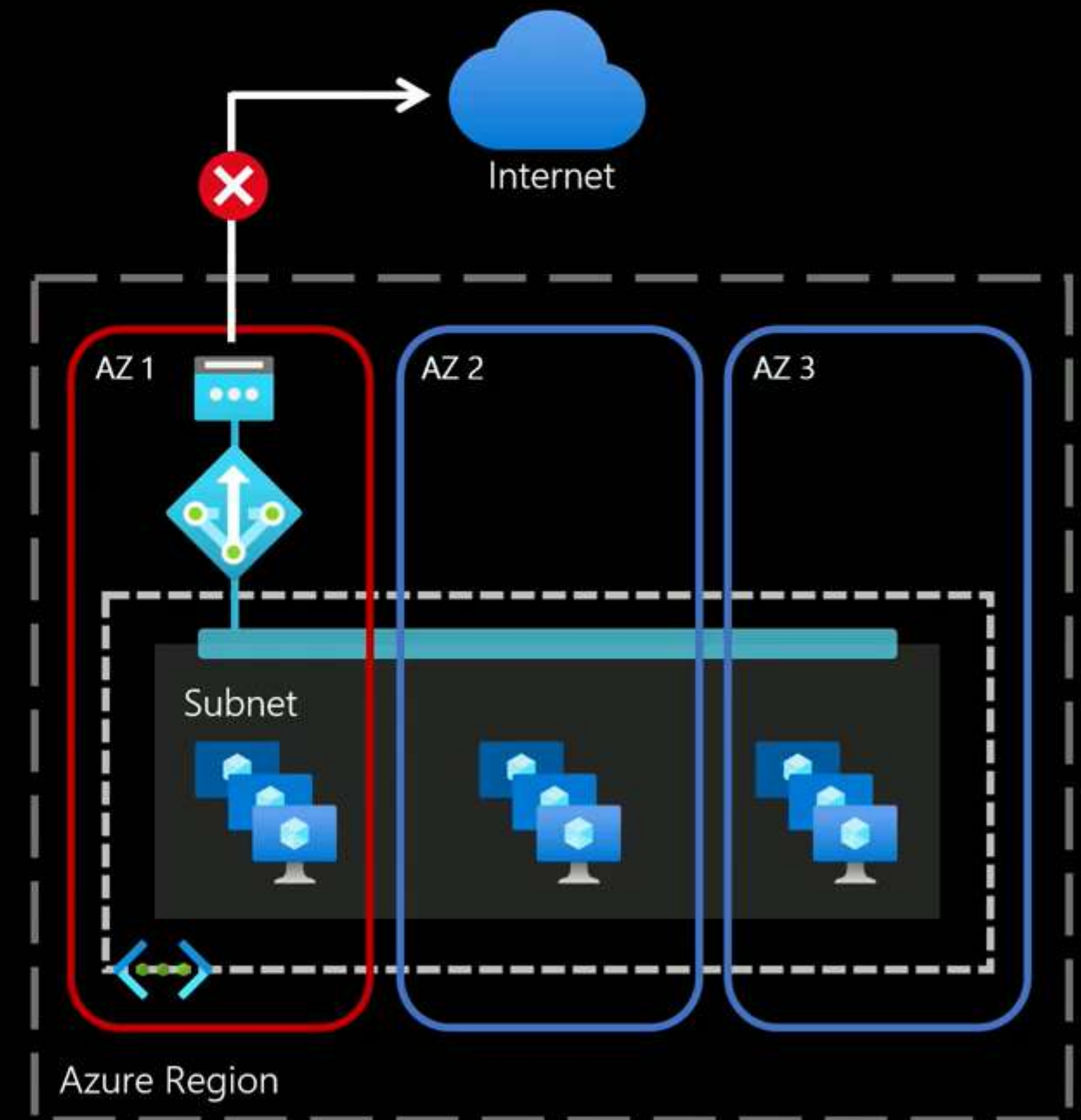
Azure NAT Gateway creation

Azure NAT Gateway availability zone

Is **zonal resource**, can be created in a specific availability zone or placed in 'no zone'.

Doesn't support multiple availability zones. (could change in the future)

Zone 1 outage causes **loss of outbound connectivity** across all availability zones.
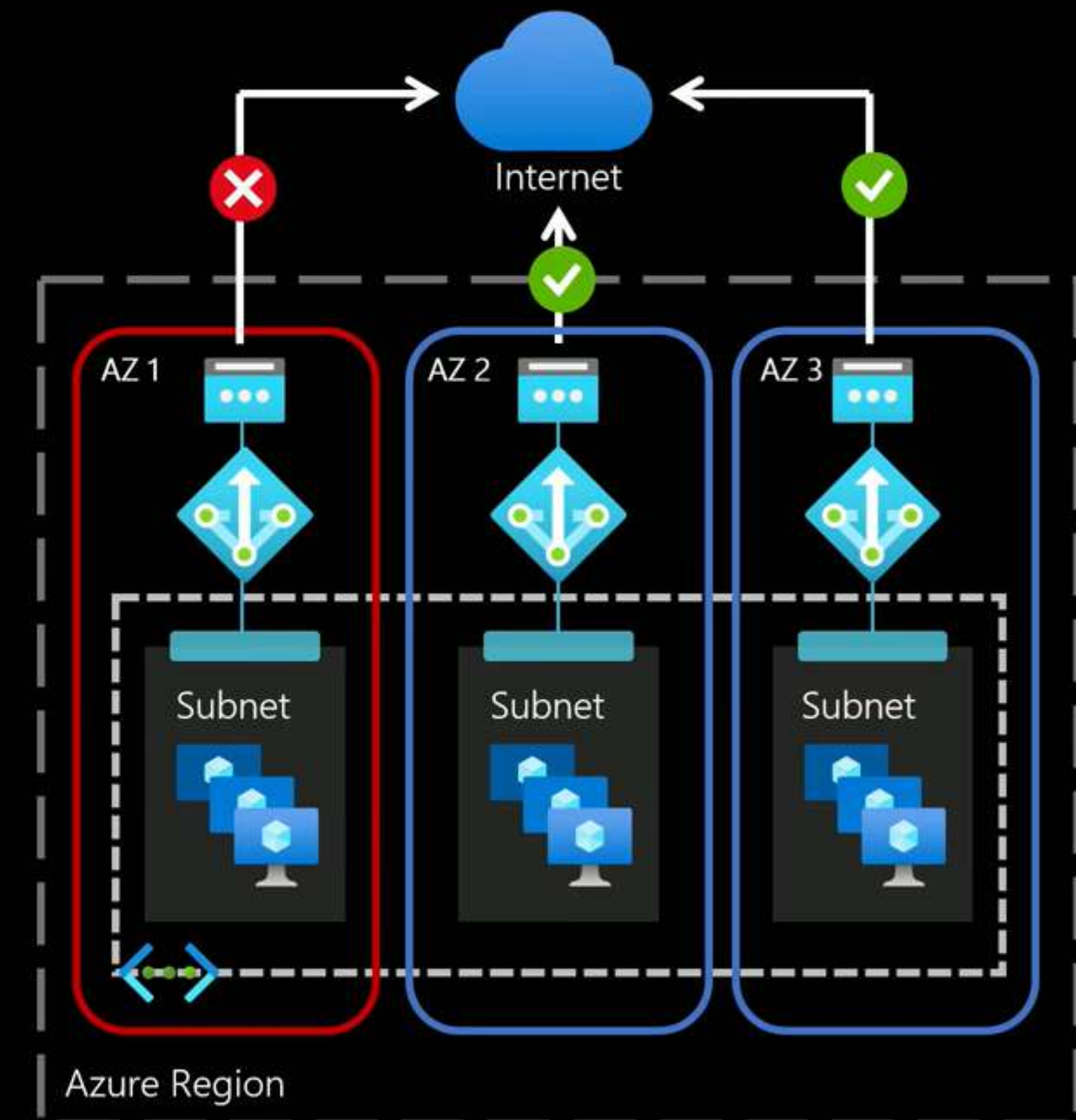
NAT Gateway zonal deployment

Zonal-stack deployment of NAT gateway resources.

NAT Gateway instance is **deployed in each zone**.

Zone 1 outage causes loss of outbound connectivity for **zone 1 ONLY**.

NAT Gateway & Load Balancer together

NAT Gateway for outbound traffic,

and Load Balancer for inbound.

Replaces internet destination for subnet.

No UDRs on route table needed.

Takes precedence over other outbound

options like Load balancer and instance-level

Public IPs.

Subnet 1

Backend Pool

IL PIPs are configured directly to VMs

Load balancer is configured to a backend pool of multiple VMs

Subnet 2

Configured to 1 or more subnets within same virtual network

Overrides other outbound methods present

Allows for inbound and outbound on same subnet