Microsoft Azure Fundamentals
Training Bootcamp

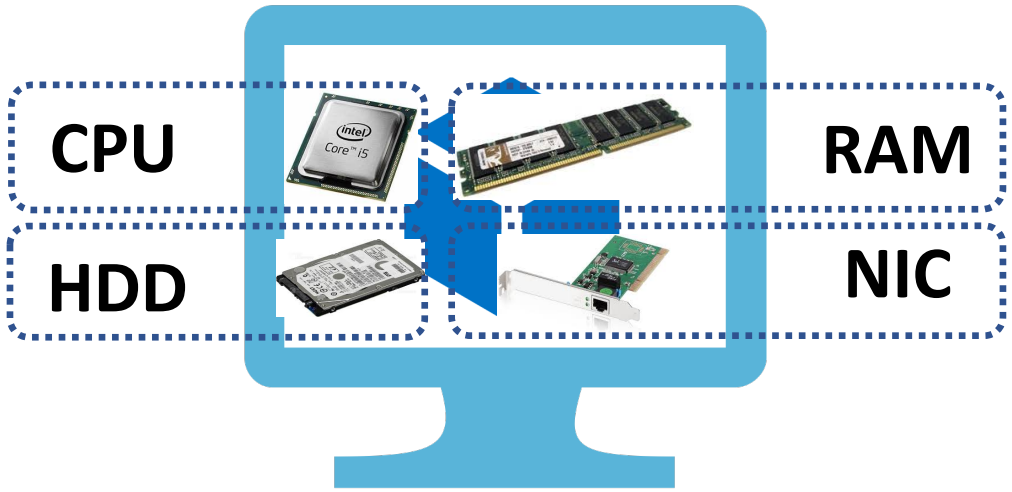
Module Completion & Exam Hints

Microsoft Azure Fundamentals
Training Bootcamp

Virtual Machines (VM) Introduction

Azure Virtual Machines (VMs)

- Virtual machines, or VMs, are software emulations of physical computers -> Virtual Servers running in Azure Cloud



VM Family Sizes and Storage Options

- Azure VMs are available in different sizes (families), being able to serve different use cases :
  - General Purpose
  - Memory Optimized
  - GPU
  - Compute Optimized
  - Storage Optimized
  - High Performance Compute

- Storage for VM (IaaS):
  - Standard HDD
  - Premium SSD
  - Standard SSD
  - Ultra Disk

Microsoft Azure Fundamentals
Training Bootcamp

Azure Networking and High Availability

VMs Networking Basics – Azure vNETs

- Azure Virtual Networks (vNETs) are the fundamental building block for your private network in Azure (your own DC in the Azure cloud)
- vNETs enable VMs to communicate between them, over the internet and with your on-prem DC
- Think of your traditional IP network that you need to setup in your organization or your DC; vNETs are your dedicated network, running in Azure

VMs Availability Options in Azure Cloud

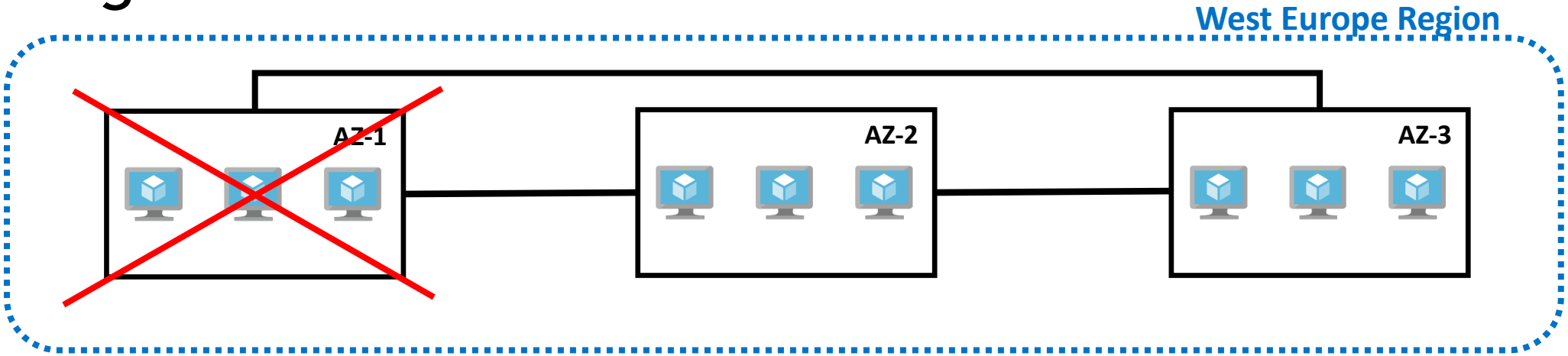
- With Azure you can easily achieve High Availability (HA), Scalability and Redundancy with your Apps

- Available Azure technologies and capabilities:
  - High Availability
  - Availability Sets
  - Virtual Machine Scale Sets

VMs High Availability – Availability Zones

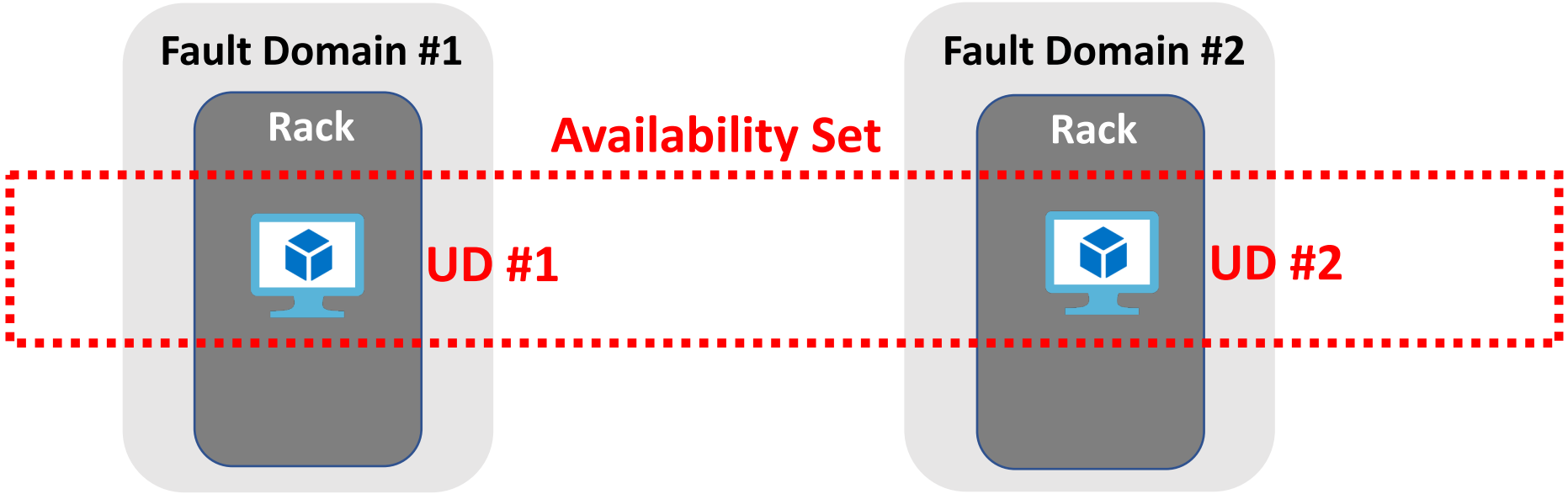
- When deploying highly available, mission-critical apps, it's a good idea to use Azure Availability Zones

- Availability Zones are physically separate datacenters within an Azure region, with independent power, network and cooling



VMs High Availability – Availability Sets

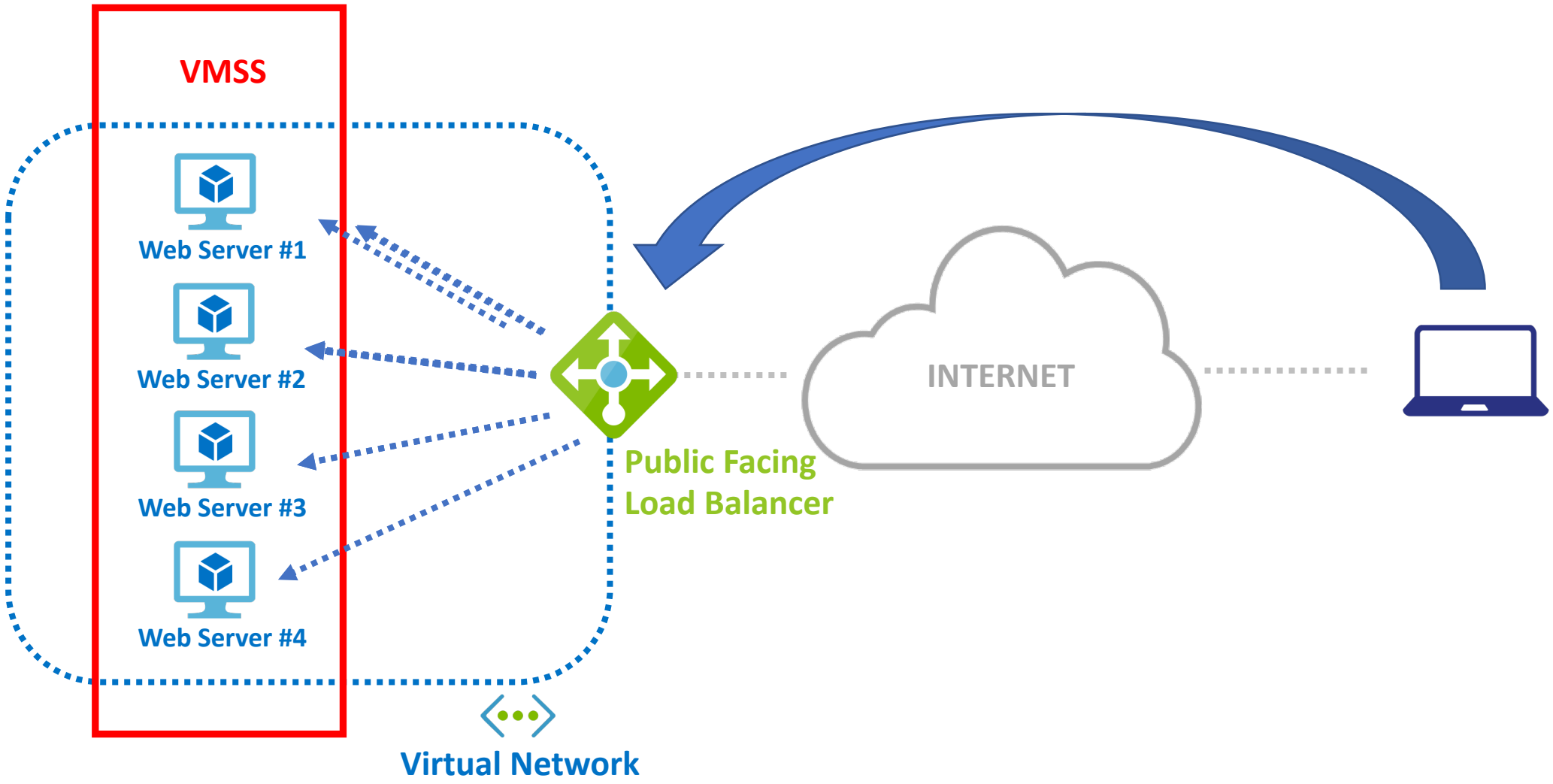
- An availability set is a logical grouping of two or more VMs within a DC; Azure will split your fleet of VMs on different racks of servers, on different *fault domains* and *update domains*



Virtual Machine Scale Sets (VMSS)

- Azure virtual machine scale sets let you create and manage a group of identical load balanced VMs
- The number of VM instances can automatically increase or decrease in response to traffic demand or a defined schedule
- In order to achieve high availability, a minimum of 2 VMs should be placed in a VMSS; 99,95% Azure SLA

Virtual Machine Scale Sets (VMSS)



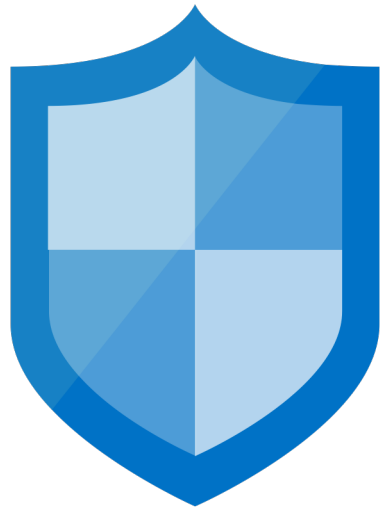
Microsoft Azure Fundamentals
Training Bootcamp

Azure NSGs and ASGs

Network Security Groups (NSGs) Overview

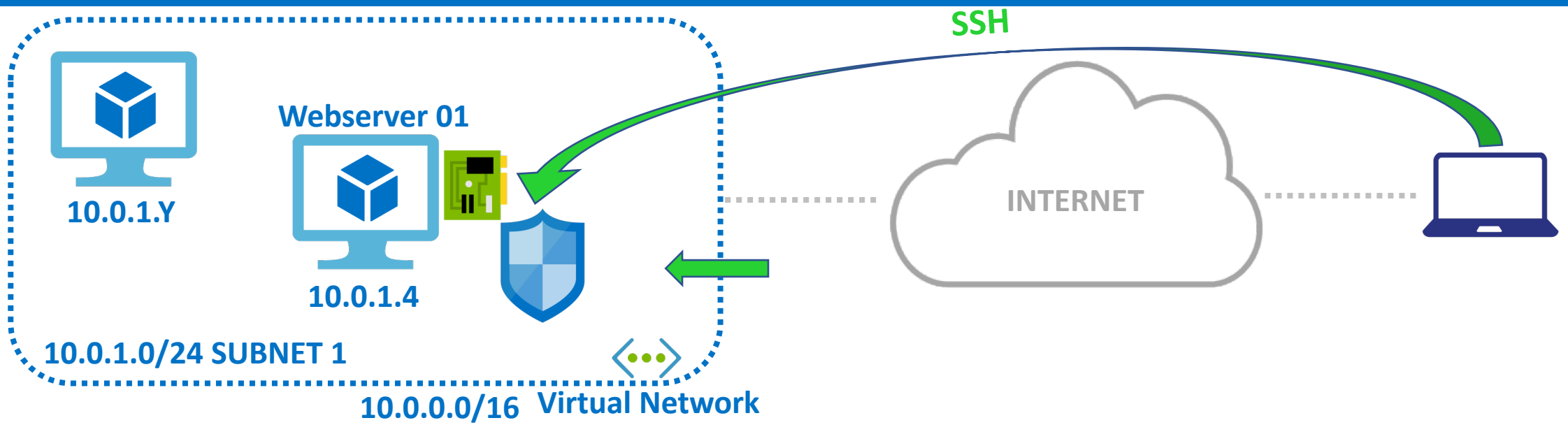
- Azure Network Security Groups act as a virtual firewall for your VMs to control inbound (to VM) and outbound traffic (from VM)

- NSGs enforce security at the subnet or NIC card level and different VMs can have different NSGs applied



- In a NSG you add rules that control inbound traffic to instances and separate rules that control outbound traffic

NSGs – Inbound Security Rules



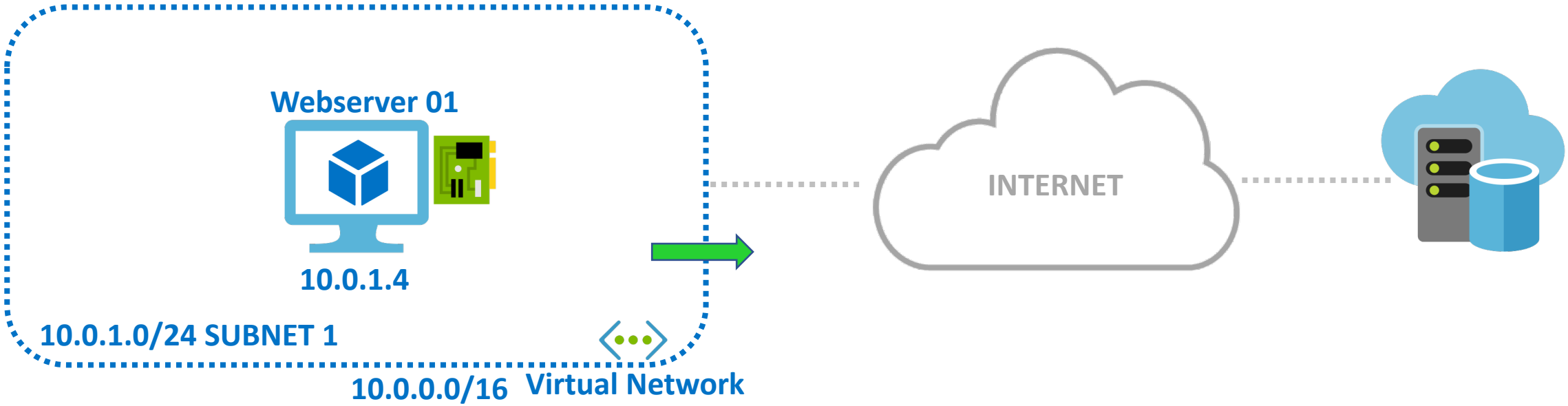
Inbound port rules | Outbound port rules | Application security groups | Load balancing

Network security group Webserver01-nsg (attached to network interface: webserver01228)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

NSGs – Outbound Security Rules



Inbound port rules | Outbound port rules | Application security groups | Load balancing

Network security group Webserver01-nsg (attached to network interface: webserver01228)
Impacts 0 subnets, 1 network interfaces

Add outbound port rule

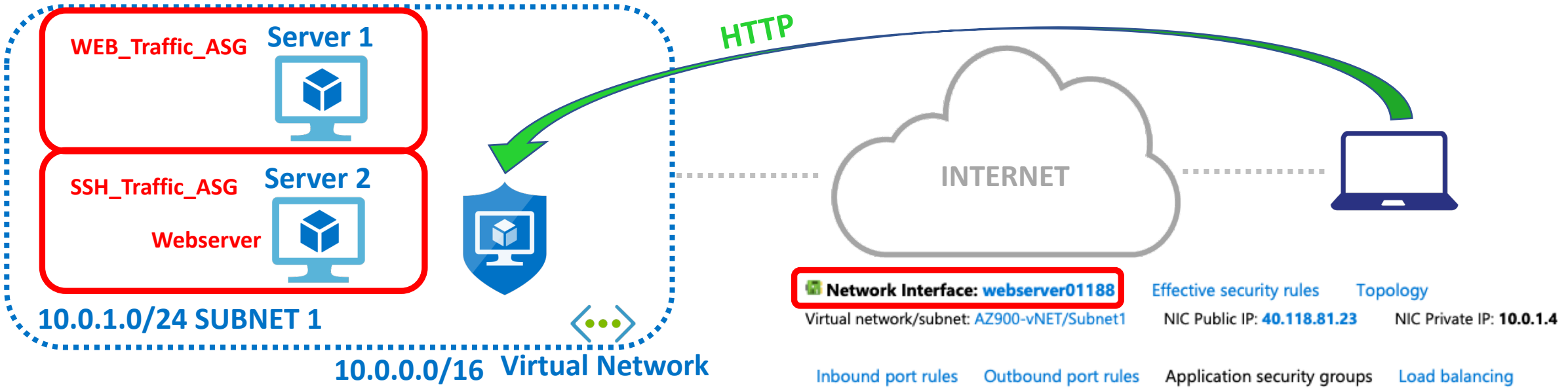
Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Application Security Groups (ASGs) Overview

- Application Security Groups allow you to group virtual machines and define network security policies based on those groups

- In an ASG you add rules that control inbound traffic to instances and separate rules that control outbound traffic

ASGs – Security Rules



Network Interface: webserver01188 Effective security rules Topology

Virtual network/subnet: AZ900-vNET/Subnet1 NIC Public IP: **40.118.81.23** NIC Private IP: **10.0.1.4**

Inbound port rules | Outbound port rules | Application security groups | Load balancing

WEB_Traffic_ASG | Configure the application security groups

Inbound port rules | Outbound port rules | Application security groups | Load balancing

Network security group Webserver01-nsg (attached to network interface: webserver01188)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_HTTP_80	80	Any	Any	WEB_Traffic_ASG	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Microsoft Azure Fundamentals
Training Bootcamp

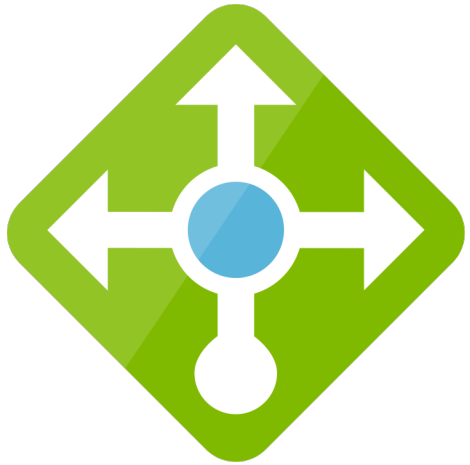
Azure Load Balancers

Load Balancing Overview

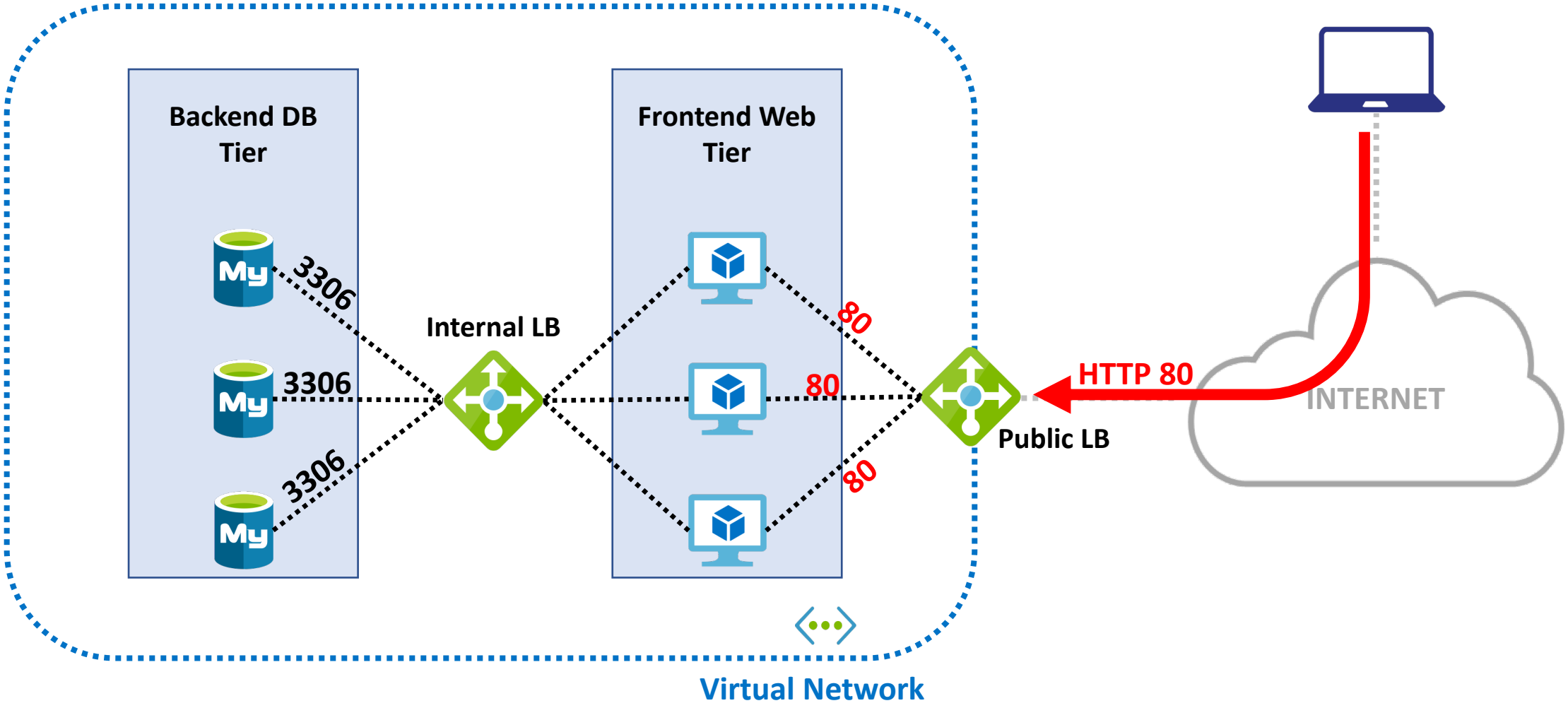
- The LB is the single point of contact for its clients; distributes incoming traffic to backend pool of VMs

- Two types of LBs are available:
  - Internal LB and Public LB

- Load Balancer resources:
  - Backend Pool
  - Health Probe
  - Load Balancing Rule



Azure Load Balancers: Public and Internal



Azure Virtual Machines - Quiz

Microsoft Azure Fundamentals

Microsoft Azure Fundamentals
Training Bootcamp

Thank you