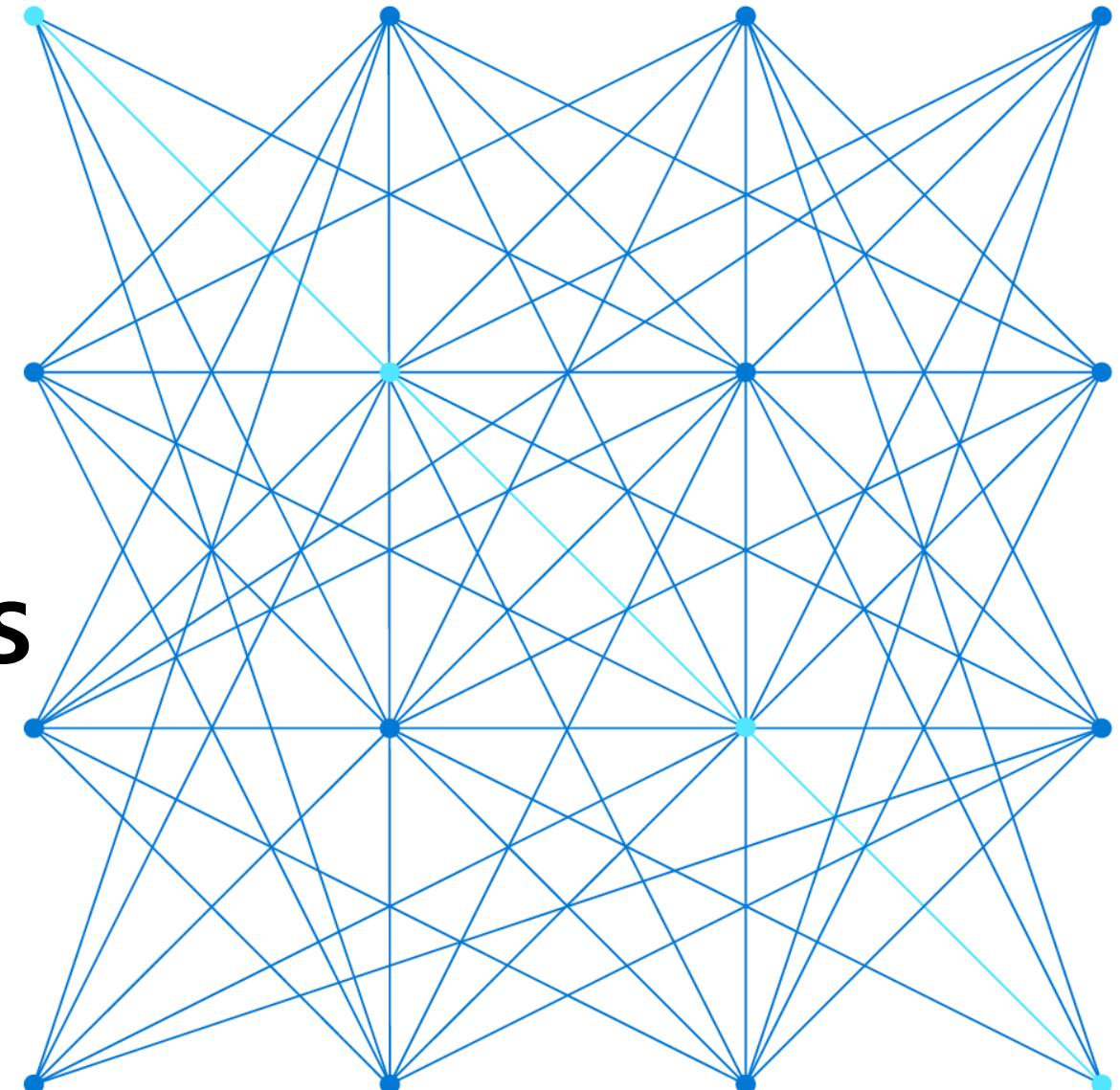


AZ-500

Microsoft Azure Security Technologies



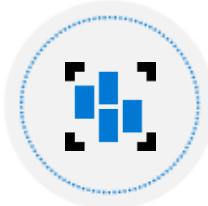
AZ-500 Agenda



Learning Path 1 Identity and Access



Learning Path 2 Implement Platform Protection

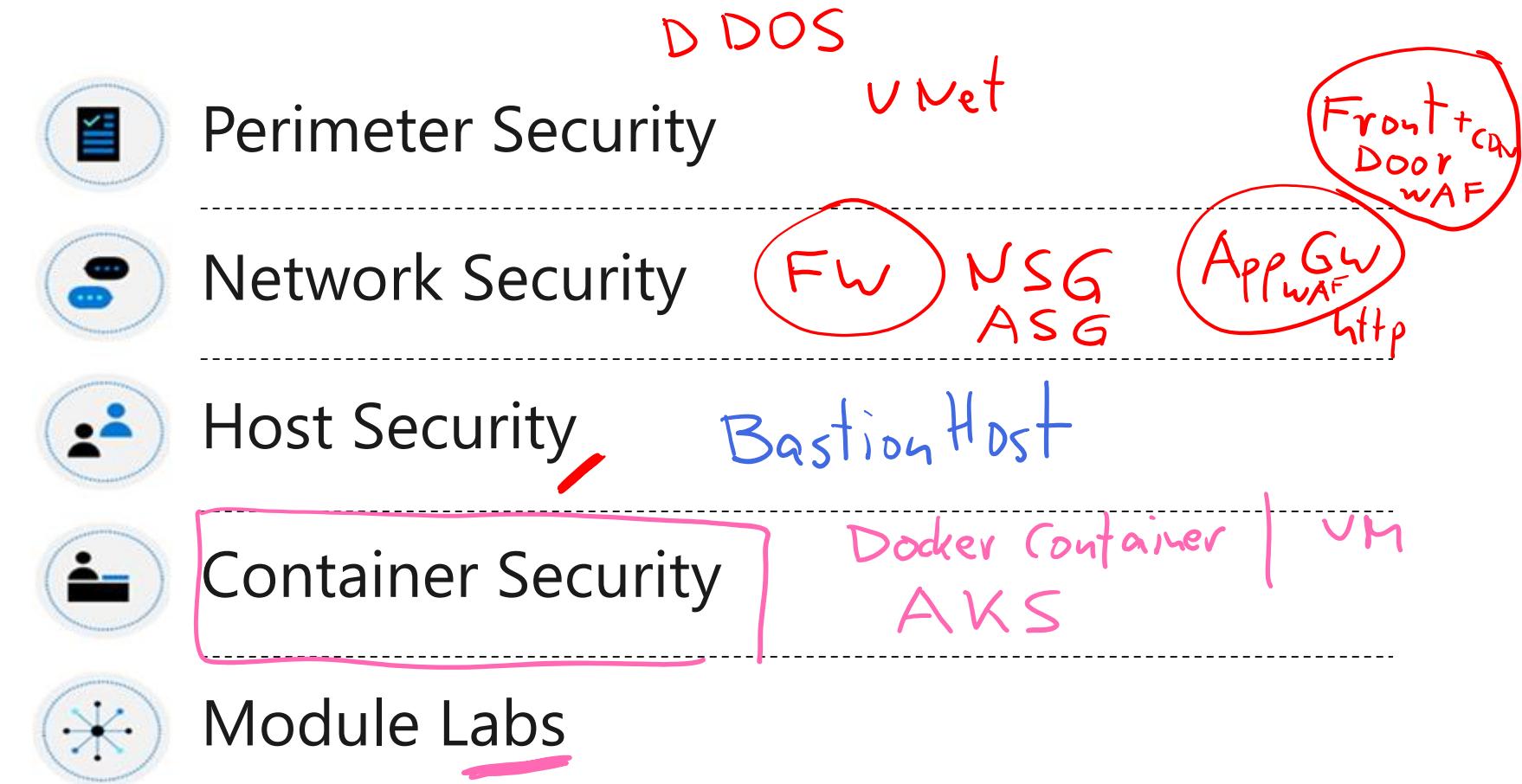


Learning Path 3 Data and Application Security



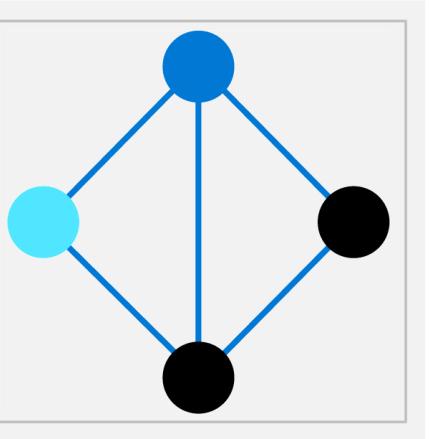
Learning Path 4 Security Operations

Learning Path: Implement Platform Protection



Perimeter Security

= DMZ



Perimeter Security



Defense in Depth

Virtual Network Security

Distributed Denial of Service (DDoS)

DDoS Implementation

Azure Firewall Features

Azure Firewall Implementation

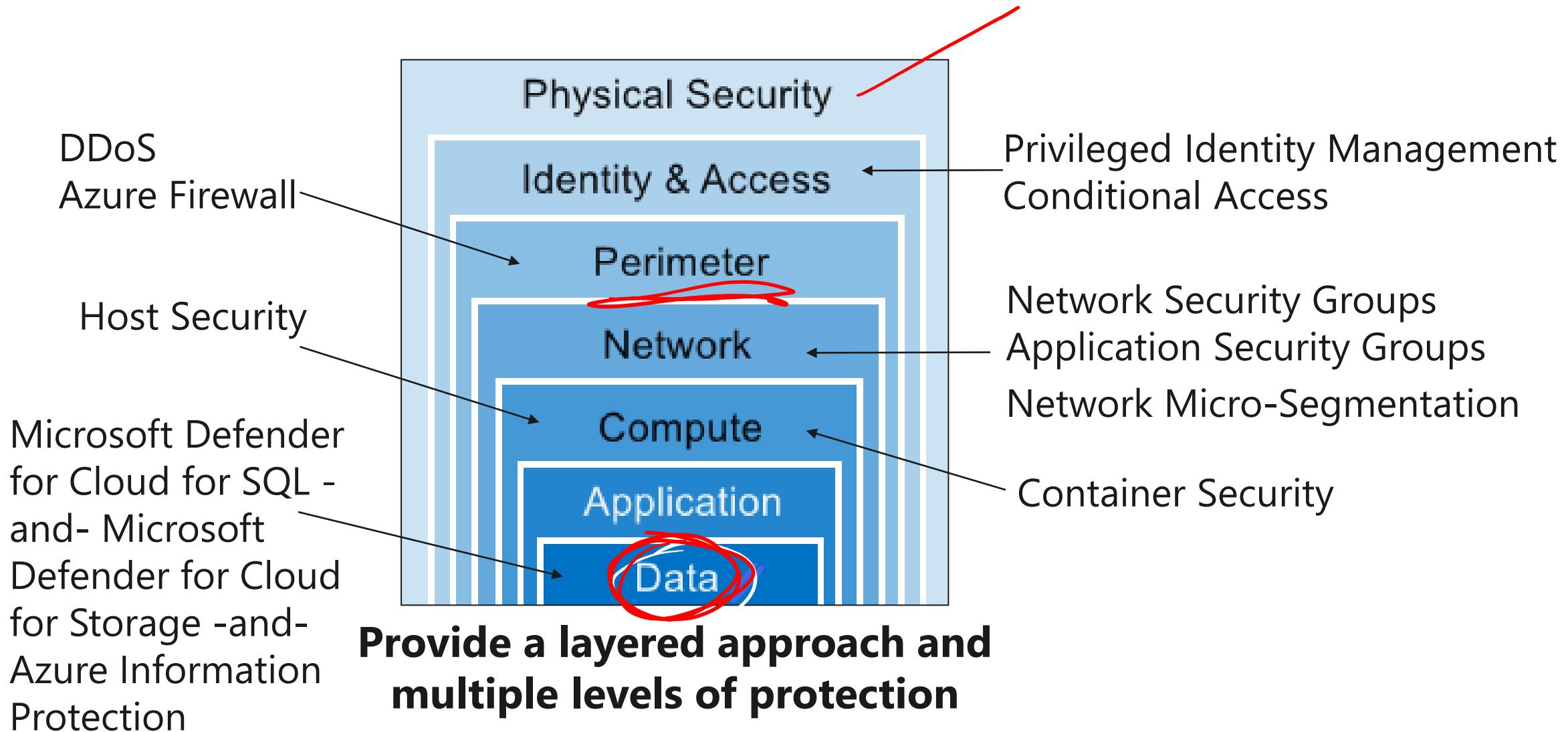
VPN Forced Tunneling

UDRs and NVAs

User Defined
Route

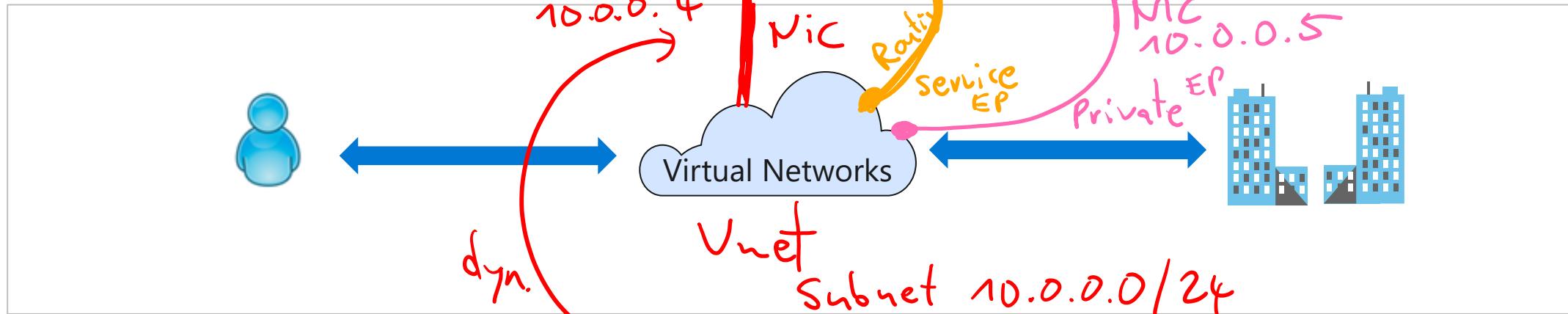
Network Virt Applianc

Defense in Depth



2001:cafe ::/64

Virtual Network Security



- Dynamic and reserved public IP addresses
- Direct virtual machine access
- Load balancing
- DNS hosting
- Traffic management
- DDoS protection

- Bring your own network
- Segment with subnets
- Add network security groups
- Create user defined routes

- Point-to-site for dev/test
- VPN Gateways for site-to-site
- ExpressRoute for private connectivity

IPSec
:500
IKE

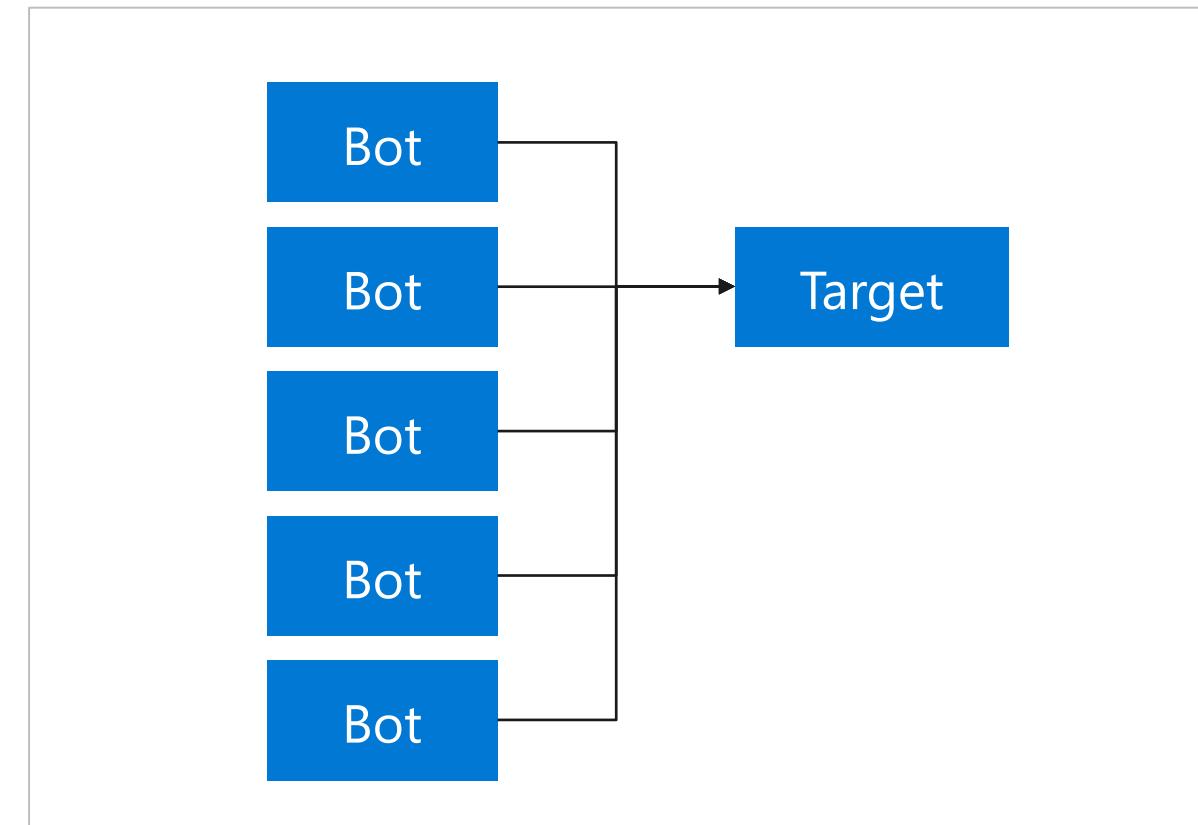
Distributed Denial of Service (DDoS)

The goal of a DoS (Denial of Service) attack is to prevent access to services or systems.

Botnets are collections of internet-connected systems that an individual controls and uses without their owners' knowledge

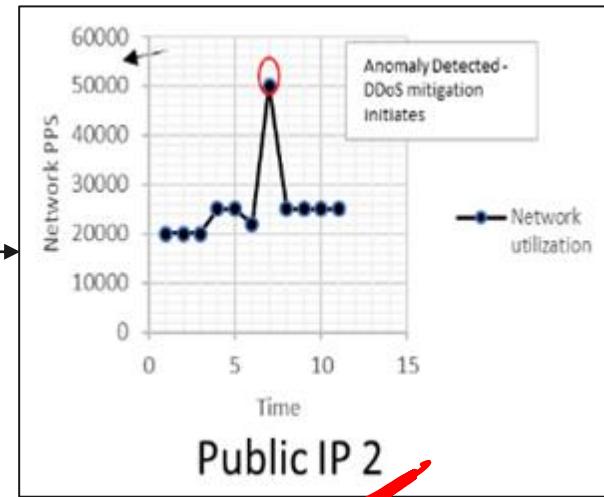
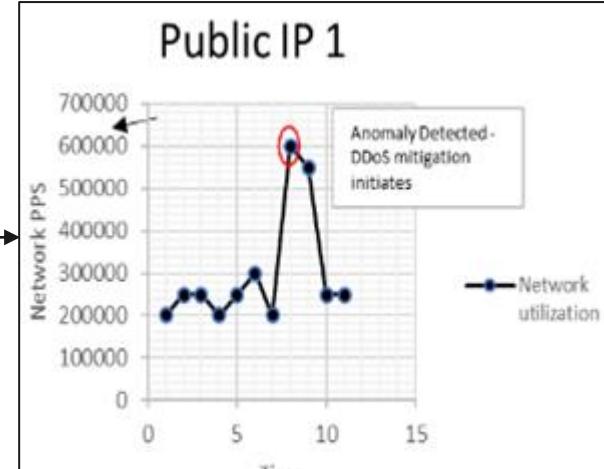
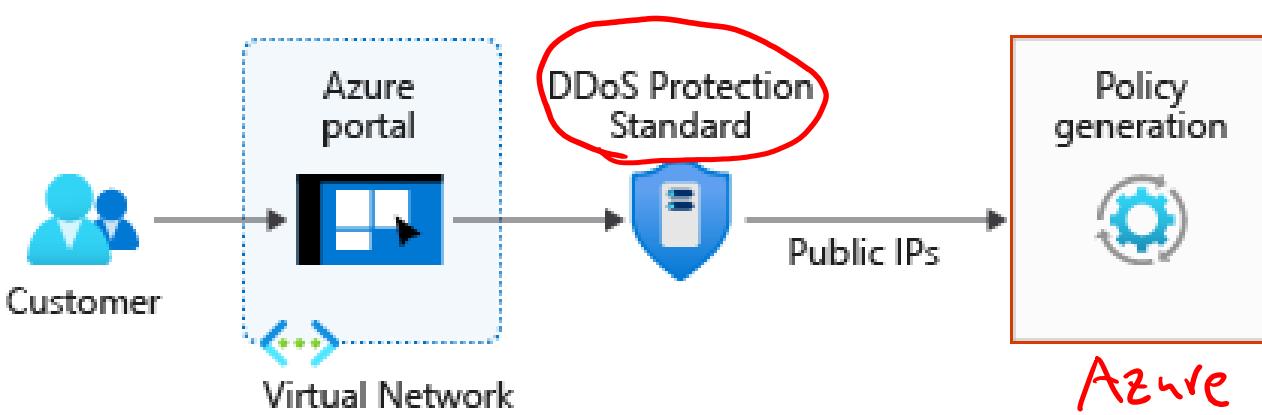
DDoS is a collection of attack types aimed at disrupting the availability of a target

DDoS involves many systems sending traffic to targets as part of a botnet



DDoS Implementation

Basic
• Free
• No Metrics



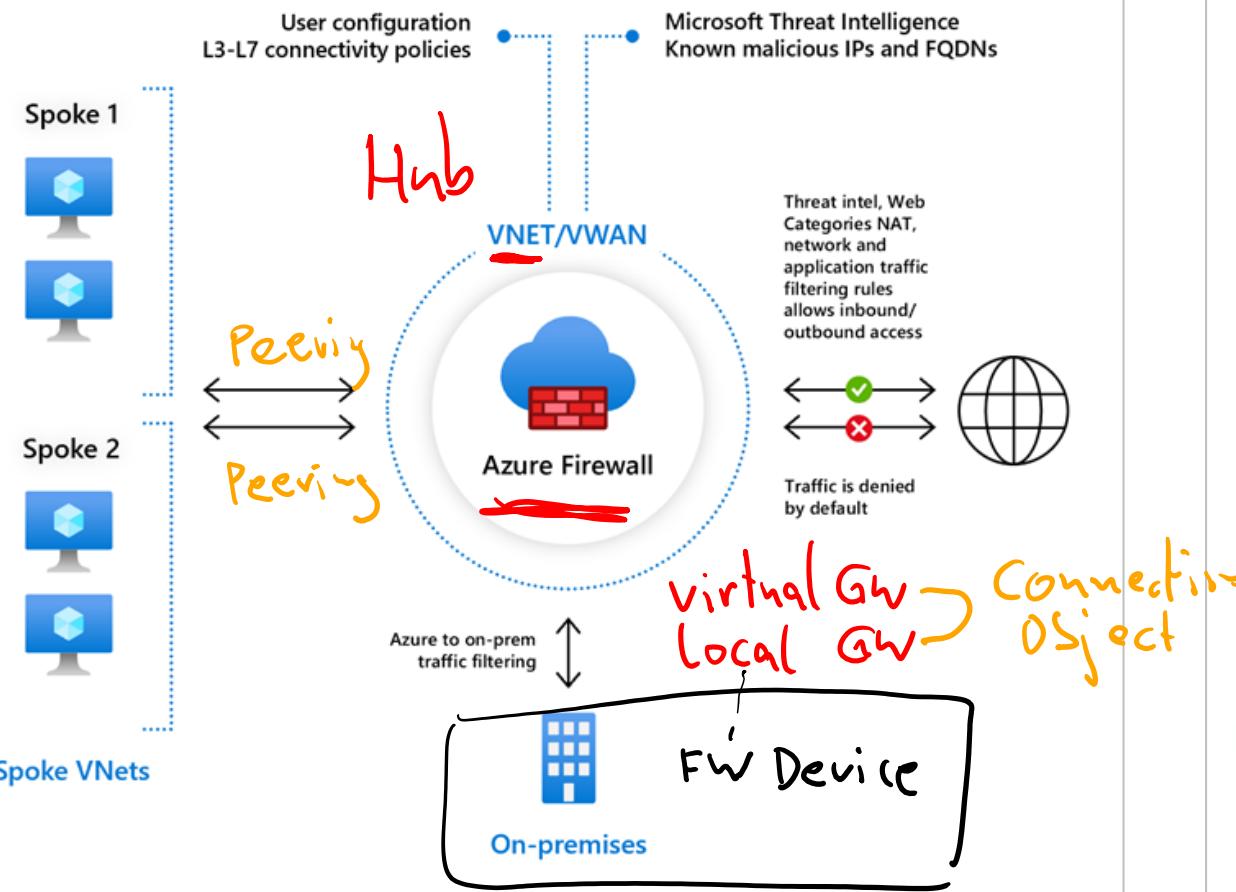
SKUs: DDoS IP Protection and DDoS Network Protection

Mitigates volumetric attacks, protocol attacks, and application layer attacks

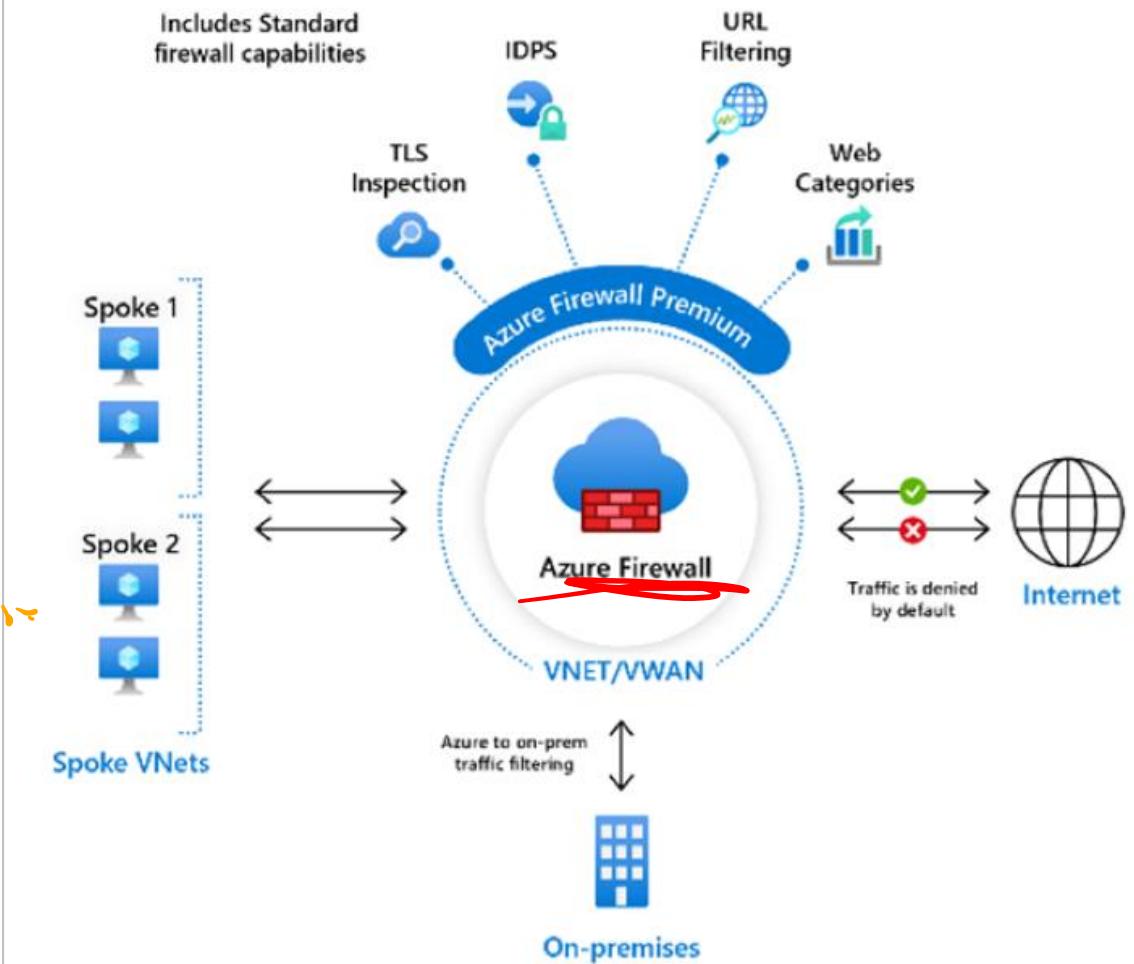
Checks for malformed packets and spoofing

Azure Firewall

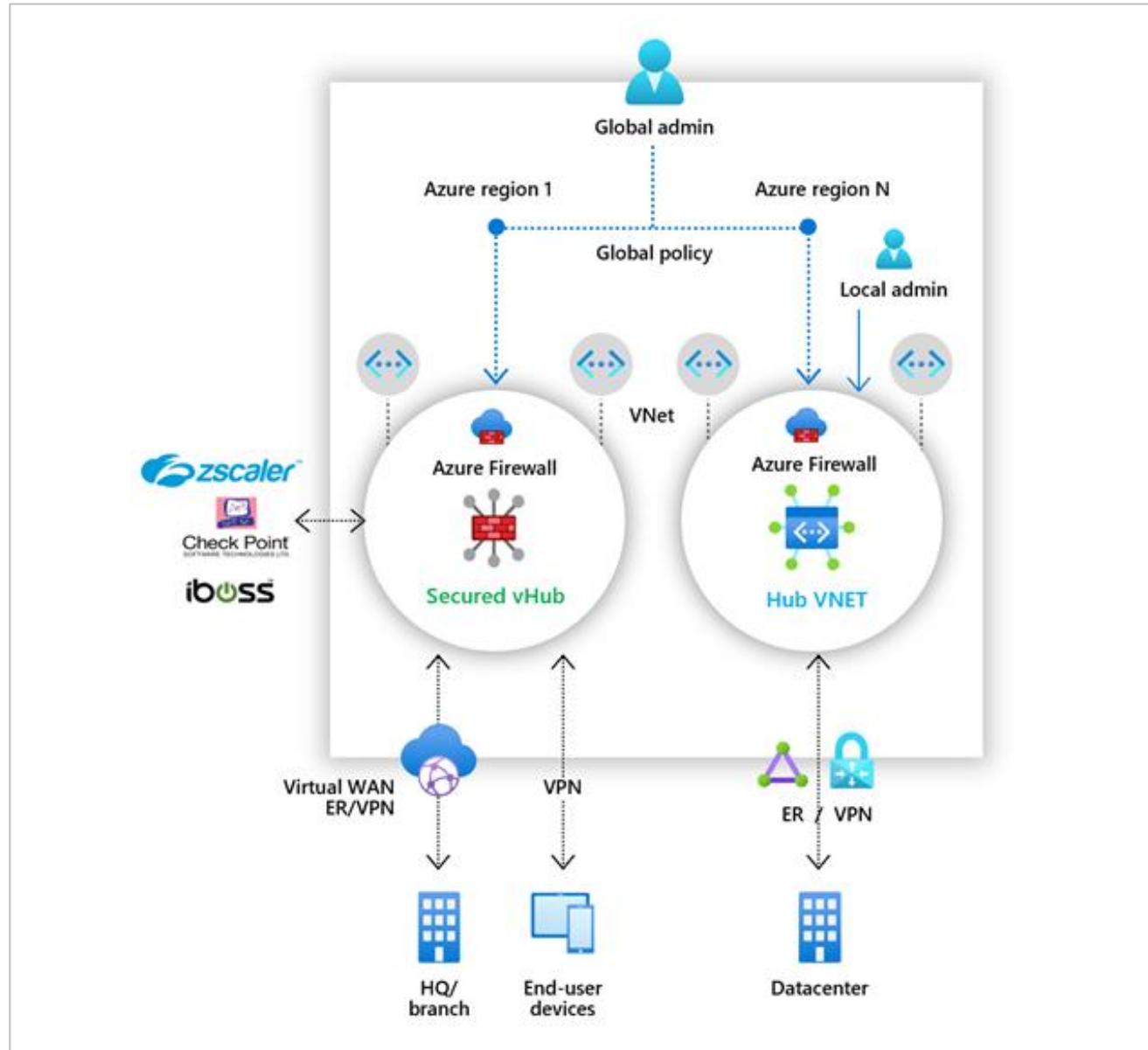
Azure Firewall Standard



Azure Firewall Premium



Azure Firewall Manager



Azure Firewall Implementation

2.

Application FQDN filtering rules

1.

Network traffic filtering rules

FQDN tags

Outbound SNAT

Inbound DNAT support

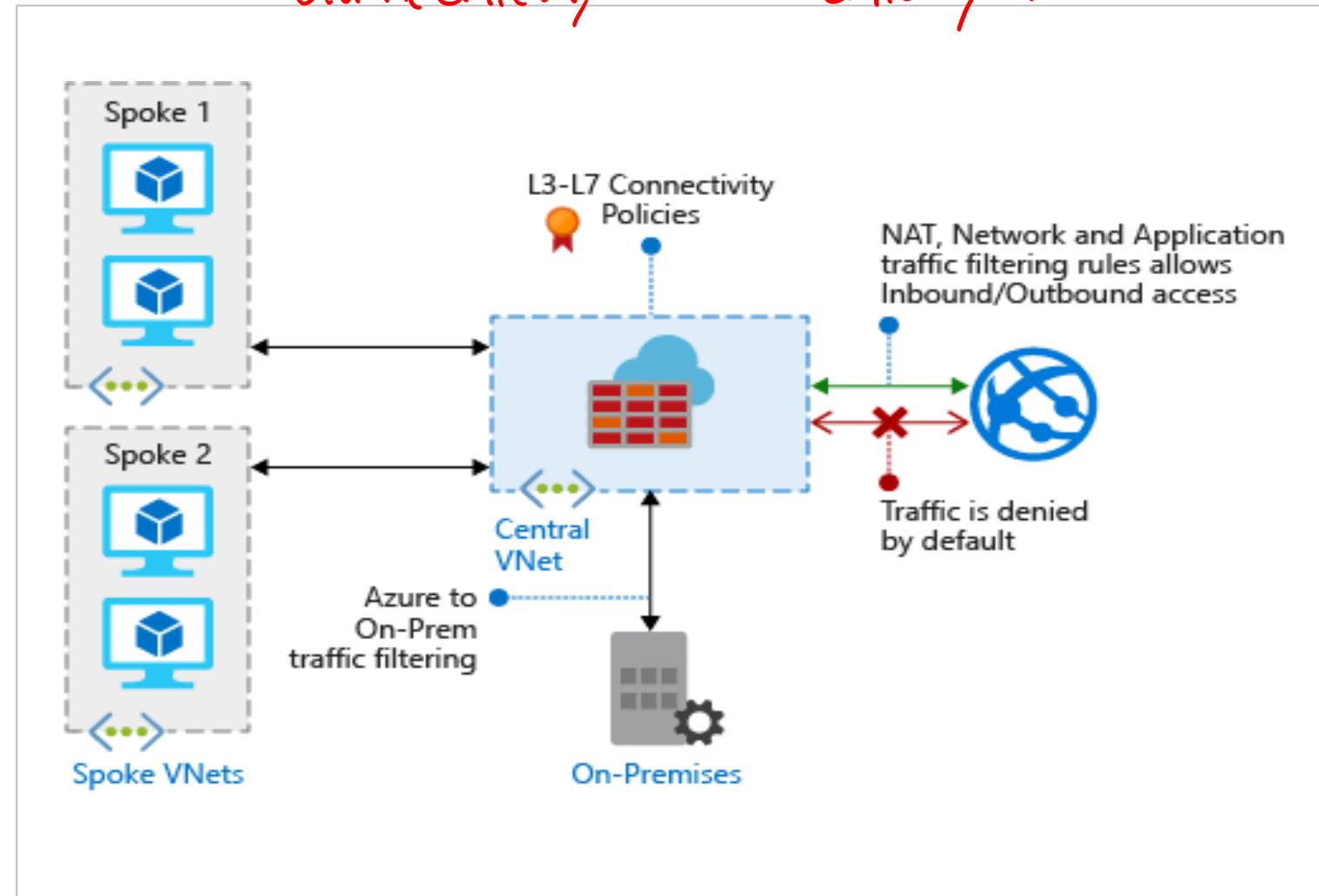
L3-L7 connectivity policies

Separate firewall subnet

Static public IP address

App GW
FW
Bastion
Virtual Gateway

(legal)
Azure Firewall Subnet
Azure Bastion Subnet
Gateway Subnet

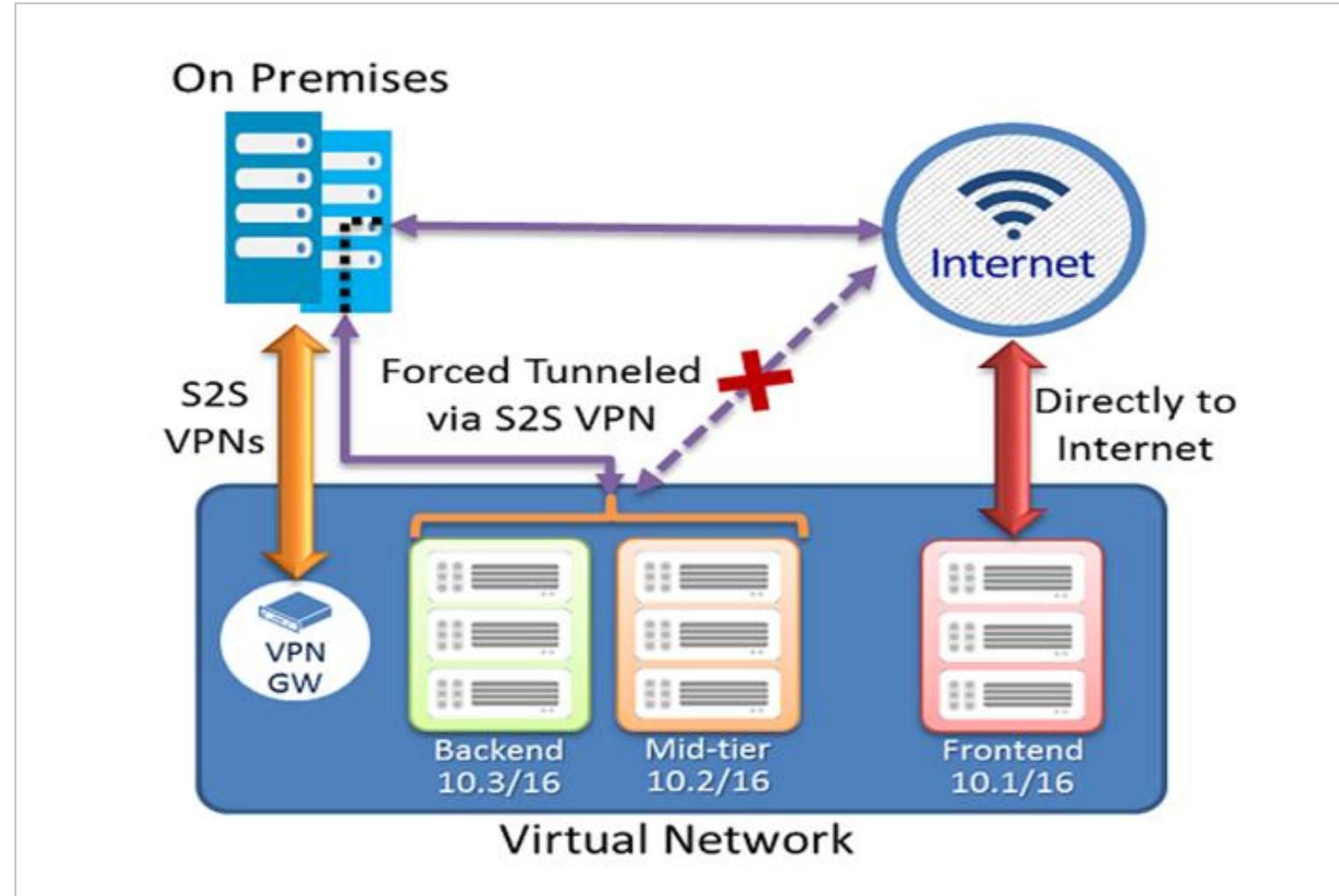


Forced tunnelling – Push all internet traffic for specific next hop (example – on-premises device).

VPN Forced Tunneling

Redirect internet-bound traffic back to the company's on-premises infrastructure for inspection and auditing

Internet-bound traffic from VMs always traverses from Azure network infrastructure directly out to the internet, without inspection or audit



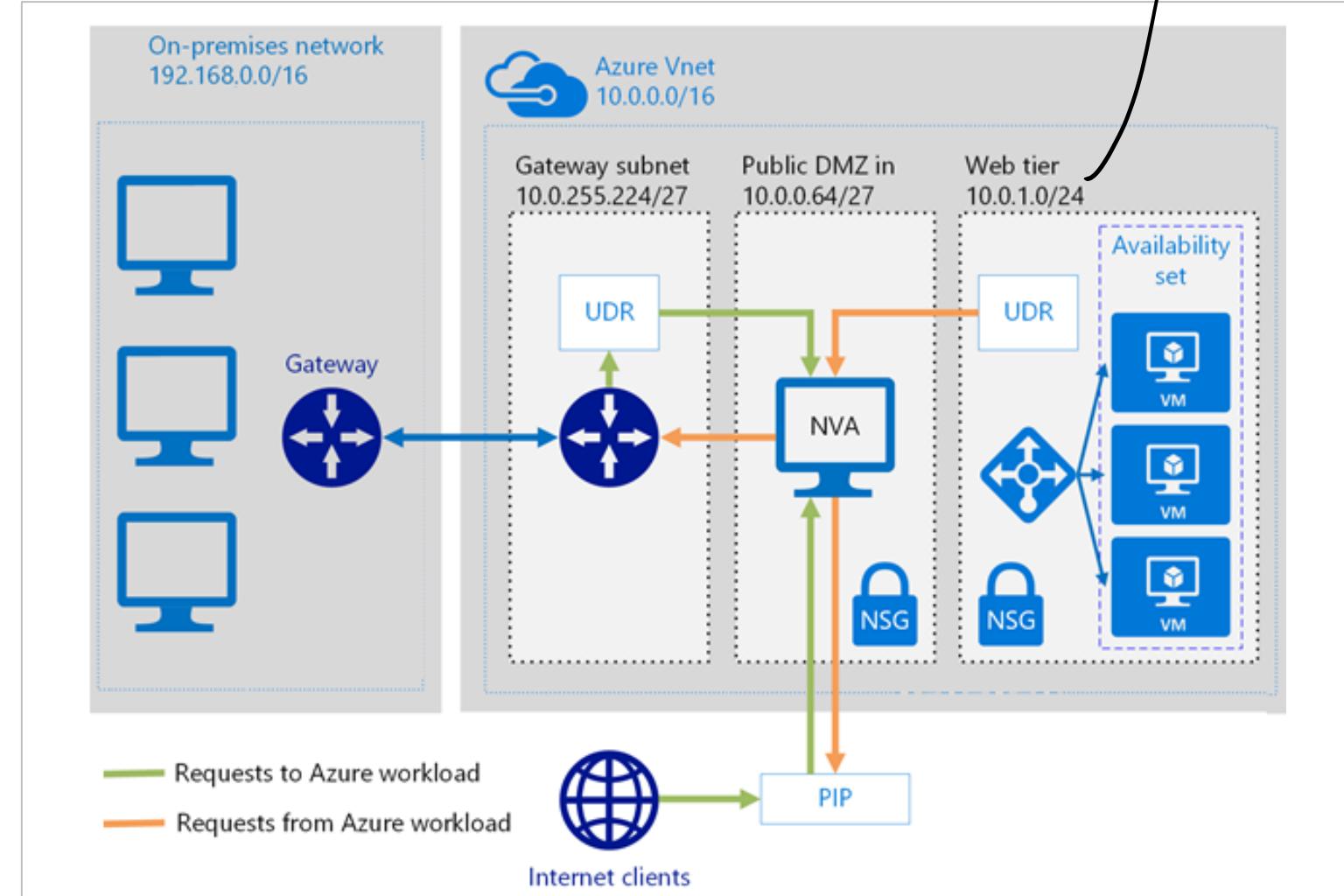
User Defined Routes and Network Virtual Appliances

UDR

route add ...

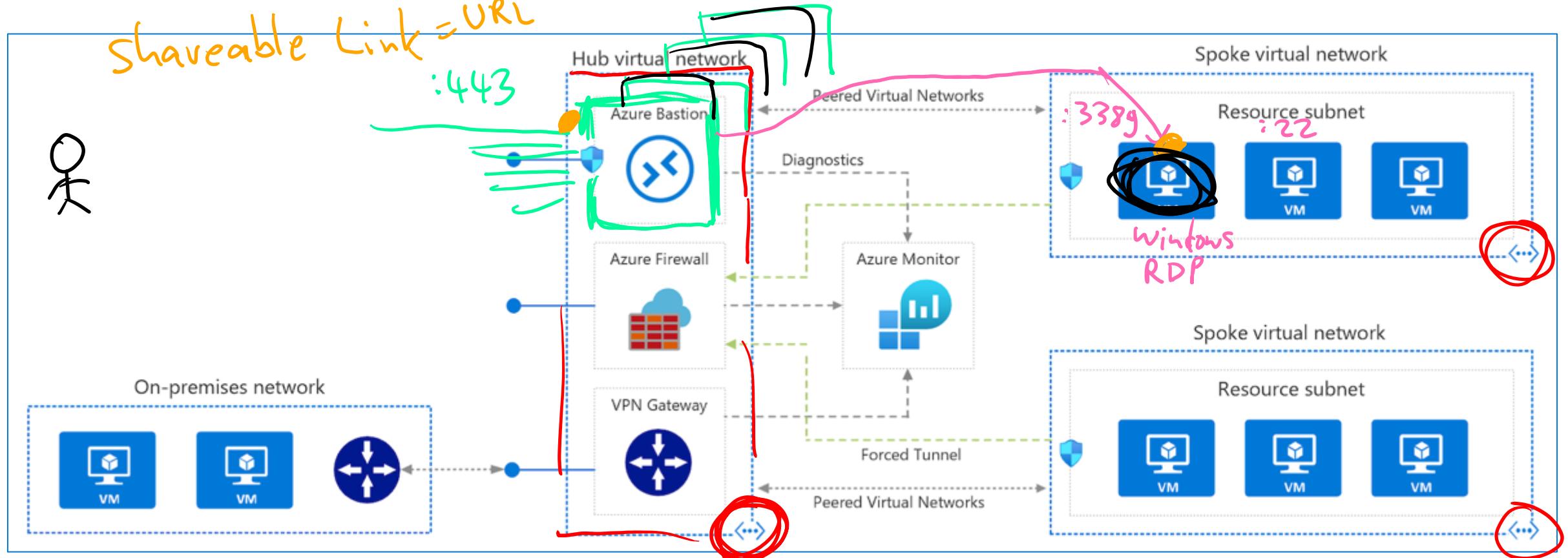
UDRs override the default system routes and are associated with a subnet

NVAs control the flow of network traffic from one network to another



Hub and Spoke topology with Azure

standard

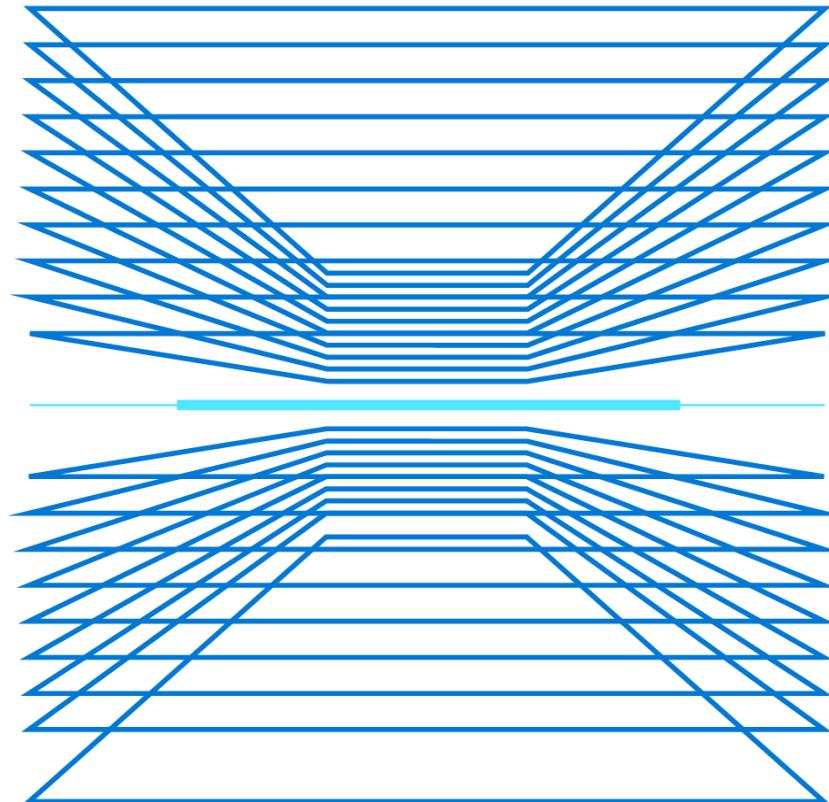


Hub is a virtual network in Azure that acts as a central point of connectivity to your on-premises network.

Spokes are virtual networks that peer with the hub and can be used to isolate workloads.

Demonstration: Perimeter Security

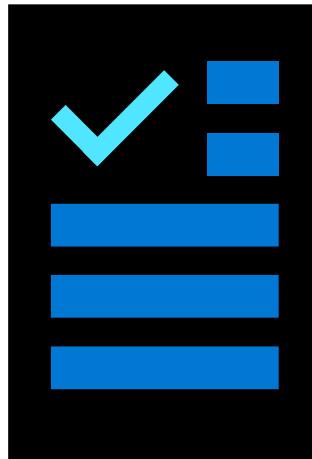
- VNet Peering
- Azure Firewall



Additional Study – Perimeter Security

Module Review Questions

Microsoft Learn Modules (docs.microsoft.com/Learn)



Fundamentals of network security

Fundamentals of computer networking

Manage and control traffic flow in your Azure deployment with routes (Exercise)

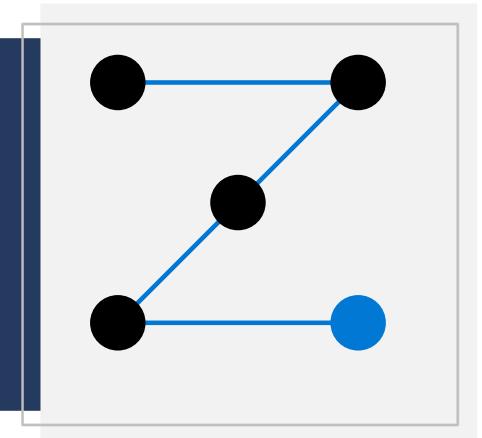
Distribute your services across Azure virtual networks and integrate them by using virtual network peering (Exercise)

Microsoft Azure Well-Architected Framework – Security

Configure the network for your virtual machines (Exercise)

Richard Feynman

Network Security



Network Security



Network Security Groups (NSG)



NSG Implementation



Application Security Groups

~~ASG~~



Service Endpoints



Private Endpoints



Azure Application Gateway



Web Application Firewall



Azure Front Door



ExpressRoute

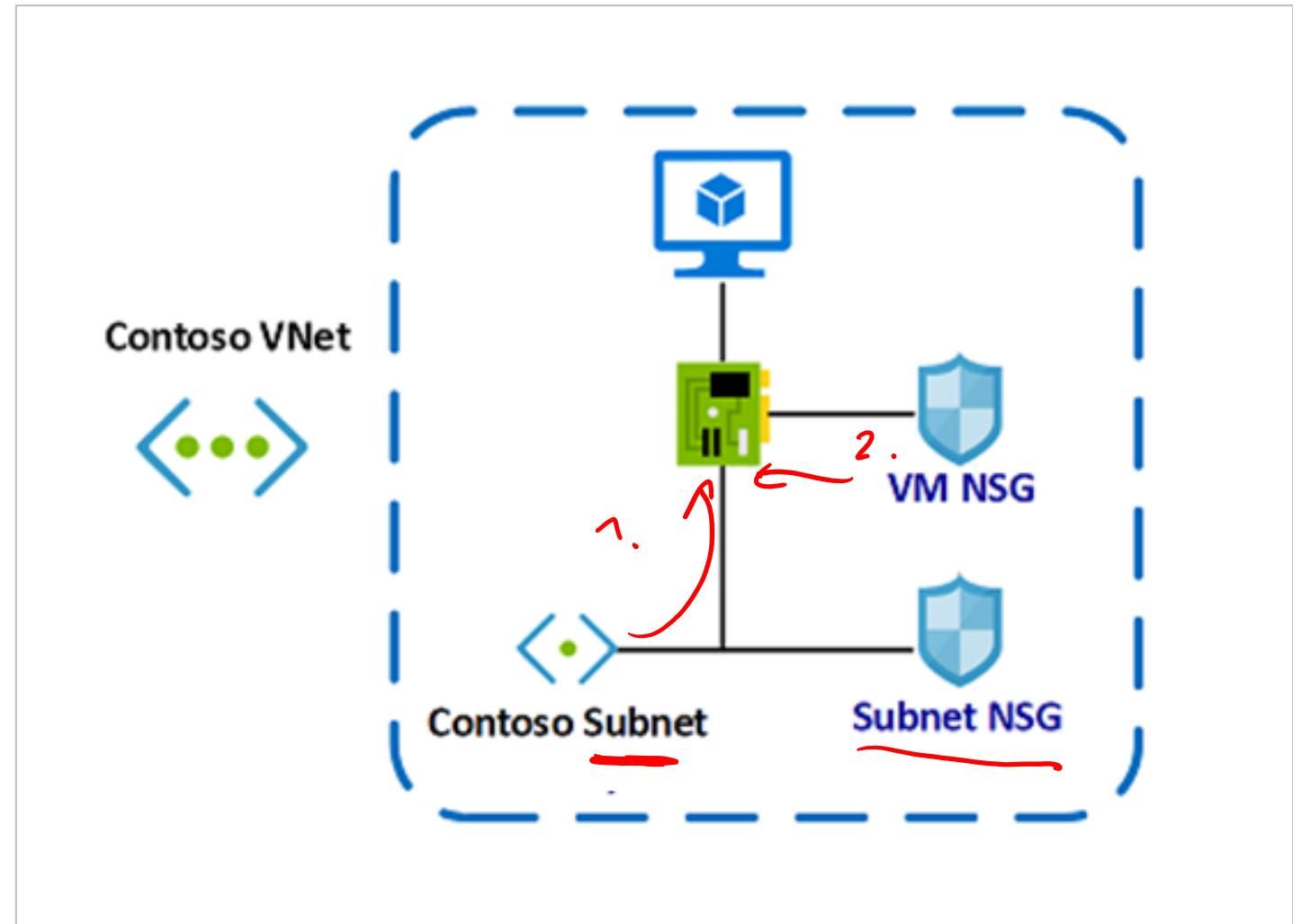
Network Security Groups (NSG)

Limit virtual network traffic

Can be associated to a subnet or a network interface

Uses security rules to allow or deny network traffic

Default inbound and outbound rules allow virtual network and load balancers – all other traffic denied



NSG Implementation

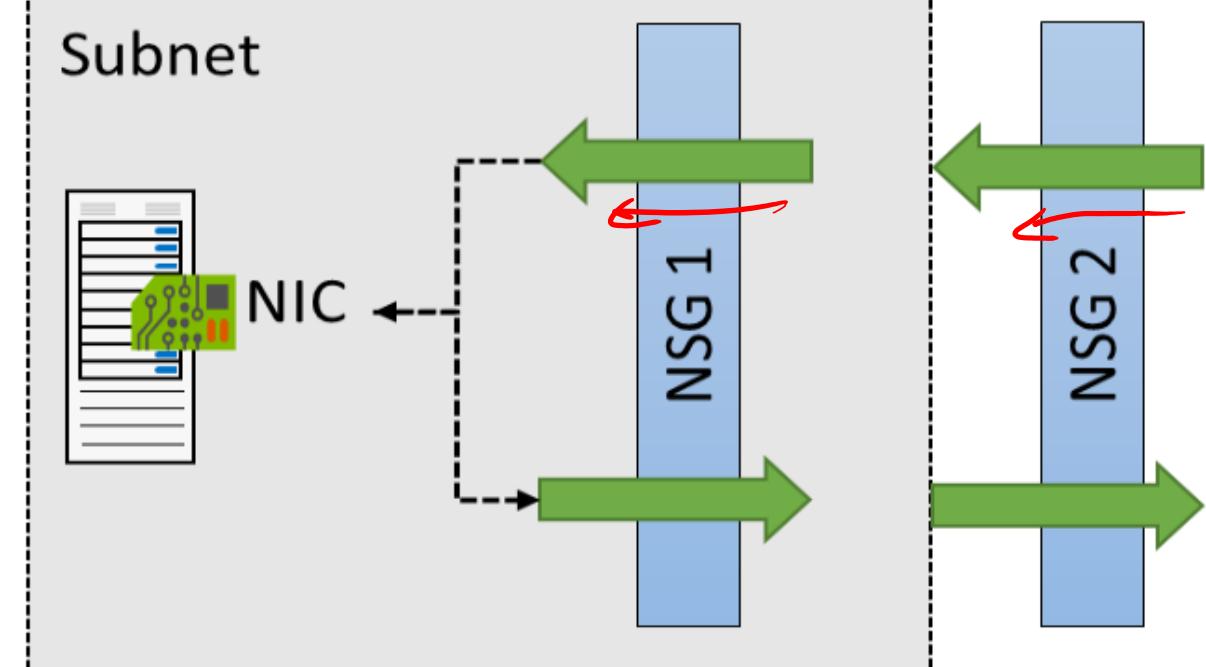
stateful

NSGs are evaluated independently for the subnet and NIC

An "allow" rule must exist at both levels for traffic to be admitted

You can add more rules – many preconfigured selections (SSH, RDP, FTP...)

Troubleshoot with the Effective Security Rules link



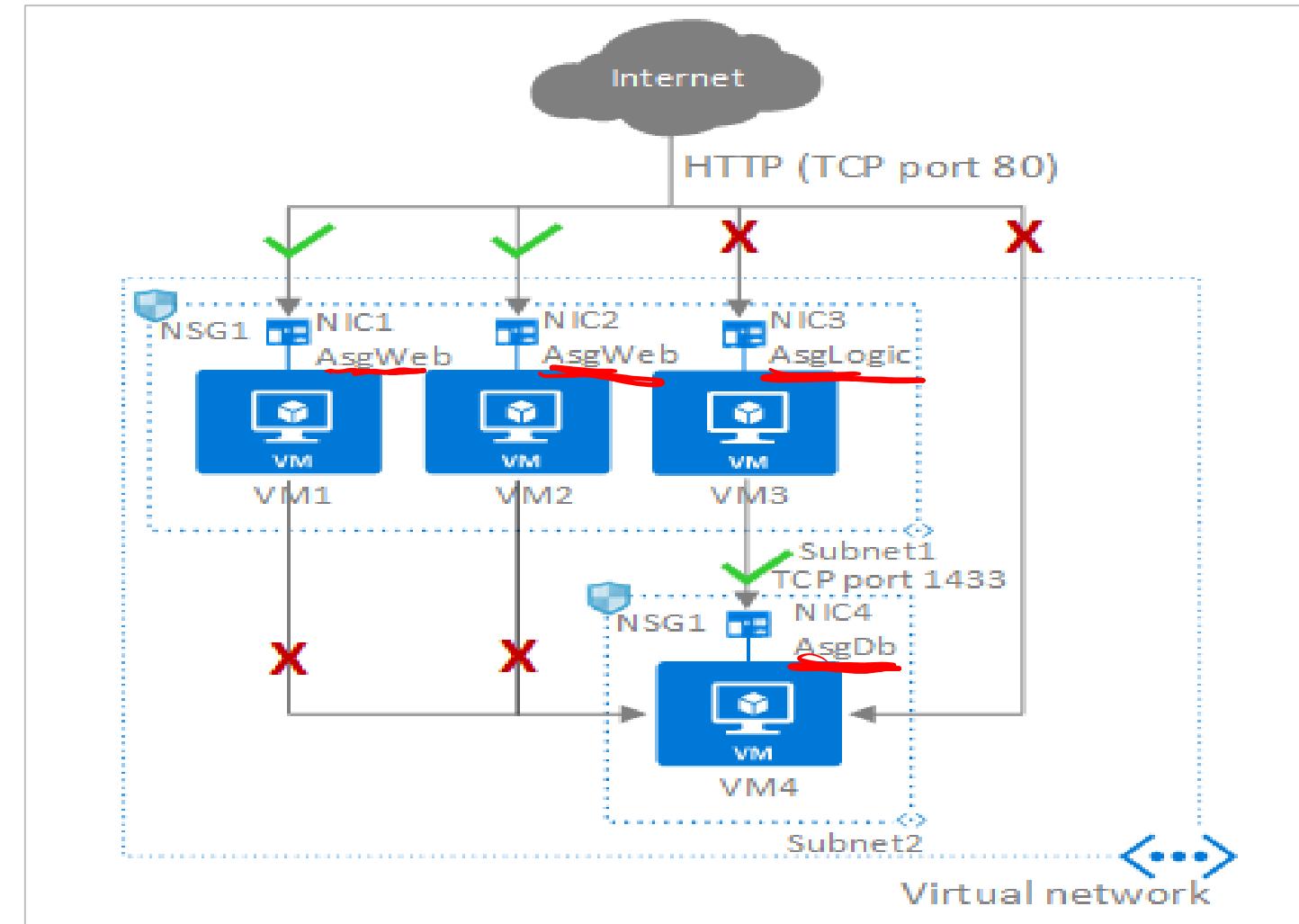
Application Security Groups (ASGs)

Extends your application's structure

ASGs logically group virtual machines – web servers, application servers

Define rules to control the traffic flow

Wrap the ASG with an NSG for added security



Service Endpoints

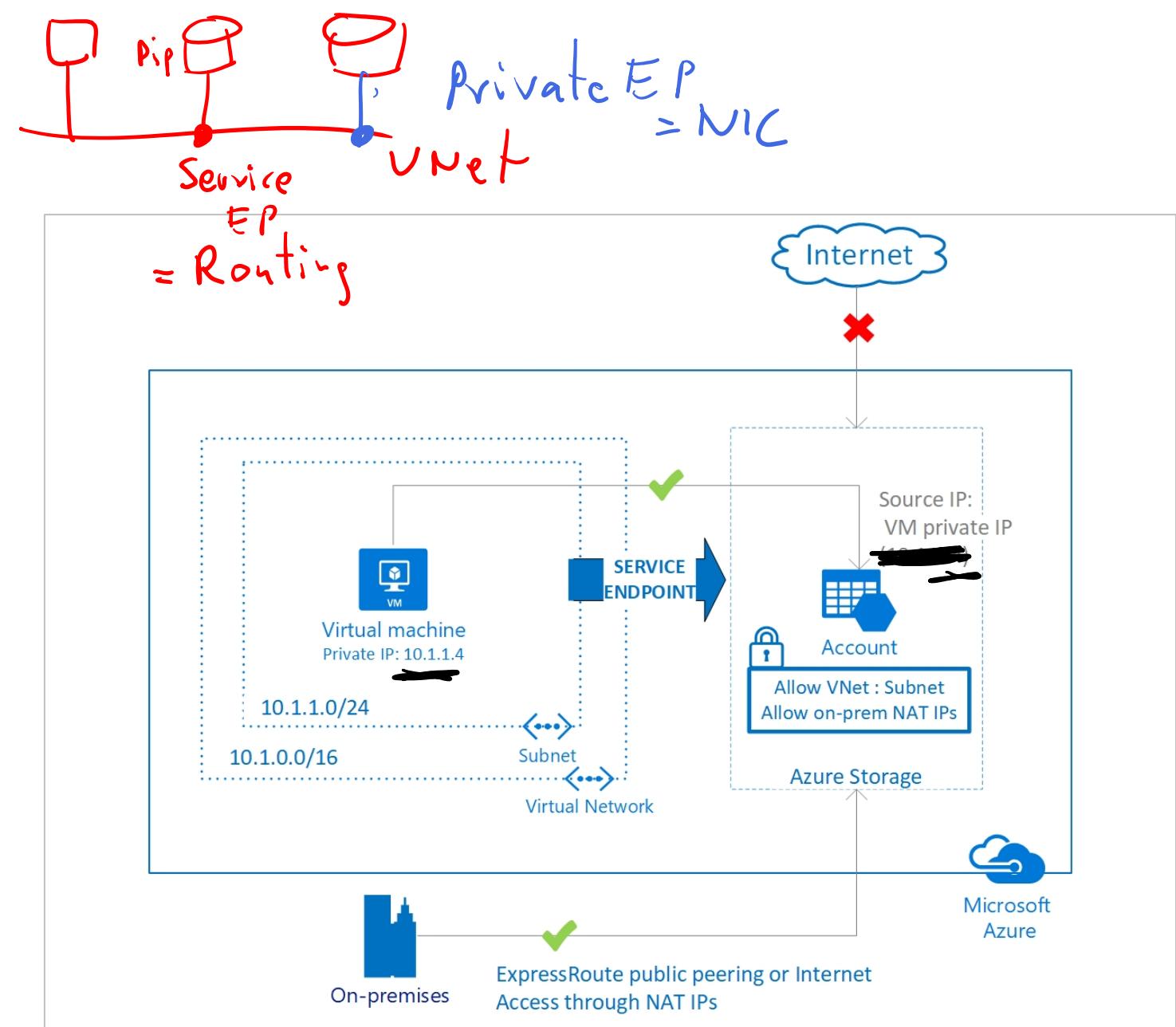
Endpoints limit network access to specific subnets and IP addresses

Improved security for your Azure service resources

Optimal routing for Azure service traffic from your virtual network

Endpoints use the Microsoft Azure backbone network

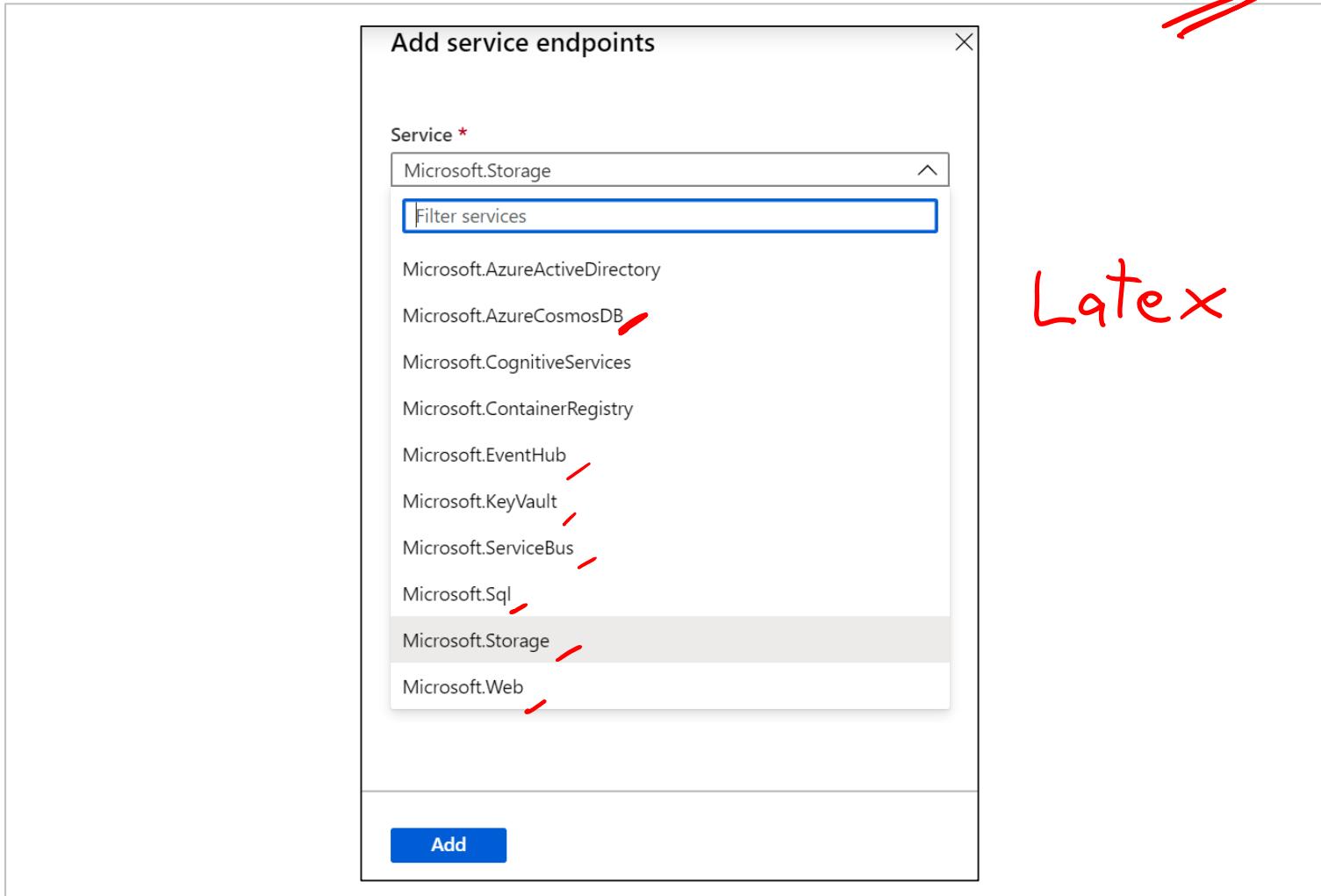
Simple to set up with less management overhead



Service Endpoint Services

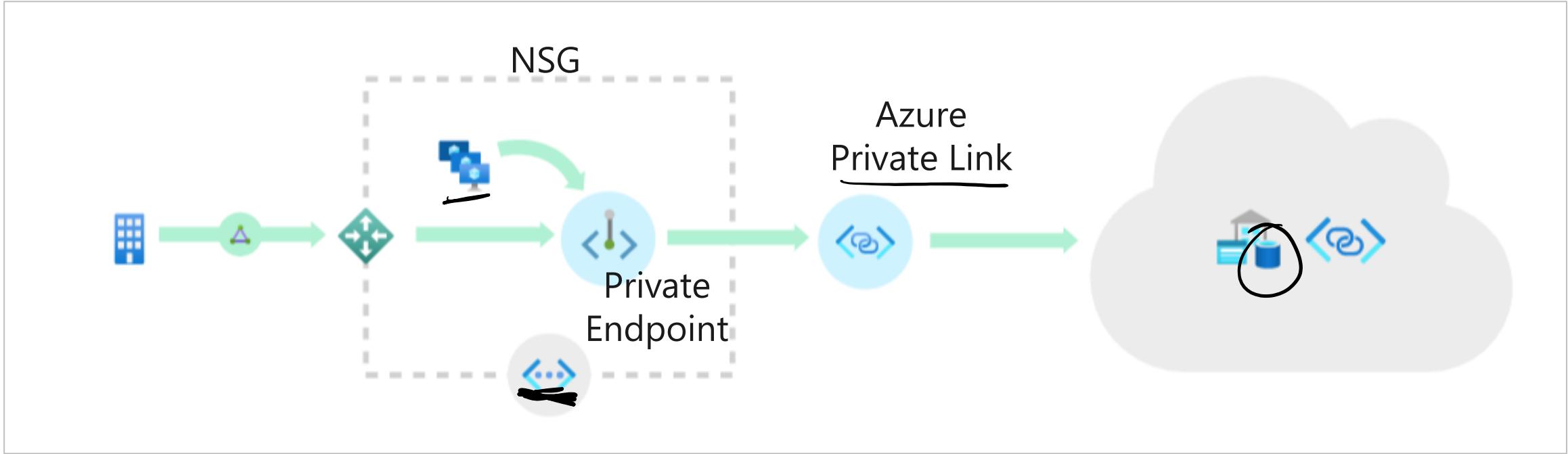
- ✓ Adding service endpoints can take up to 15 minutes to complete

TCP/IP Vint Cerf
Latex Leslie Lamport
TeX Don Knuth



Latex

Private Endpoint



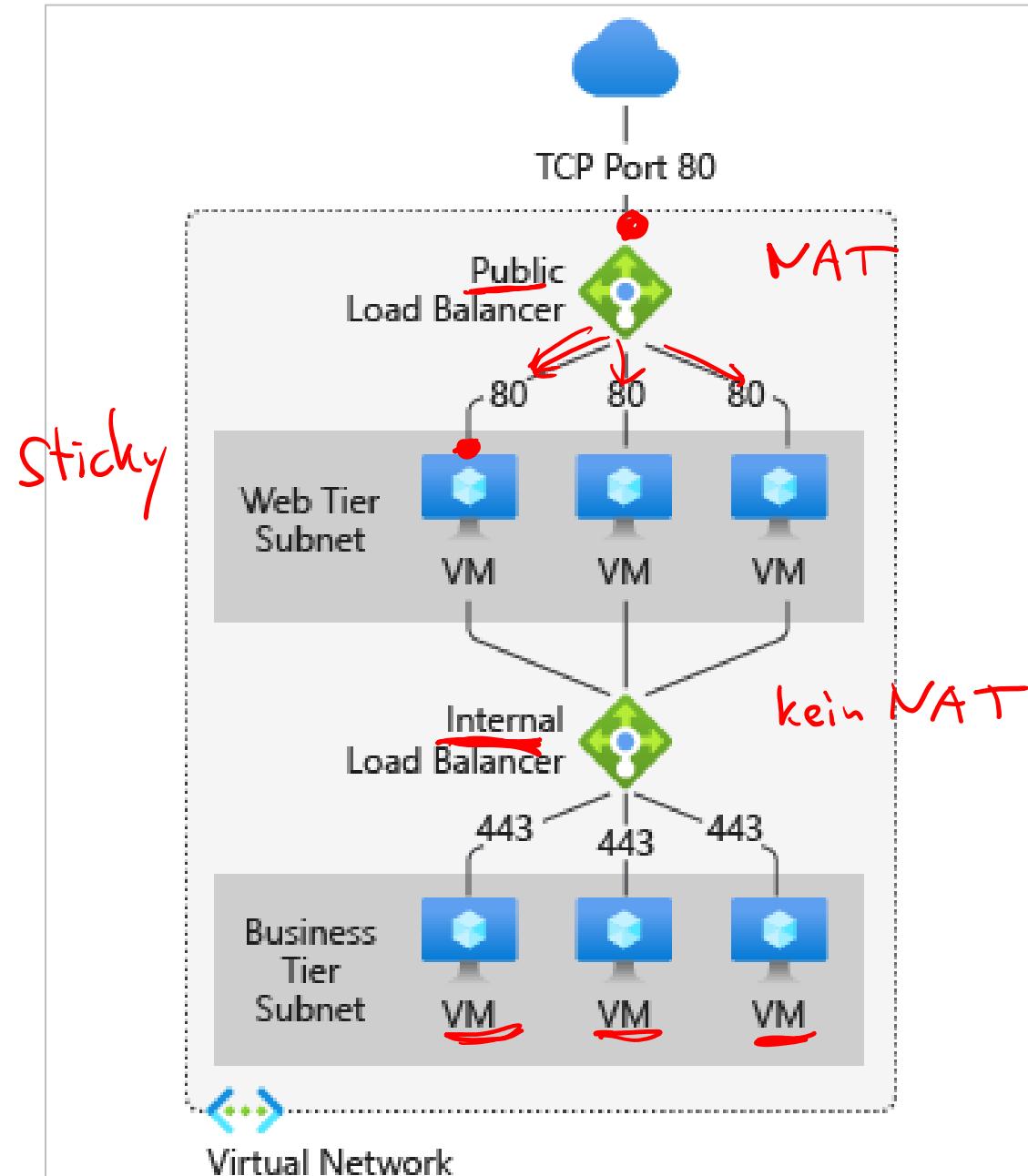
Private connectivity to services on Azure

Integration with on-premises and peered networks

Traffic remains on the Microsoft network,
with no public internet access

During a security incident within your network,
only the mapped resource would be accessible

Load Balancer

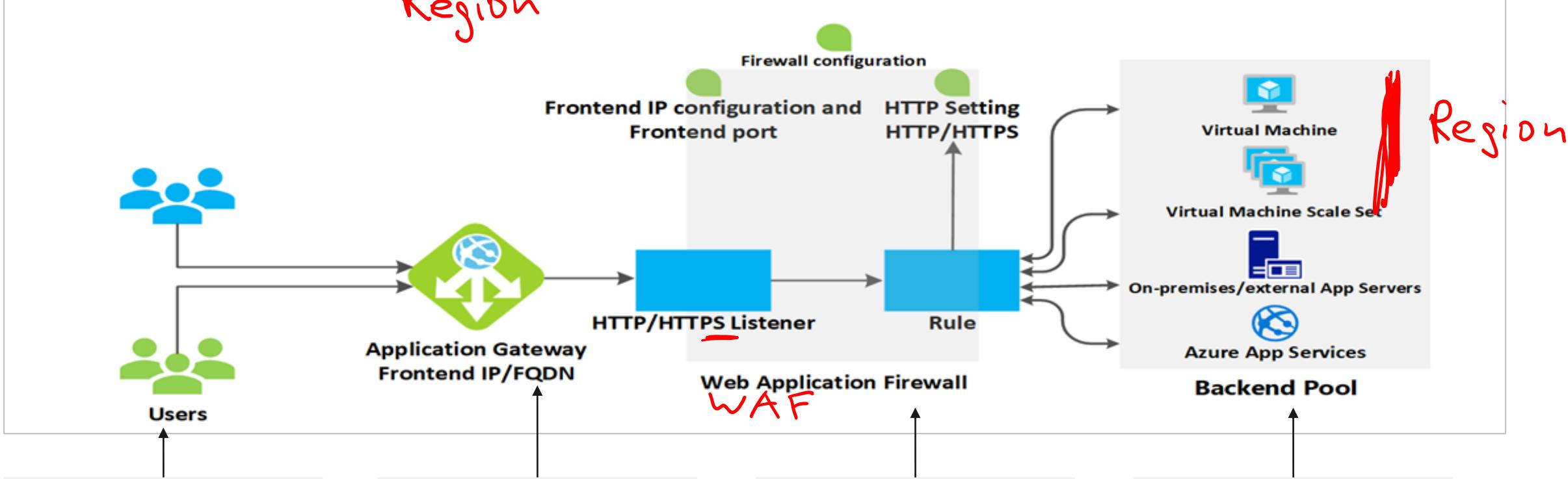


Balancing multi-tier applications by using both **public** and **internal** Load Balancer

Azure Application Gateway

http
https

Region



- Websocket and HTTP/2 traffic
- Custom error pages
- Rewrite HTTP headers

- Secure Sockets Layer (SSL/TLS) termination
- Multiple site hosting

- URL based routing
- Path-based redirection
- Session affinity

- Connection draining

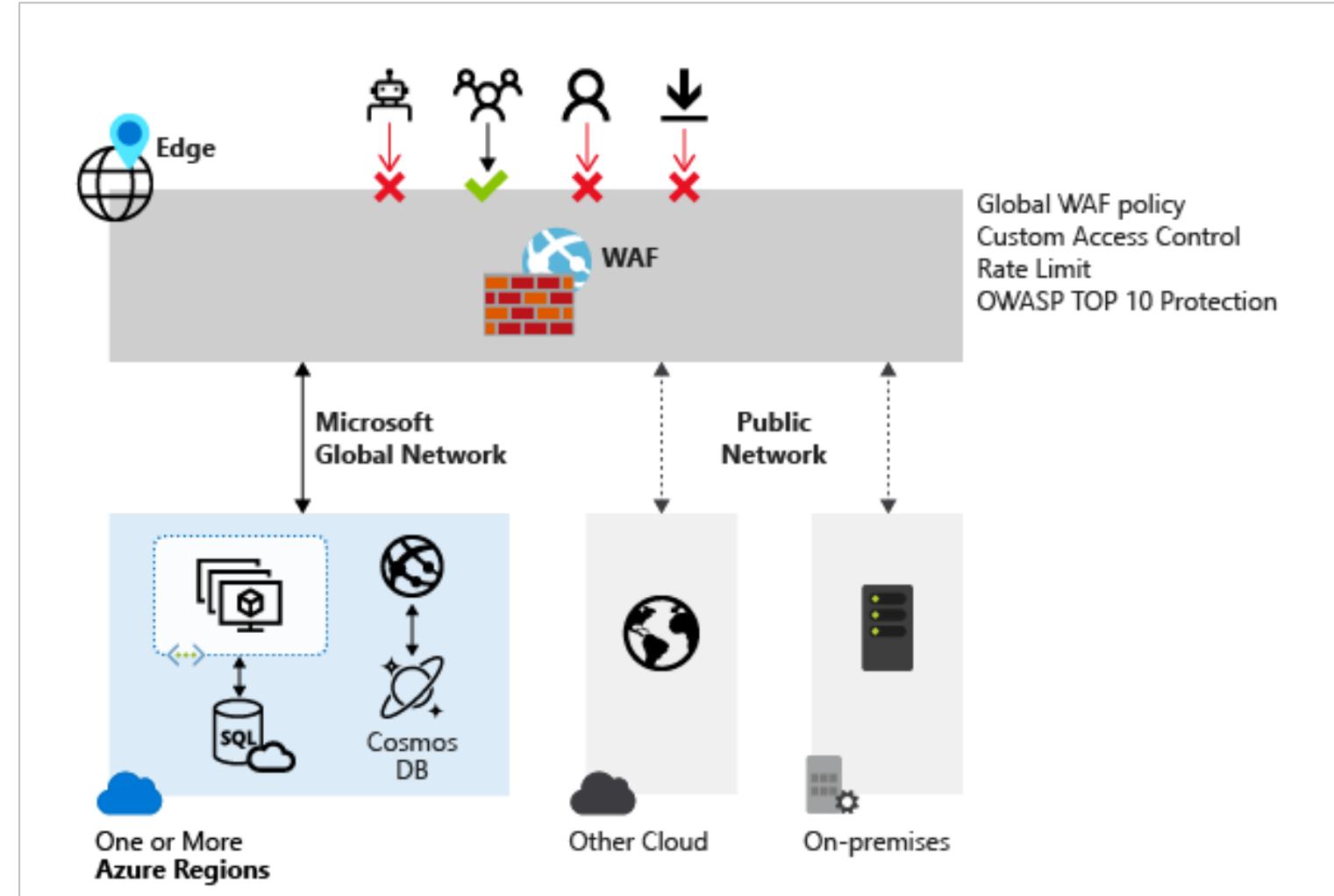
Web Application Firewall *WAF*

Protects against cross site scripting and SQL injection

OWASP Core Rule sets 3.1, 3.0, 2.29

Custom access control

Supports Azure Front Door, Azure Application Gateway, and CDN (preview)



Azure Front Door

Global

+ CDN

Layer 7 global routing

Accelerate application performance with
anycast and split TCP

URL-based routing and session affinity

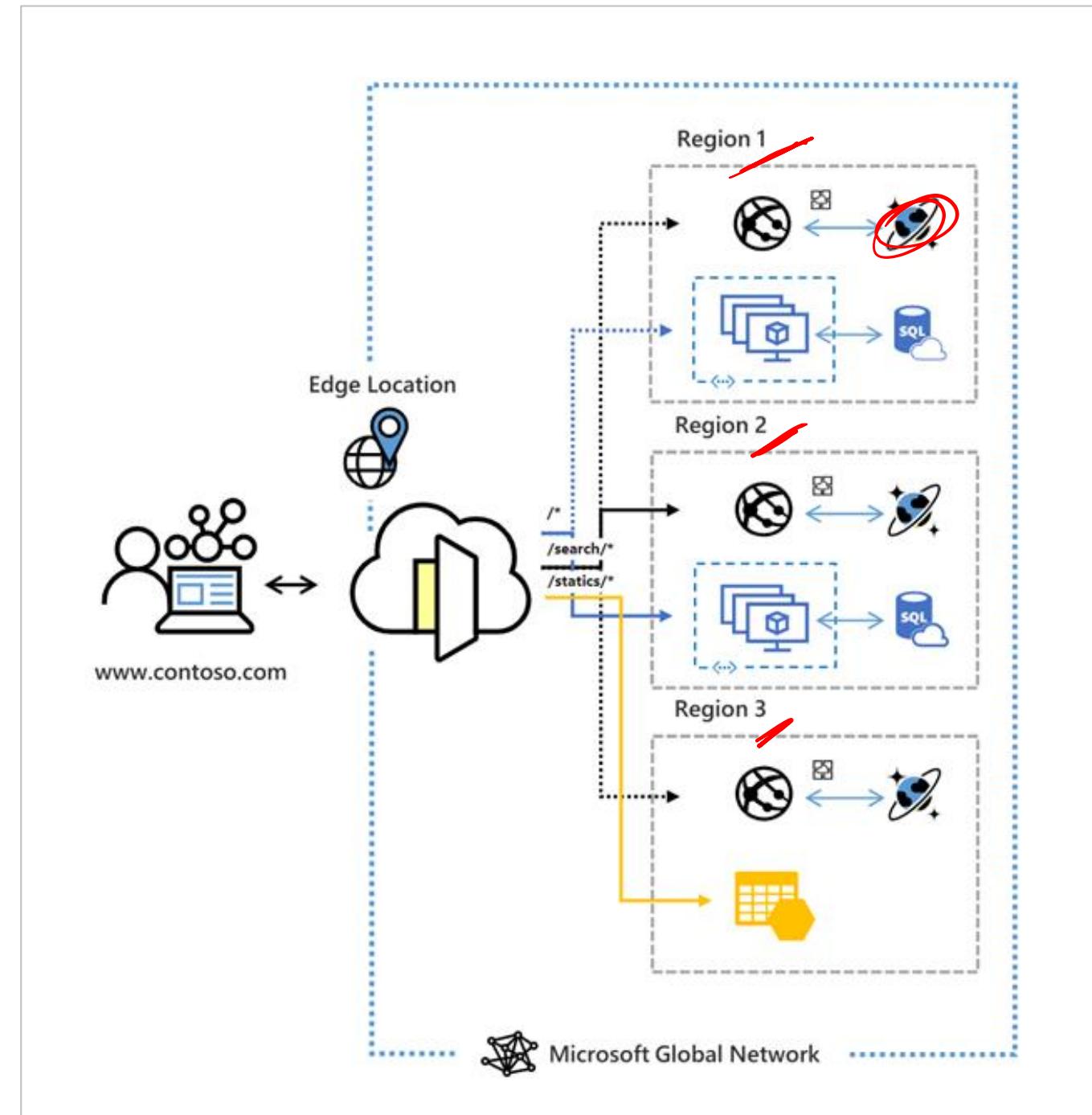
Multi-site hosting

Custom domains and certificate management

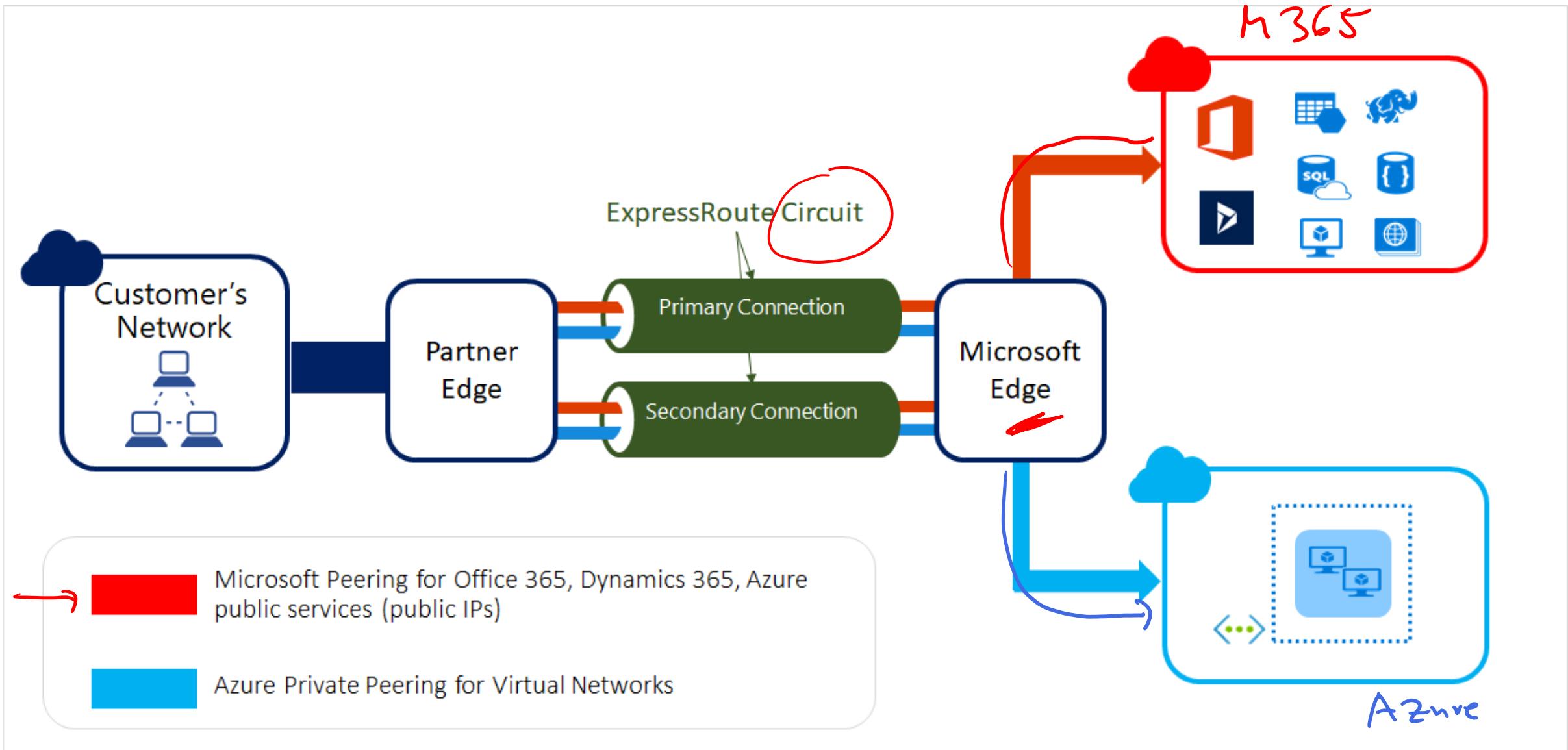
Application layer security - WAF

URL redirection and URL rewrite

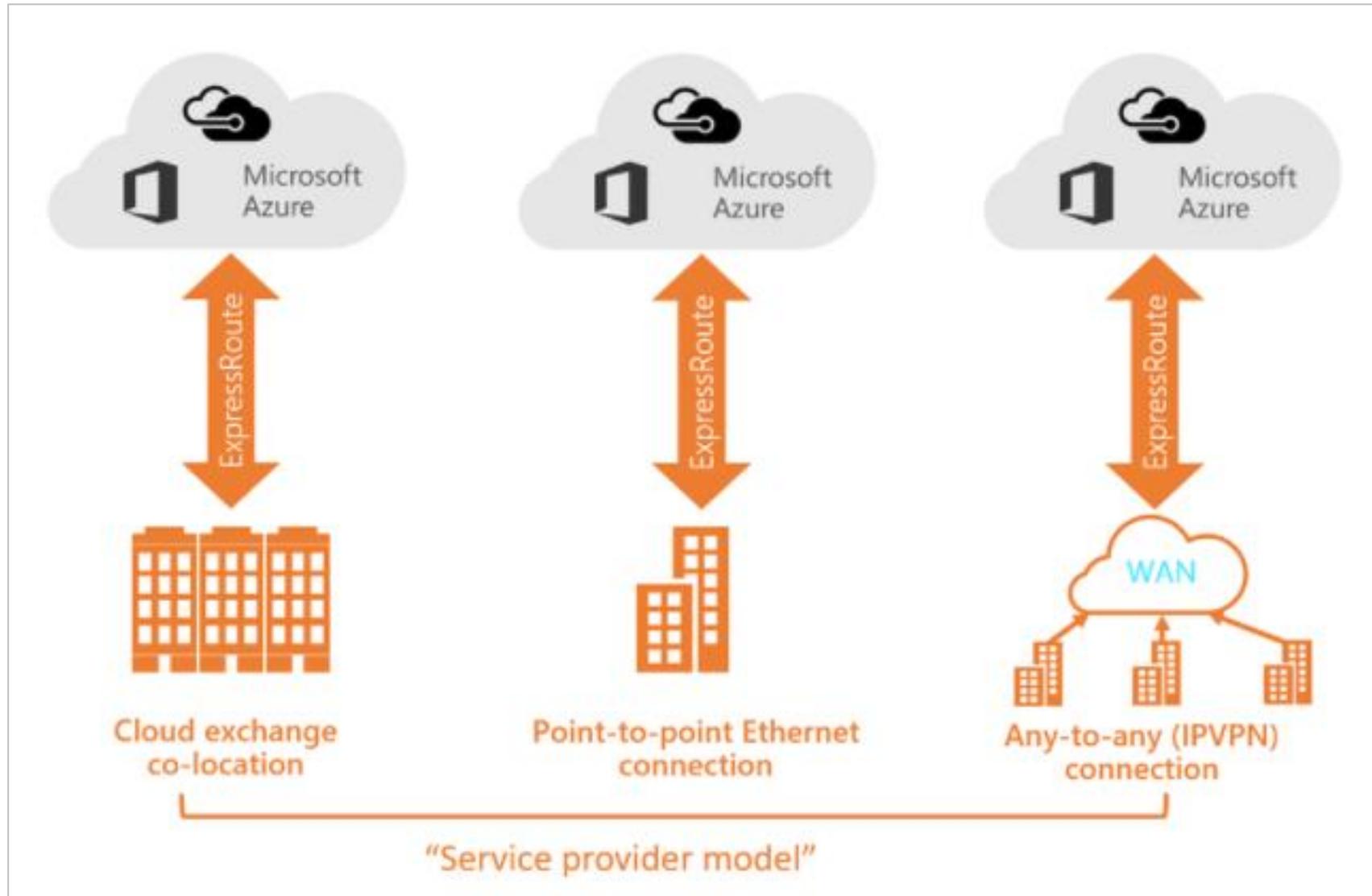
Protocol support – IPv6 and HTTP/2 traffic



ExpressRoute



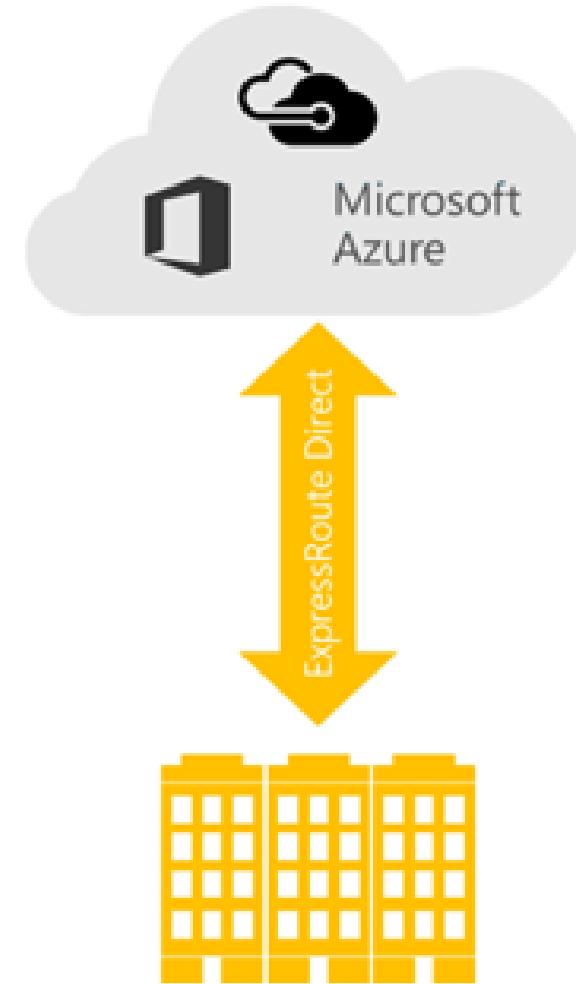
ExpressRoute – Service Provider Model



Note: Connectivity providers may offer one or more connectivity models.

ExpressRoute Direct

You can connect directly into the Microsoft's global network at a peering location strategically distributed across the world.



ExpressRoute site

“Direct model”

ExpressRoute using a service provider vs. ExpressRoute Direct

ExpressRoute Direct	ExpressRoute using a service provider
Requires 100 Gbps/10 Gbps infrastructure and full management of all layers	Uses service providers to enable fast onboarding and connectivity into existing infrastructure
Direct/Dedicated capacity for regulated industries and massive data ingestion	Integrates with hundreds of providers including Ethernet and Multiprotocol Label Switching (MPLS)
Customer may select a combination of the following circuit SKUs on 100-Gbps ExpressRoute Direct: 5 Gbps 10 Gbps 40 Gbps 100 Gbps	Circuits SKUs from 50 Mbps to 10 Gbps
Customer may select a combination of the following circuit SKUs on 10-Gbps ExpressRoute Direct: 1 Gbps 2 Gbps 5 Gbps 10 Gbps	
Optimized for single tenant with multiple business units and multiple work environments	Optimized for single tenant

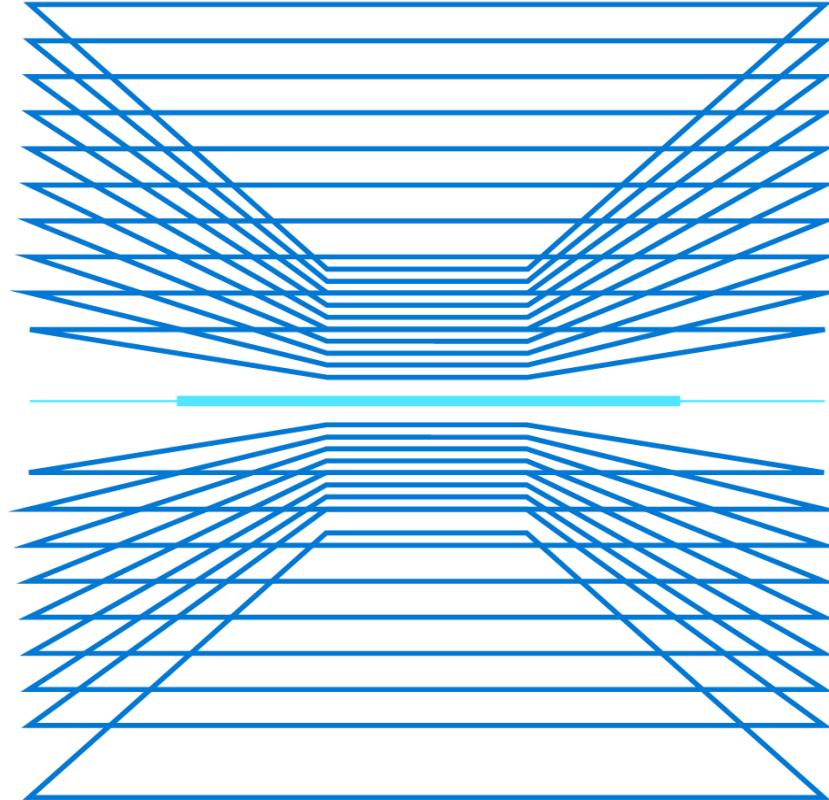
Circuit SKUs

Circuit Sizes	
100-Gbps ExpressRoute Direct	10-Gbps ExpressRoute Direct
Subscribed Bandwidth: 200 Gbps	Subscribed Bandwidth: 20 Gbps
<ul style="list-style-type: none">• 5 Gbps	<ul style="list-style-type: none">• 1 Gbps
<ul style="list-style-type: none">• 10 Gbps	<ul style="list-style-type: none">• 2 Gbps
<ul style="list-style-type: none">• 40 Gbps	<ul style="list-style-type: none">• 5 Gbps
<ul style="list-style-type: none">• 100 Gbps	<ul style="list-style-type: none">• 10 Gbps

Note: The physical port pairs are 100 Gbps or 10 Gbps only and can have multiple virtual circuits

Demonstrations: Network Connectivity

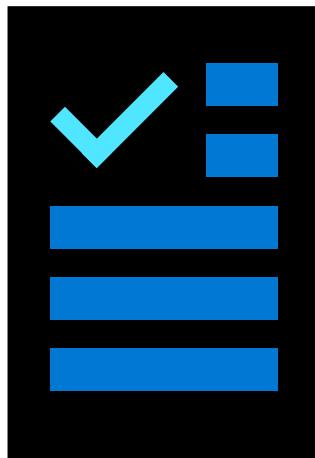
- Network Security Groups
- Application Security Groups



Additional Study – Network Security

Module Review Questions

Microsoft Learn Modules (docs.microsoft.com/Learn)



Encrypt network traffic end to end with Azure Application Gateway (Exercise)

Connect your on-premises network to the Microsoft global network by using ExpressRoute

Design a hybrid network architecture on Azure

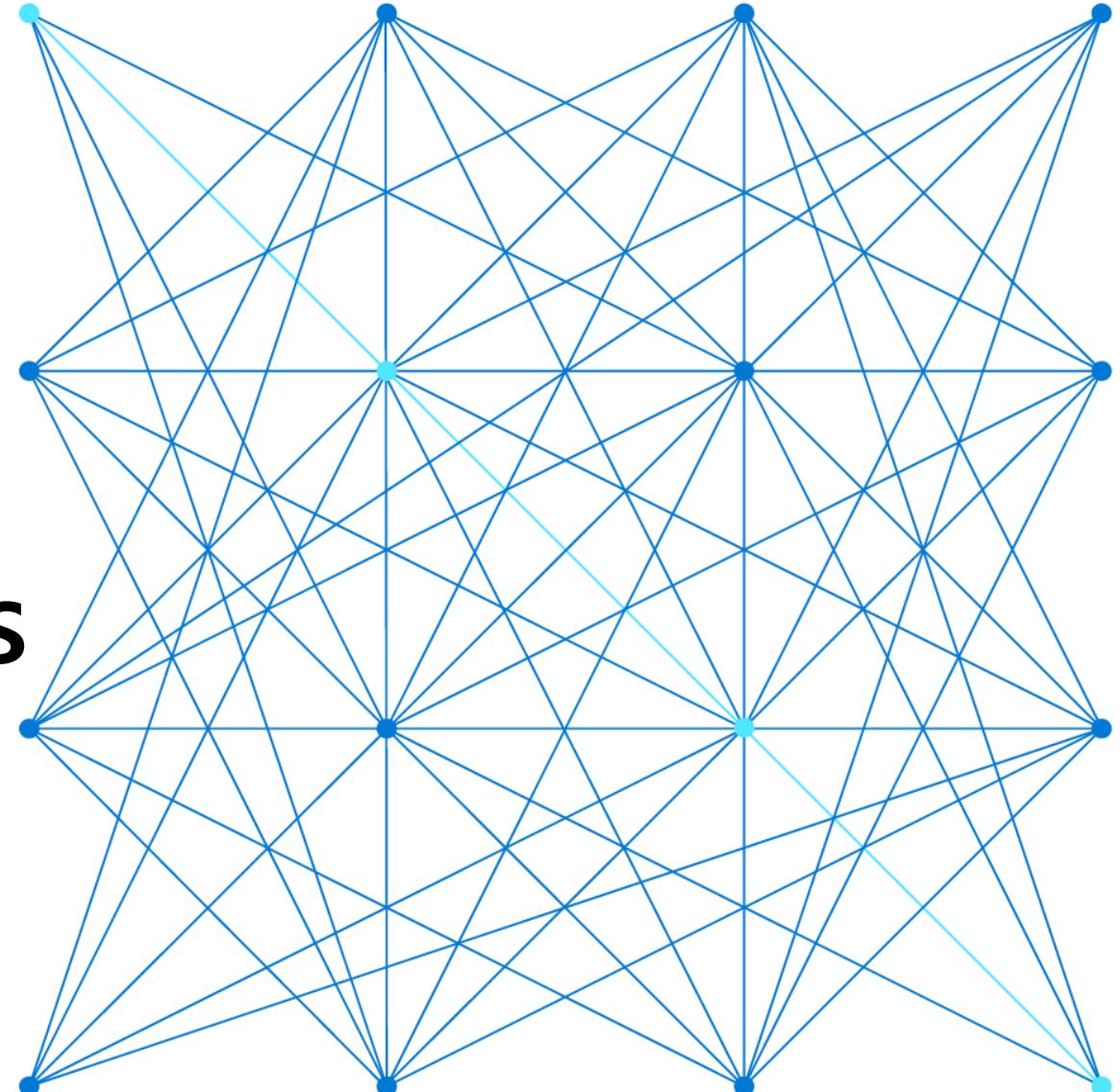
Secure and isolate access to Azure resources by using network security groups and service endpoints (Exercise)

AZ-500

Tag 3

Microsoft Azure Security Technologies

Guten Morgen !



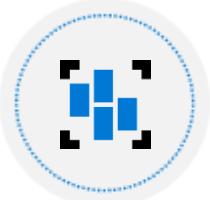
AZ-500 Agenda



Learning Path 1 Identity and Access



Learning Path 2 Implement Platform Protection

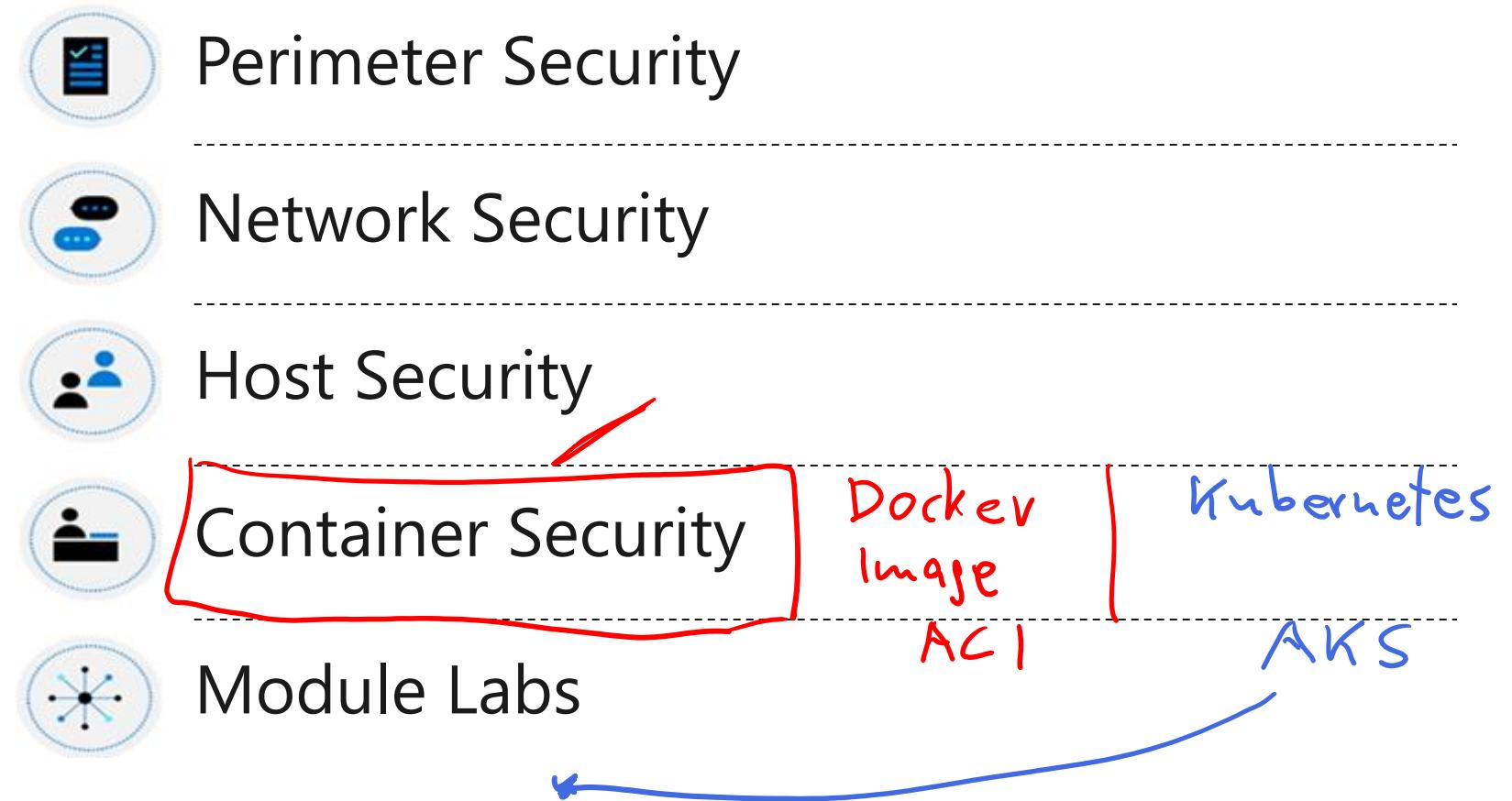


Learning Path 3 Data and Application Security



Learning Path 4 Security Operations

Learning Path: Implement Platform Protection



Host Security



Host Security



Endpoint Protection



Privileged Access Workstations



Virtual Machine Templates



Remote Access Management



Update Management



Disk Encryption



Microsoft Defender



Microsoft Defender for Cloud Recommendations



Securing Azure Workloads

Endpoint Protection



Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks **prevent, detect, investigate, and respond** to advanced threats.



Core Defender
Vulnerability
Management



Attack surface
reduction



Next-generation
protection



Endpoint detection
and response



Automated investigation
and remediation

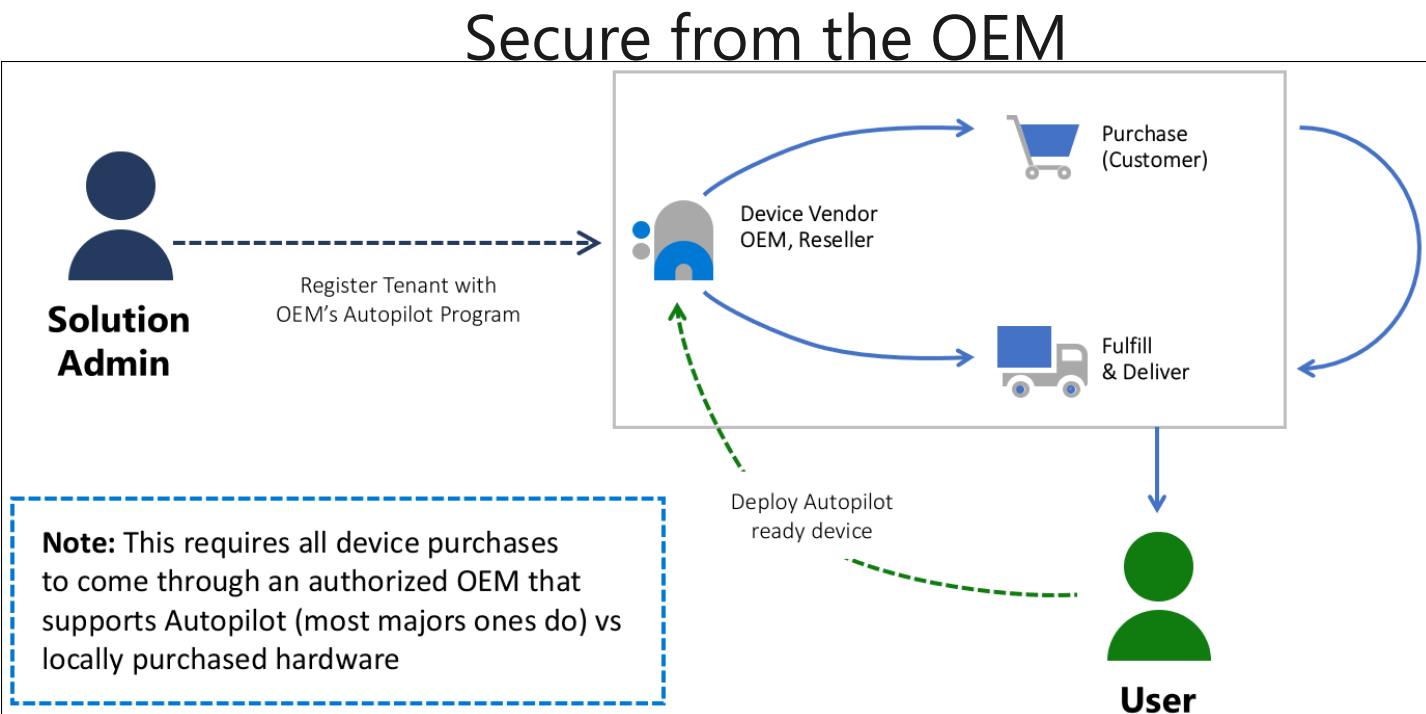


Microsoft
Threat Experts



Microsoft Defender for Endpoint is available in two plans, Defender for Endpoint Plan 1 and Plan 2.

Privileged Access Device Strategy



Hardware Root-of-Trust

- Trusted Platform Module (TPM) 2.0
- BitLocker Drive Encryption
- UEFI Secure Boot
- Drivers and Firmware Distributed through Windows Update
- Virtualization and HVCI Enabled
- Drivers and Apps HVCI-Ready
- Windows Hello
- DMA I/O Protection
- System Guard
- Modern Standby

Privileged Access Workstations



Separate dedicated administrative accounts and workstations.

Protects from Internet attacks and threat vectors phishing attacks, application and OS vulnerabilities, and credential theft attack

Appropriate for accounts with access to high value assets -Administrators and High Sensitivity Information Workers

Virtual Machine Templates

Improves consistency

Express complex deployments

Reduce manual, error prone tasks

Express requirements through code

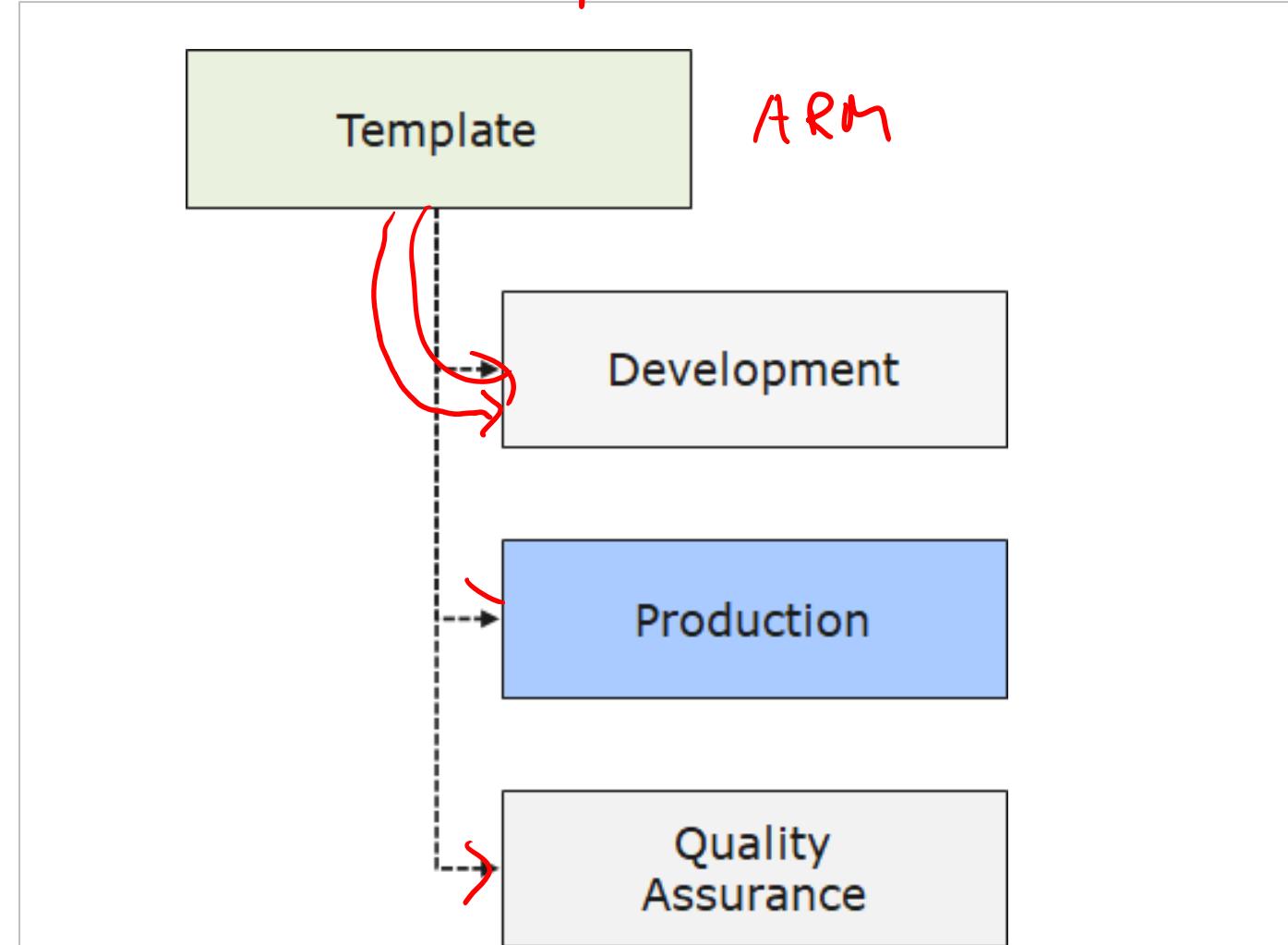
Promotes reuse

Modular and can be linked

Simplifies orchestration

Enforces security concerns

"Semper idem"
idem potent

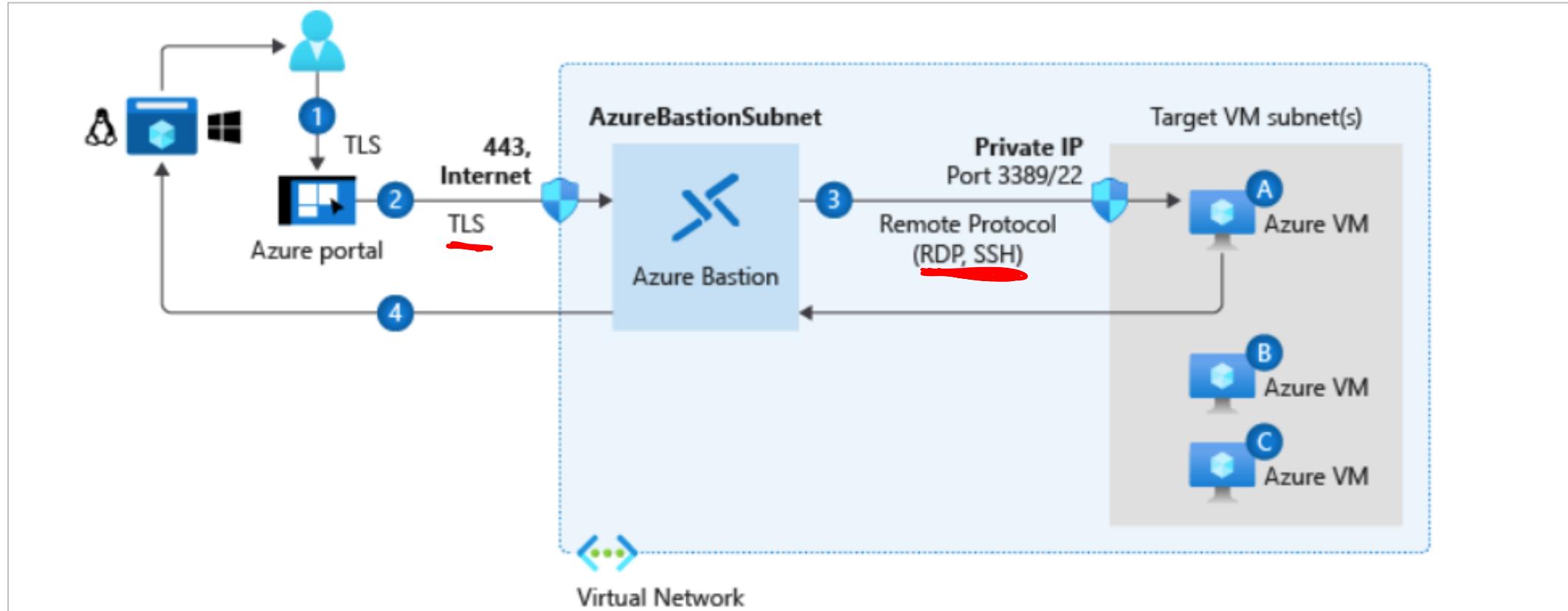


Remote Access Management

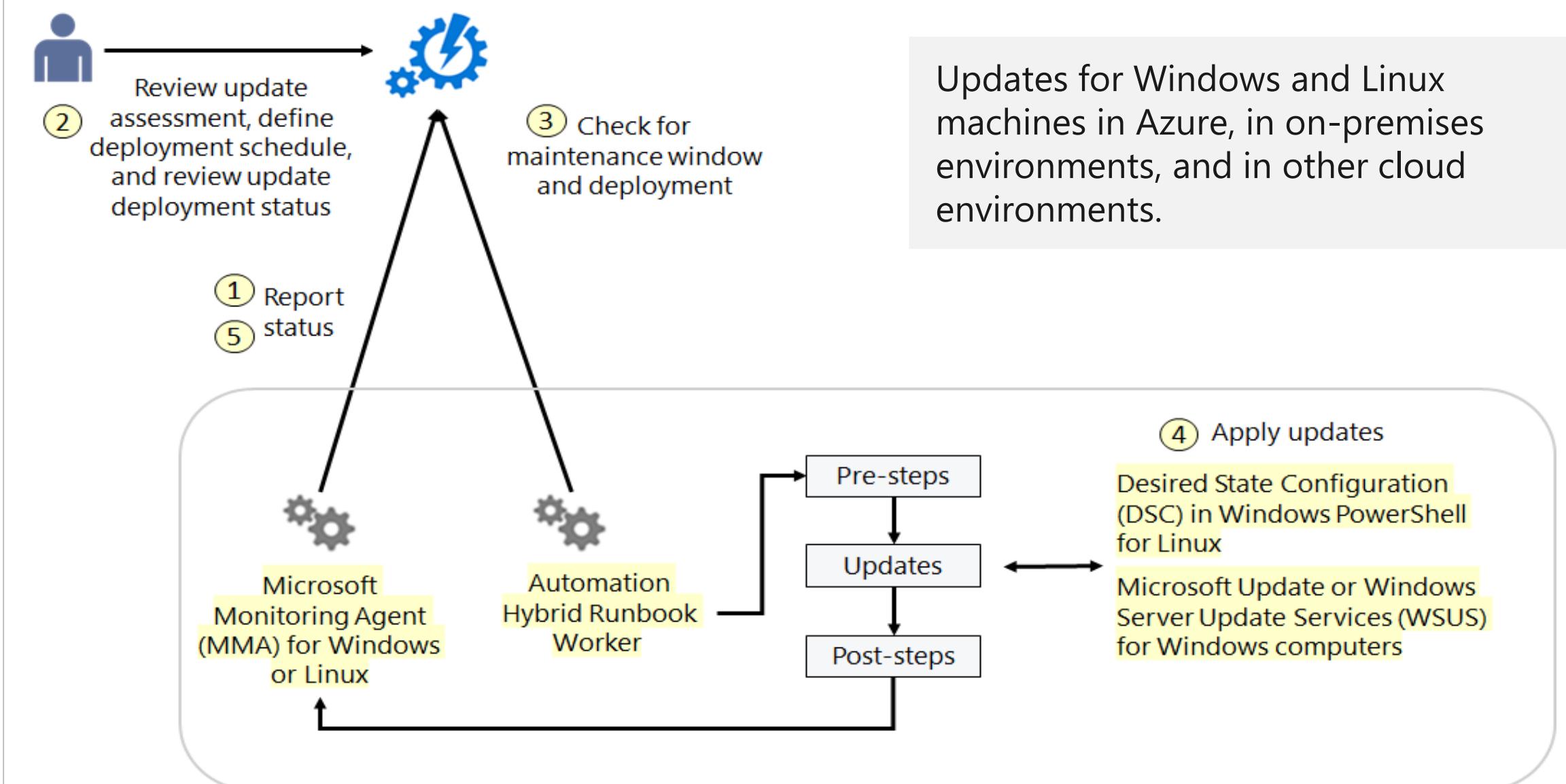
Remote Desktop Protocol (RDP) for Windows-based virtual machines

Secure Shell Protocol (SSH) for Linux based virtual machines

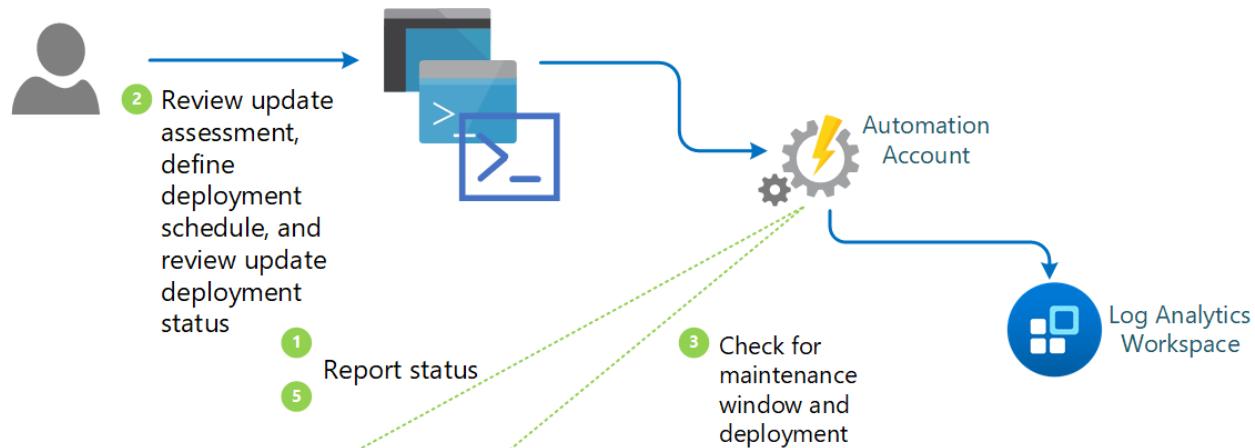
Bastion Subnet for RDP/SSH through the Portal over SSL



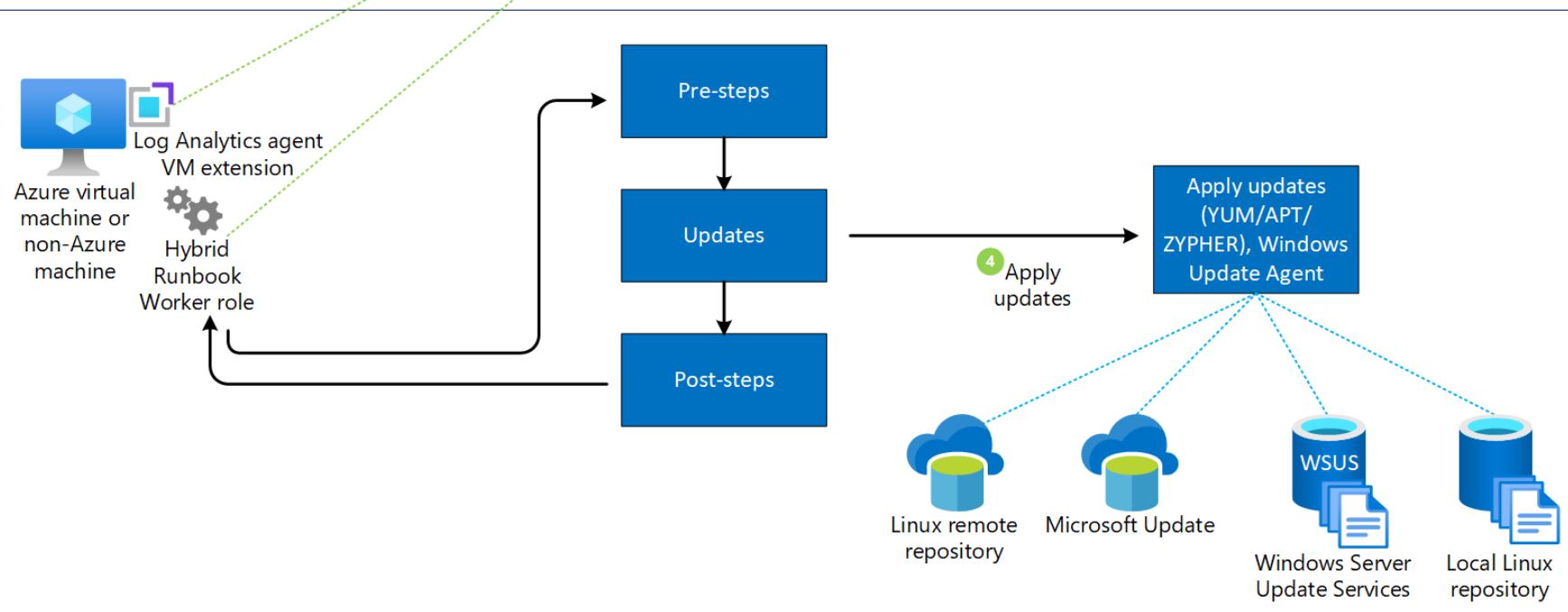
Update Management



Azure Automation Update Management Overview



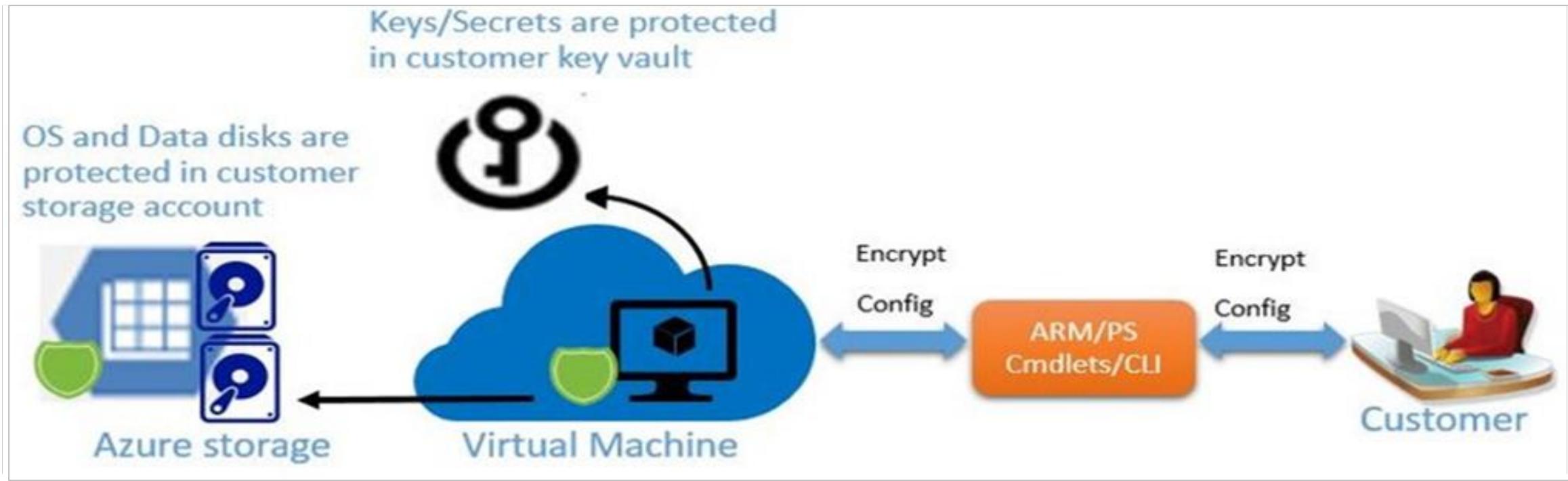
Updates for Windows and Linux machines in Azure, in on-premises environments, and in other cloud environments.



Azure Automation Update Management Overview (cont'd)

Connected source	Supported	Description
Windows	Yes	<p>Update Management collects information about system updates from Windows machines with the Log Analytics agent and installation of required updates.</p> <p>Machines need to report to Microsoft Update or Windows Server Update Services (WSUS).</p>
Linux	Yes	<p>Update Management collects information about system updates from Linux machines with the Log Analytics agent and installation of required updates on supported distributions.</p> <p>Machines need to report to a local or remote repository.</p>
Operations Manager management group	Yes	<p>Update Management collects information about software updates from agents in a connected management group.</p> <p>A direct connection from the Operations Manager agent to Azure Monitor logs isn't required. Log data is forwarded from the management group to the Log Analytics workspace.</p>

Disk Encryption



Provides encryption of the operating system and data disks

Windows VMs (BitLocker) and Linux VMs (DM-Crypt)

Stores encryption keys in a customer-managed key vault

Managed disk Encryption Options

	Encryption at rest (OS and data disks)	Temp disk encryption	Encryption of caches	Data flows encrypted between Compute and Storage	Customer control of keys	Does not use your VM's CPU	Works for custom images	Enhanced Key Protection	Microsoft Defender for Cloud disk encryption status
Azure Disk Storage Server-Side Encryption at rest	✓	✗	✗	✗	✓ When configured with Data Encryption Standard (DES)		✗	✗	Unhealthy not applicable if exempt
Azure Disk Encryption	✓	✓	✓	✓	✓	✗	✗	✗	Healthy
Encryption at Host	✓	✓							Unhealthy not applicable if exempt
Confidential disk encryption	✓ For the OS disk only	✗	✓ For the OS disk only	✓ For the OS disk only	✓ For the OS disk only	✗	✓	✓	Unhealthy not applicable if exempt



For **Encryption at host** and **Confidential disk encryption**, Microsoft Defender for Cloud does not detect the encryption state. We are in the process of updating Microsoft Defender.

Microsoft Defender for Endpoint – Supported Operating Systems

Supported Windows versions	
Windows 11	Enterprise, Education, Pro, Pro Education
Windows 10	Enterprise, Enterprise LTSC: 2016 (or later), Enterprise IoT, Enterprise Education, Windows 10 Pro, Windows 10 Pro Education
Windows 8.1	Enterprise, and Pro
Windows 7 SP1	Enterprise (Requires ESU for support.), and Pro (Requires ESU for support.)
Windows Server	2008 R2 SP1 (Requires ESU for support), 2012 R2, 2016, version 1803 or later, 2019 and later, 2019 core edition, and 2022
Windows	Virtual Desktop
Windows	365
Other Operating Systems	
macOS	
Linux	
Android	
iOS	

Microsoft cloud security benchmark in Defender for Cloud

- The Microsoft cloud security benchmark (MCSB) provides best practices and recommendations, with input from a set of holistic Microsoft and industry security guidance that includes:



Cloud Adoption Framework: Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.



Azure Well-Architected Framework: Guidance on securing your workloads on Azure.



The Chief Information Security Officer (CISO) Workshop: Program guidance and reference strategies to accelerate security modernization using Zero Trust principles.



Other industry and cloud service providers security best practice standards and framework: Examples include the Amazon Web Services, Center for Internet Security (CIS) Controls, National Institute of Standards and Technology, and the Payment Card Industry Data Security Standard.

Regulatory compliance dashboard

Microsoft Defender for Cloud streamlines the process for meeting regulatory compliance requirements, using the regulatory compliance dashboard.

The compliance dashboard gives you a view of your overall compliance standing.

Security for non-Azure platforms follows the same cloud-neutral security principles as Azure.

The screenshot shows the Microsoft Defender for Cloud Regulatory Compliance Dashboard. At the top, there are navigation links: Download report, Manage compliance policies, Open query, Compliance over time workbook, Audit reports, and Compliance offerings. A message indicates that users can now fully customize the standards they track in the dashboard by selecting 'Manage compliance policies' above. Below this, there are two main sections: 'Microsoft cloud security benchmark' and 'Lowest compliance regulatory standards'. The 'Microsoft cloud security benchmark' section shows a progress bar for 52 of 62 passed controls. The 'Lowest compliance regulatory standards' section lists four standards with their respective scores: SOC TSP (1/13), PCI DSS 3.2.1 (13/43), ISO 27001 (9/20), and Azure CIS 1.4.0 (94/109). Further down, there's a survey question 'Is the regulatory compliance experience clear to you?' with 'Yes' and 'No' options. Below that, there are tabs for 'Microsoft cloud security benchmark', 'ISO 27001', 'PCI DSS 3.2.1', 'SOC TSP', and 'Azure CIS 1.4.0'. A note states that recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to the user to evaluate the environment. These services are subject to the terms and conditions in the [licensing terms](#). A specific note mentions that the Microsoft cloud security benchmark is applied to the subscription MCAPS-Hybrid-REQ-48118-2022-serlingdavis. At the bottom, there's a checkbox for 'Expand all compliance controls' and a list of three categories: NS. Network Security (red X), IM. Identity Management (green checkmark), and PA. Privileged Access (red X).

Download report Manage compliance policies Open query Compliance over time workbook Audit reports Compliance offerings

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

Microsoft cloud security benchmark

52 of 62 passed controls

Lowest compliance regulatory standards

Show all 5

Standard	Score
SOC TSP	1/13
PCI DSS 3.2.1	13/43
ISO 27001	9/20
Azure CIS 1.4.0	94/109

Is the regulatory compliance experience clear to you? Yes No

Microsoft cloud security benchmark ISO 27001 PCI DSS 3.2.1 SOC TSP Azure CIS 1.4.0

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to you to evaluate a environment. These services are subject to the terms and conditions in the [licensing terms](#).

Microsoft cloud security benchmark is applied to the subscription MCAPS-Hybrid-REQ-48118-2022-serlingdavis

Expand all compliance controls

NS. Network Security (red X)

IM. Identity Management (green checkmark)

PA. Privileged Access (red X)

Recommendations

Using the policies, Defender for Cloud periodically analyzes the compliance status of your resources to identify potential security misconfigurations and weaknesses.

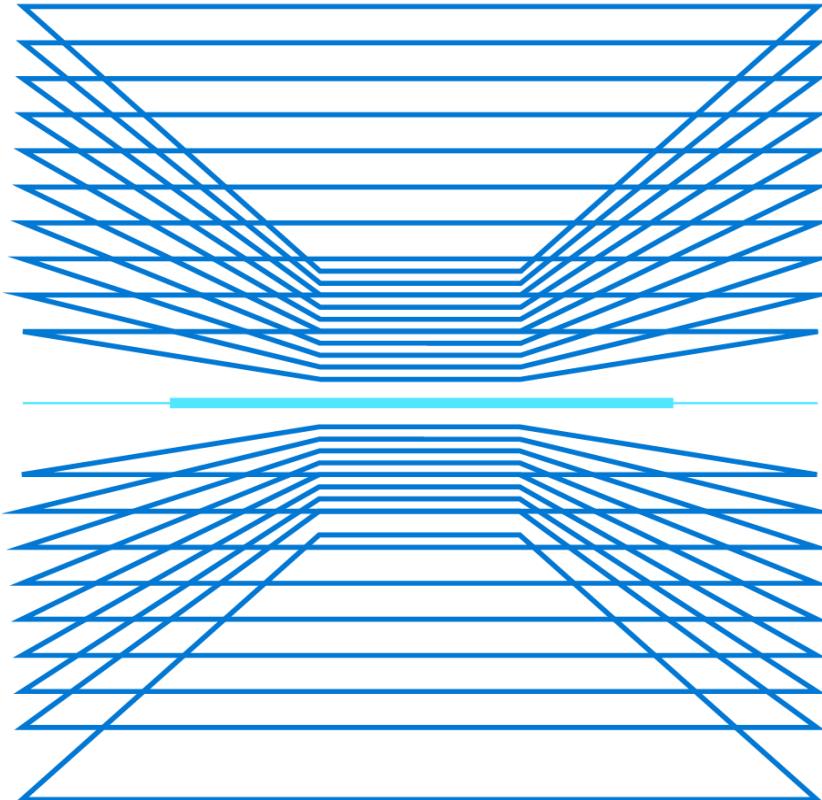
It then provides you with recommendations on how to remediate those issues.

Recommendations result from assessing your resources against the relevant policies and identifying resources that aren't meeting your defined requirements.

Secure score recommendations		All recommendations
 77%	Secure score ⓘ	 7/38 Active recommendations
<input type="text"/> Search recommendations		Recommendation status == None ×
 ⓘ Name ↑		Max score ↓
 > Enable MFA		10
 > Secure management ports		8
 > Remediate vulnerabilities		6
 > Apply system updates		6
 > Encrypt data in transit		4
 > Manage access and permissions		4
 > Enable encryption at rest		4
 > Remediate security configurations		4
 > Restrict unauthorized network access		4

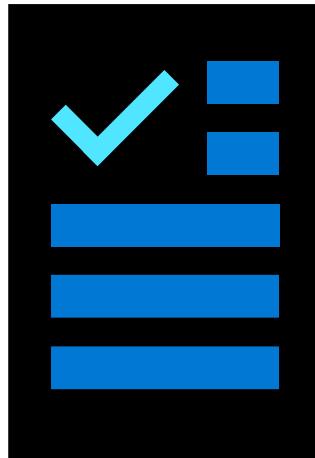
Demonstrations: Host Security

- Bastion connections
- Virtual machine updates
- Virtual machine extensions
- Disk encryption
- RDP to Windows VMs (optional)
- SSH to Linux VMs (optional)



Additional Study – Host Security

Module Review Questions



Microsoft Learn Modules (docs.microsoft.com/Learn)

Build Azure Resource Manager templates (Exercise)

Secure your Azure virtual machine disks (Exercise)

Protect against threats with Microsoft Defender for Endpoint

Introduction to Azure virtual machines (Exercise)

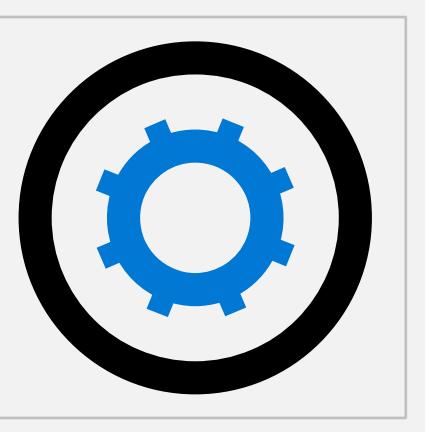
Keep your virtual machines updated (Exercise)

Create a Windows virtual machine in Azure (Exercise)

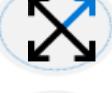
Create a Linux virtual machine in Azure (Exercise)

Security baselines

Container Security



Container Security

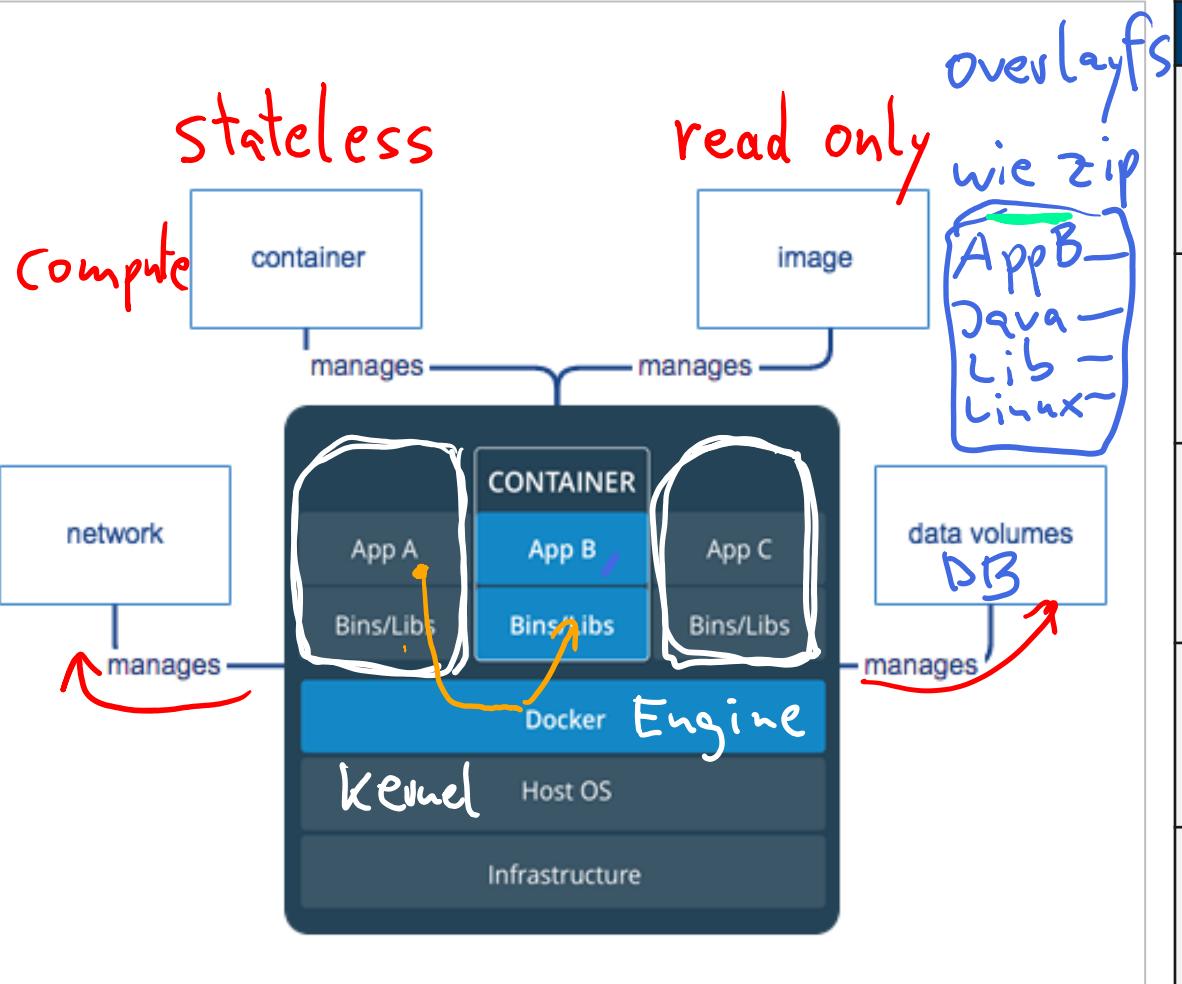
-  Containers
-  ACI Security
-  Azure Container Instances (ACI)
ACI
-  Azure Container Registry (ACR)
ACR
-  ACR Authentication
-  Azure Kubernetes Service (AKS)
AKS
-  AKS Terminology
-  AKS Architecture
-  AKS Networking
-  AKS Storage
-  AKS and Active Directory

Containers

(Image-) Container Registry

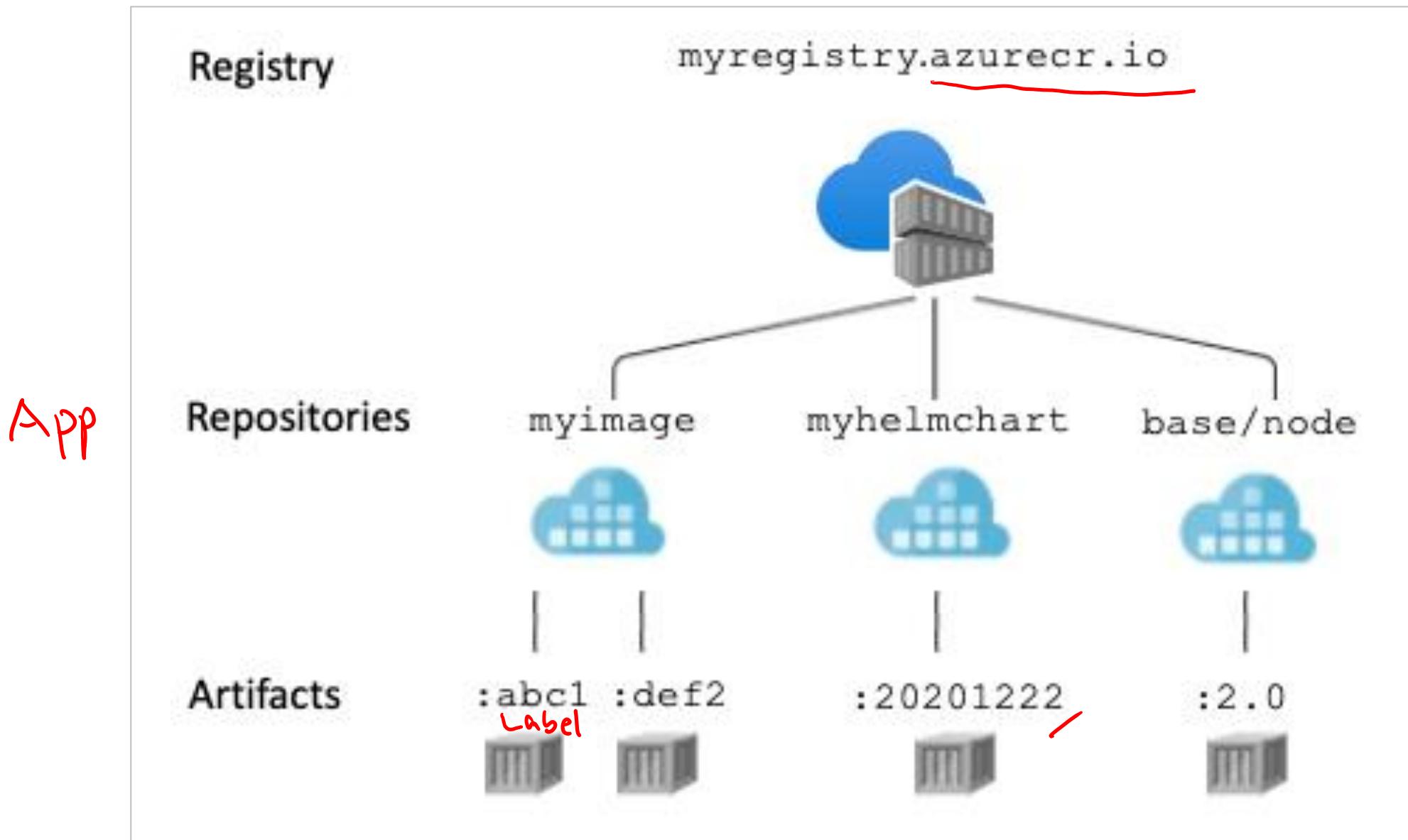
Docker Hub
Azure Container Registry

pub
priv



Feature	Containers
Isolation	Typically provides lightweight isolation from the host and other containers but doesn't provide as strong a security boundary as a virtual machine.
Operating system	Runs the user mode portion of an operating system and can be tailored to contain just the needed services for your app, using fewer system resources.
Deployment	Deploy individual containers by using Docker via command line; deploy multiple containers by using an orchestrator such as Azure Kubernetes Service.
Persistent storage	Use Azure Disks for local storage for a single node, or Azure Files (SMB shares) for storage shared by multiple nodes or servers.
Fault tolerance	If a cluster node fails, any containers running on it are rapidly recreated by the orchestrator on another cluster node.

Container Registry



Container Registry (cont'd)

docker build .

A diagram illustrating the Docker build process. On the left, a grey rectangular box contains a Dockerfile with the following content:

```
Dockerfile
FROM mcr.microsoft.com/dotnet/core/aspnet:3.0
WORKDIR /app
COPY published/aspnetapp.dll .
ENTRYPOINT ["dotnet", "aspnetapp.dll"]
```

The word "Dockerfile" is circled in blue. The first four lines of the Dockerfile are underlined in red. A blue arrow points from the "Dockerfile" icon at the top left to the "Dockerfile" section in the box. Another blue arrow points from the ".\" at the end of the COPY command to the "Docker build command" section below.

Docker build
command



Azure Container Registry (ACR)

Docker registry service

Private and hosted in Azure

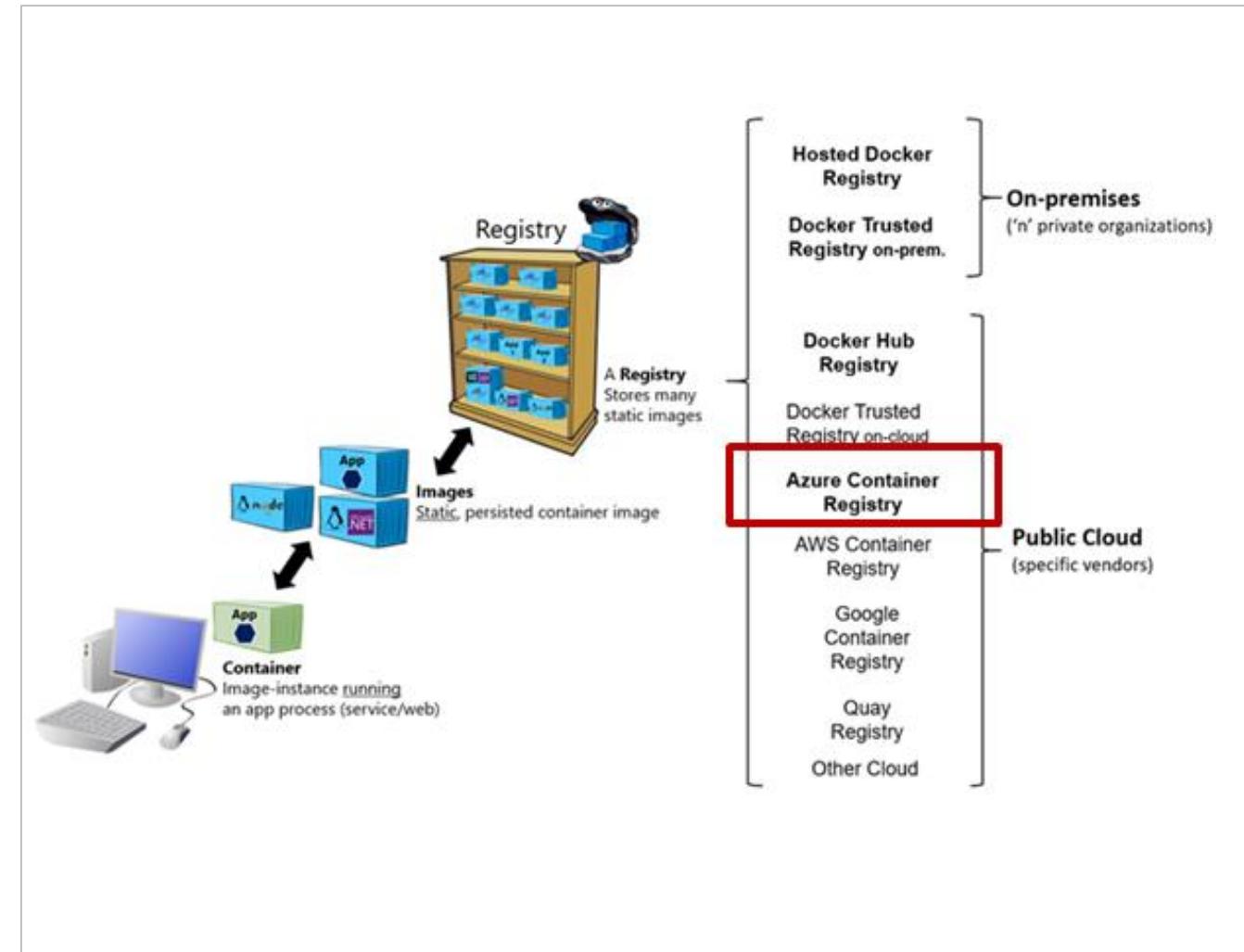
Build, store, and manage images

Push and pull with the Docker CLI or the Azure CLI

Access with Azure AD

RBAC to assign permissions

Automate using DevOps



Azure Container Registry - Key Features

- *Registry service tiers* - Create one or more container registries in your Azure subscription.
- *Security and access* - You log in to a registry using the Azure CLI or the standard docker login command.
- *Supported images and artifacts* - Grouped in a repository, each image is a read-only snapshot of a Docker-compatible container.
- *Automated image builds* - Use Azure Container Registry Tasks (ACR Tasks) to streamline building, testing, pushing, and deploying images in Azure.

Azure Container Registry - Service Tiers

Tier	Description
Basic	A cost-optimized entry point for developers learning about Azure Container Registry. Basic registries have the same programmatic capabilities as Standard and Premium (such as Azure Active Directory authentication integration, image deletion, and webhooks). However, the included storage and image throughput are most appropriate for lower usage scenarios.
Standard	Standard registries offer the same capabilities as Basic, with increased included storage and image throughput. Standard registries should satisfy the needs of most production scenarios.
Premium	Premium registries provide the highest amount of included storage and concurrent operations, enabling high-volume scenarios. In addition to higher image throughput, Premium adds features such as geo-replication for managing a single registry across multiple regions, content trust for image tag signing, private link with private endpoints to restrict access to the registry.

Azure Container Instances (ACI)

PaaS Service

Custom sizes - fast startup times

Public IP connectivity and DNS name

Hypervisor-level security

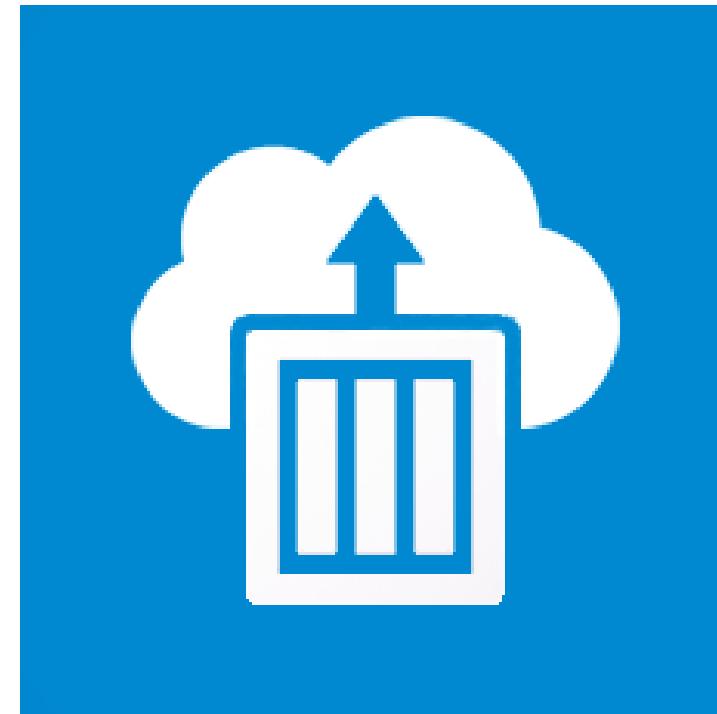
Isolation features

Co-scheduled groups

Persistent storage

Linux and Windows containers

Virtual network deployments



Gain the security of virtual machines for your container workloads, while preserving the efficiency of lightweight containers. ACI provides hypervisor isolation for each container group to ensure containers run in isolation without sharing a kernel.

Azure Container Instances (ACI)



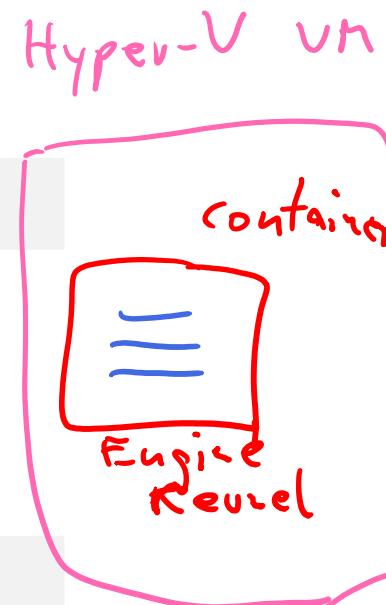
Run containers without managing servers



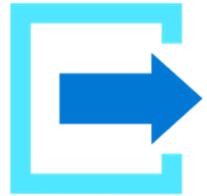
Increase agility with containers on demand



Secure applications with hypervisor isolation



Compliant Deployments



Hypervisor-level security



Customer data



Custom sizes



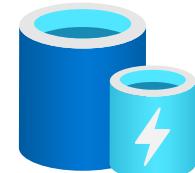
Co-scheduled groups



Virtual network deployment



Linux
and
Windows containers



Persistent storage

ACI Security

Aqua

Continuously scan registry images

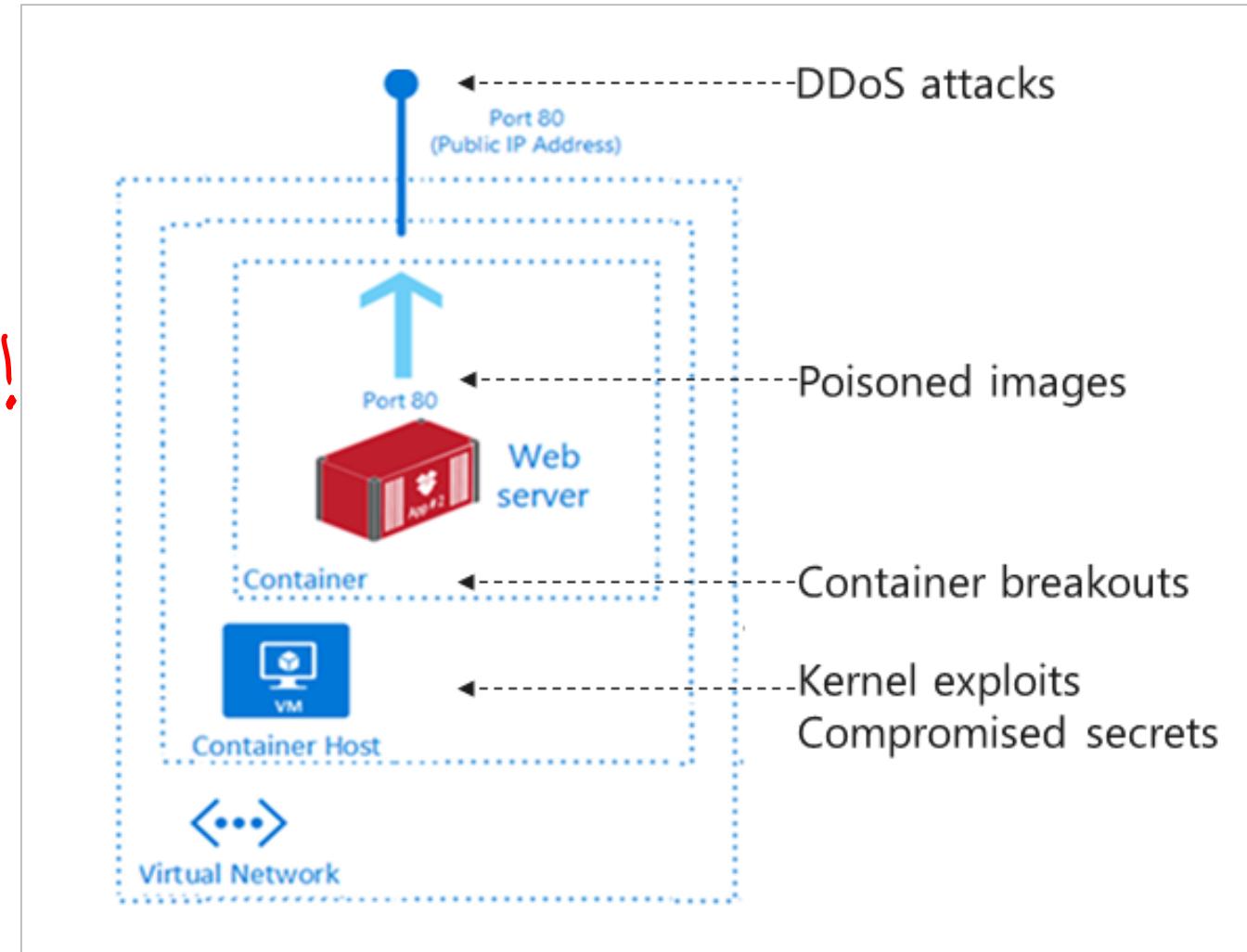
Use approved images – chain of custody, signing

Run with least privileges *non root!*

"Allow List" files the container can access

Maintain network segmentation

Monitor and log activities



ACR Authentication

Method	How to authenticate	Scenarios	Azure role-based access control (Azure RBAC)	Limitations
Individual AD identity <u> </u>	<code>az acr login</code> in Azure CLI <code>Connect-AzContainerRegistry</code> in Azure PowerShell	Interactive push/pull by developers, testers	Yes	AD token must be renewed every 3 hours
AD service principal <u> </u>	<code>docker login</code> <code>az acr login</code> in Azure CLI <code>Connect-AzContainerRegistry</code> in Azure PowerShell <code>Registry login settings in APIs or tooling</code> <code>Kubernetes pull secret</code>	Unattended push from CI/CD pipeline Unattended pull to Azure or external services	Yes	SP password default expiry is 1 year
Managed identity for Azure resources	<code>docker login</code> <code>az acr login</code> in Azure CLI <code>Connect-AzContainerRegistry</code> in Azure PowerShell	Unattended push from Azure CI/CD pipeline Unattended pull to Azure service	Yes	Use only from select Azure services that support managed identities for Azure resources

Note: Require authentication for all operations – unauthenticated access is not supported.

ACR Authentication – Cont'd

Method	How to authenticate	Scenarios	Azure role-based access control (Azure RBAC)	Limitations
AKS cluster managed identity	Attach registry when AKS cluster created or updated	Unattended pull to AKS cluster in the same or a different subscription	No, pull access only	Only available with AKS cluster Can't be used for cross-tenant authentication
AKS cluster service principal	Enable when AKS cluster created or updated	Unattended pull to AKS cluster from registry in another AD tenant	No, pull access only	Only available with AKS cluster
Admin user	docker login	Interactive push/pull to repository by individual developer or tester Unattended pull from repository by individual system or external device	Yes	Single account per registry, not recommended for multiple users
Repository-scoped access token	docker login az acr login in Azure CLI Connect-AzContainerRegistry in Azure PowerShell Kubernetes pull secret	Interactive push/pull to repository by individual developer or tester Unattended pull from repository by individual system or external device	Yes	Not currently integrated with AD identity

Note: Require authentication for all operations – unauthenticated access is not supported.

Brendan Burns → CloudShell
ACI

Azure Kubernetes Service (AKS)

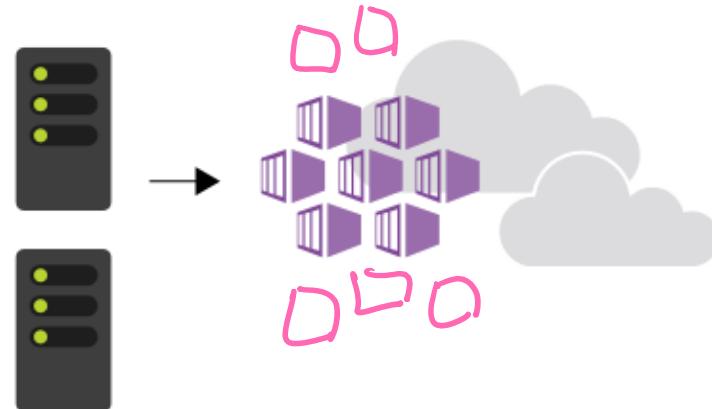
Portable, extensible open-source platform for automating deployment, scaling, and the management of containerized workloads.

Fully managed

Public IP and FQDN (Private IP option)

Accessed with RBAC or Azure AD

Micro Services



Dynamic scale containers

Automation of rolling updates and rollbacks of containers

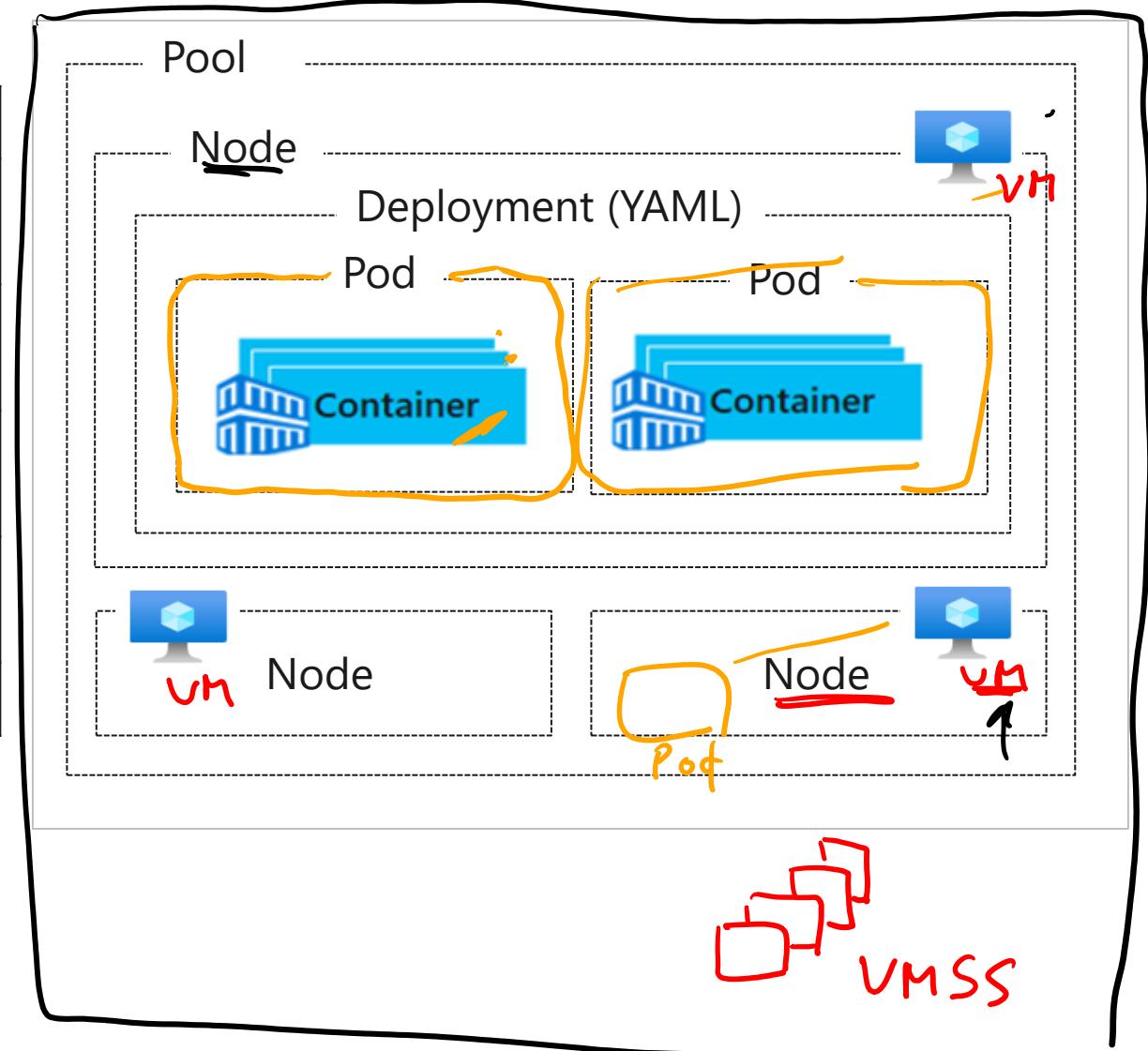
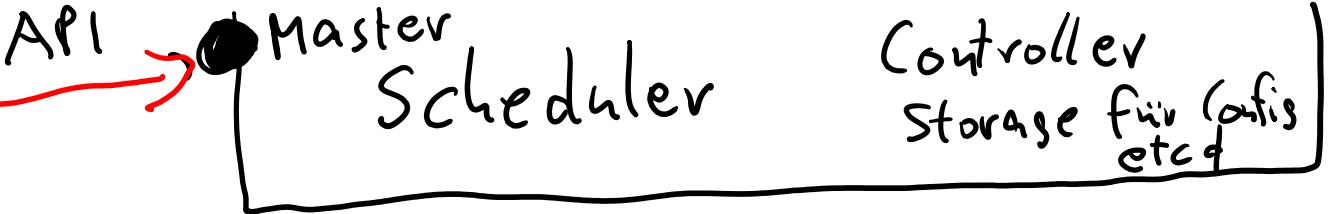
Management of storage, network traffic, and sensitive information

AKS Terminology

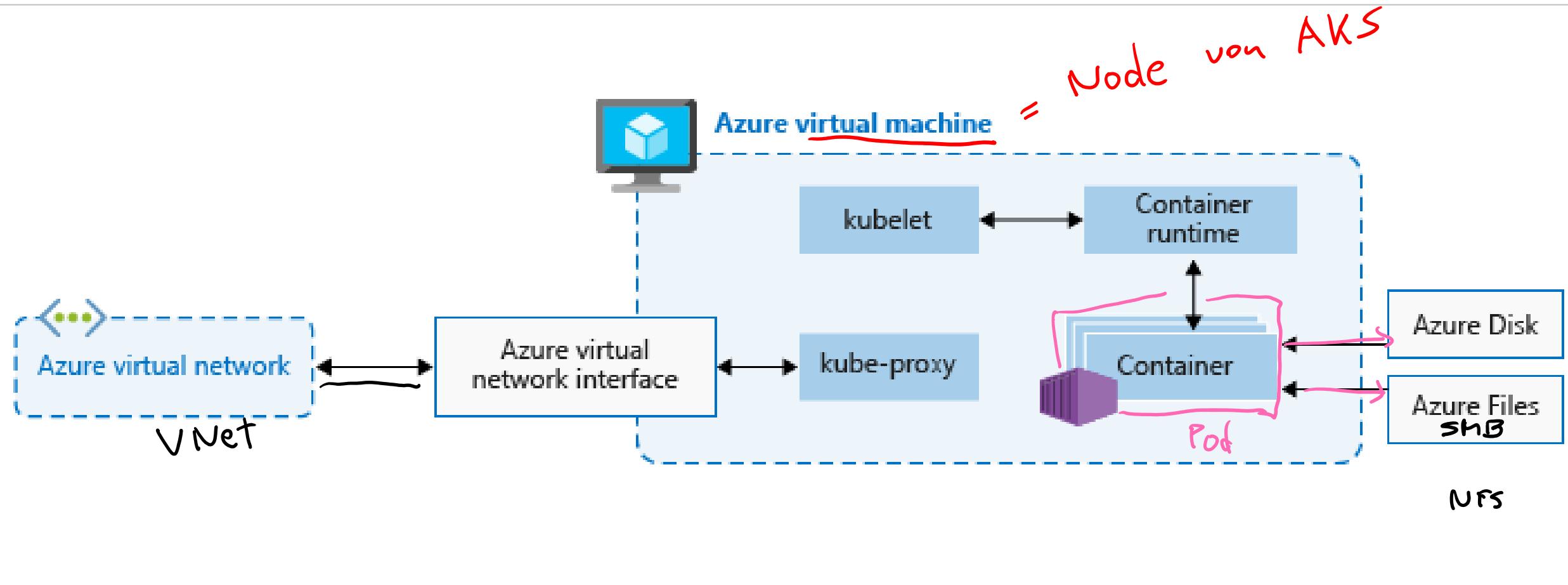
Term	Description
Pools	Groups of nodes with identical configurations.
Nodes	Individual VM running containerized applications.
Pods	Single instance of an application. A pod can contain multiple containers.
Deployment	One or more identical pods managed by Kubernetes.
Manifest	YAML file describing a deployment

=Template

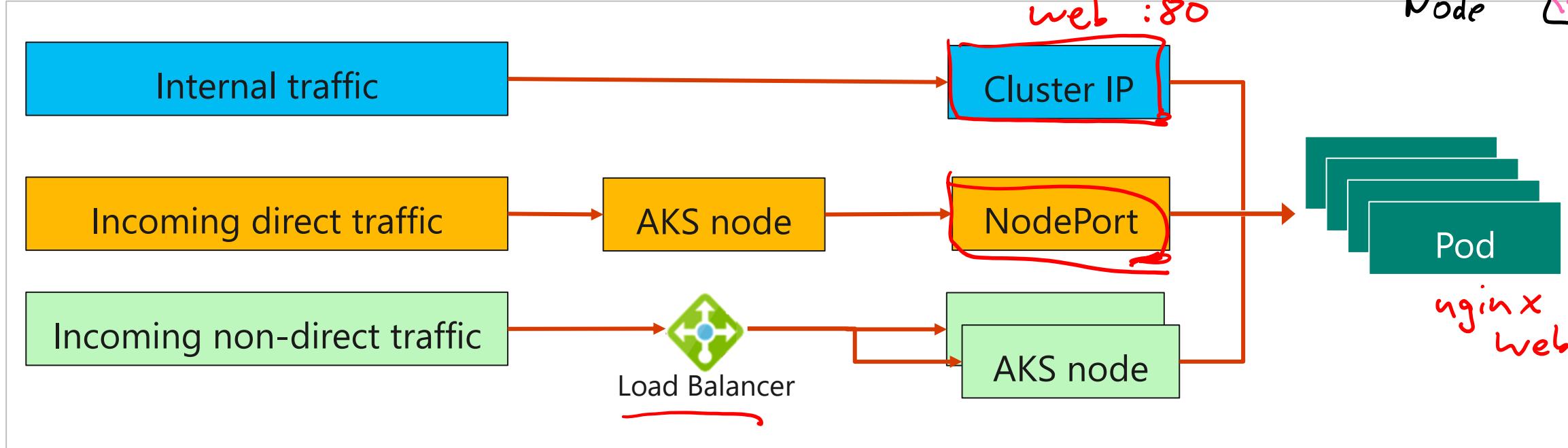
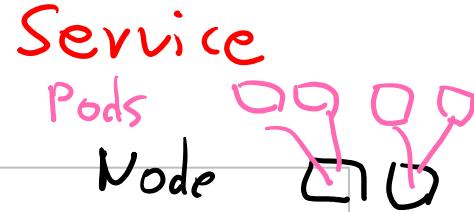
Semper idem!



AKS Architecture



AKS Networking



Pods run an instance of your application

Services group pods together to provide network connectivity

Cluster IP provides internal traffic access

NodePort provides mapping for incoming direct traffic

Load balancer has external IP address for incoming non-direct traffic

AKS Storage

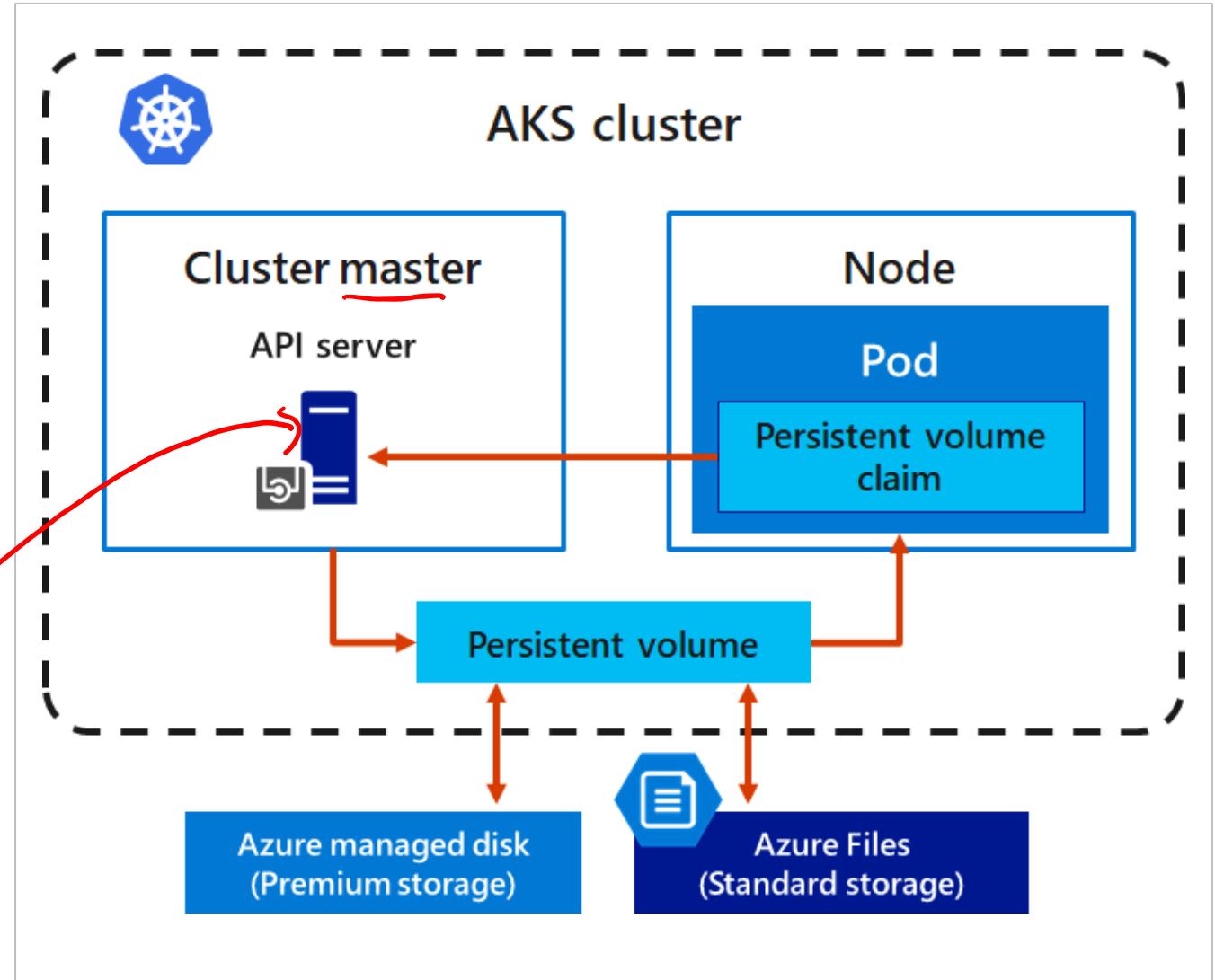
Local storage on the node is fast and simple to use

Local storage might not be available after the pod is deleted

Multiple pods may share data volumes

Storage could potentially be reattached to another pod

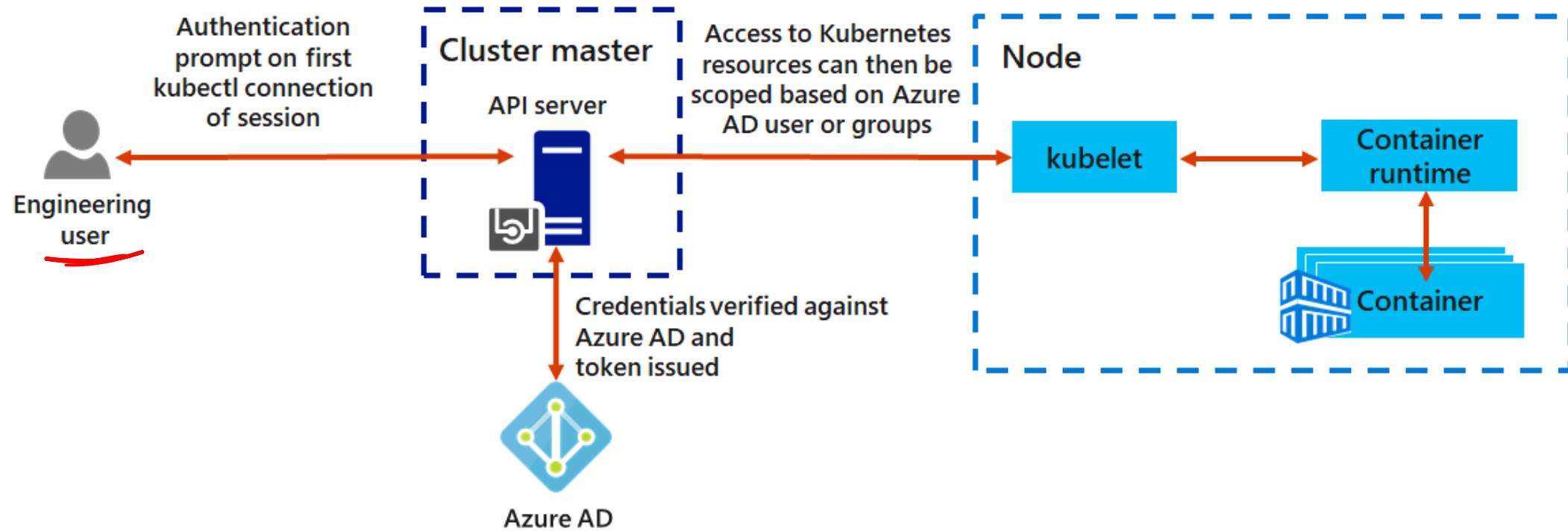
Kubectl
yaml



AKS security capabilities

Authentication and authorization		Network security
<ul style="list-style-type: none">• Azure AD integration with Azure Kubernetes Service• <u>Azure RBAC, Kubernetes RBAC</u>• Headless services and applications use Service Principals / Managed Identities		<ul style="list-style-type: none">• Deploy private AKS cluster – API server only has private IP addresses• NSG, Firewall to control the traffic to/from AKS nodes• Use Kubernetes Network Policy to secure traffic between pods• Protect data – Least privilege RBAC, Azure Key Vault

AKS and Azure Active Directory

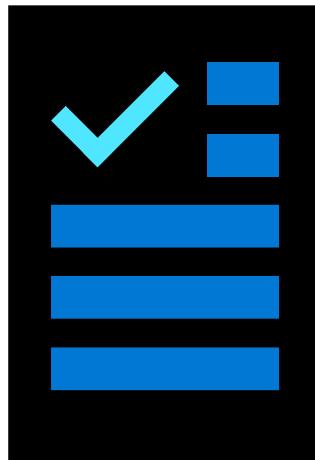


Use Azure AD as an integrated identity solution

Use service accounts, user accounts, and role-based access control

Additional Study – Container Security

Module Review Questions



Microsoft Learn Modules (docs.microsoft.com/Learn)

Core Cloud Services - Azure compute options

Build and store container images with Azure Container Registry (Exercise)

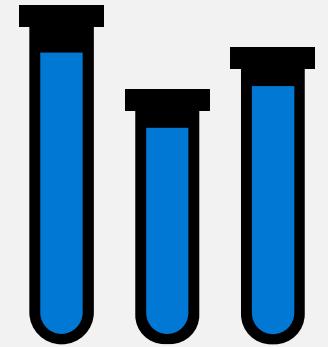
Build a containerized web application with Docker (Exercise)

Introduction to Docker containers

Run Docker containers with Azure Container Instances (Exercise)

Azure Kubernetes Service Workshop (Exercise)

Module Labs



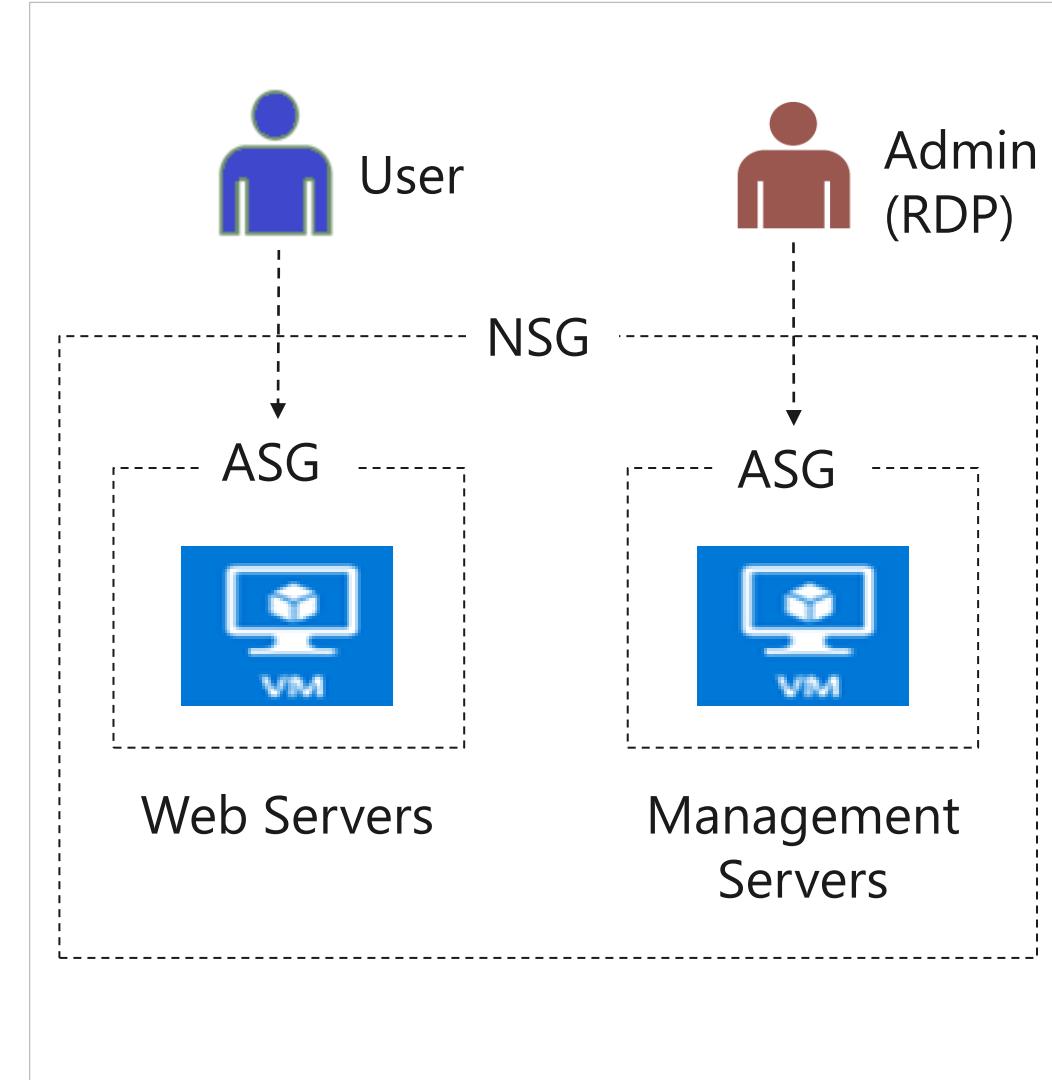
Lab 07 – Network and Application Security Groups

Create application security groups

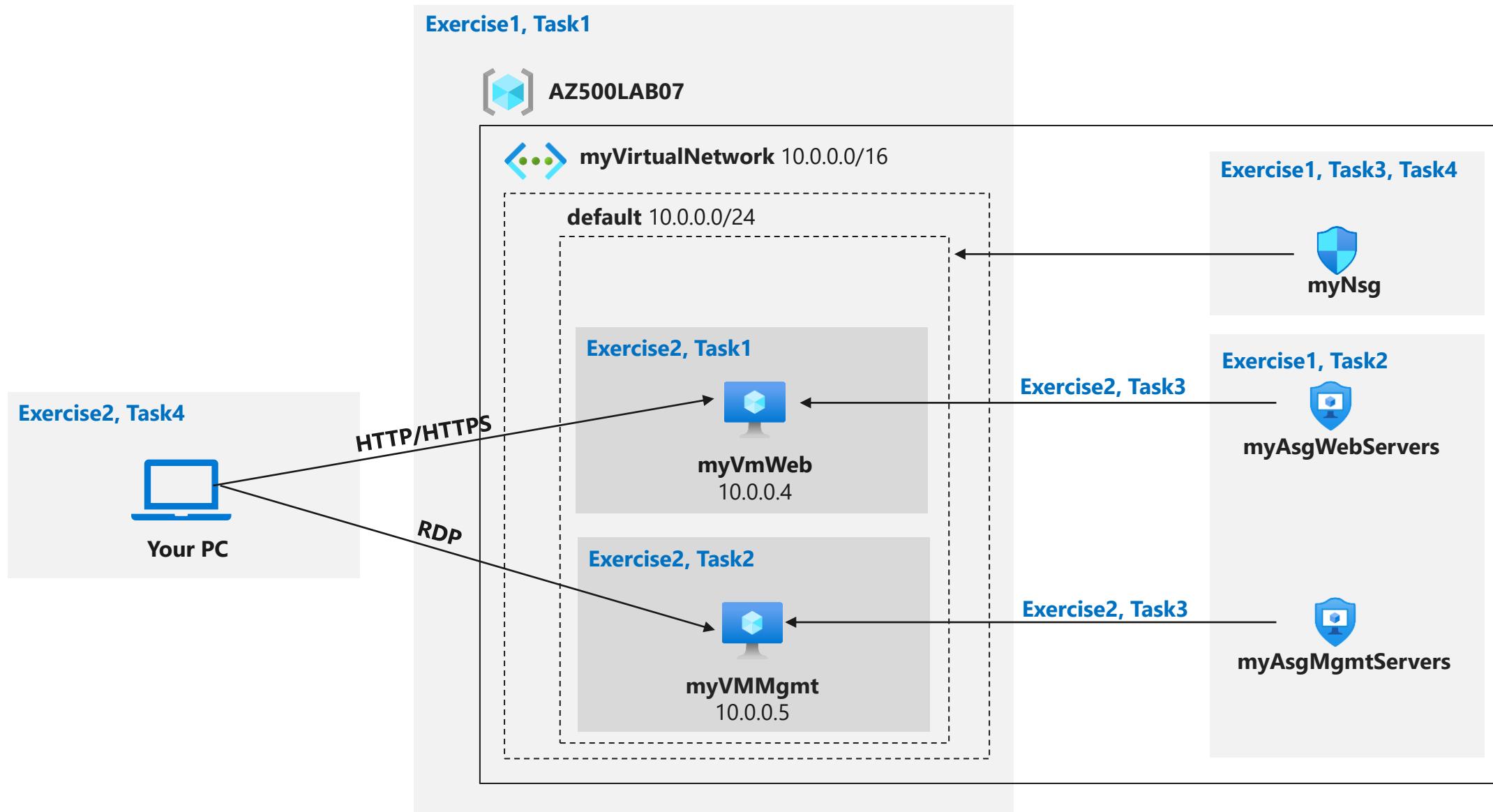
Wrap the ASGs with a Network Security Group (NSG)

Use NSG rules to route traffic:

- Admins can RDP to the management servers but not the web servers
- Users can access the web servers and see the default IIS page



Lab 07 – Network and Application Security Groups



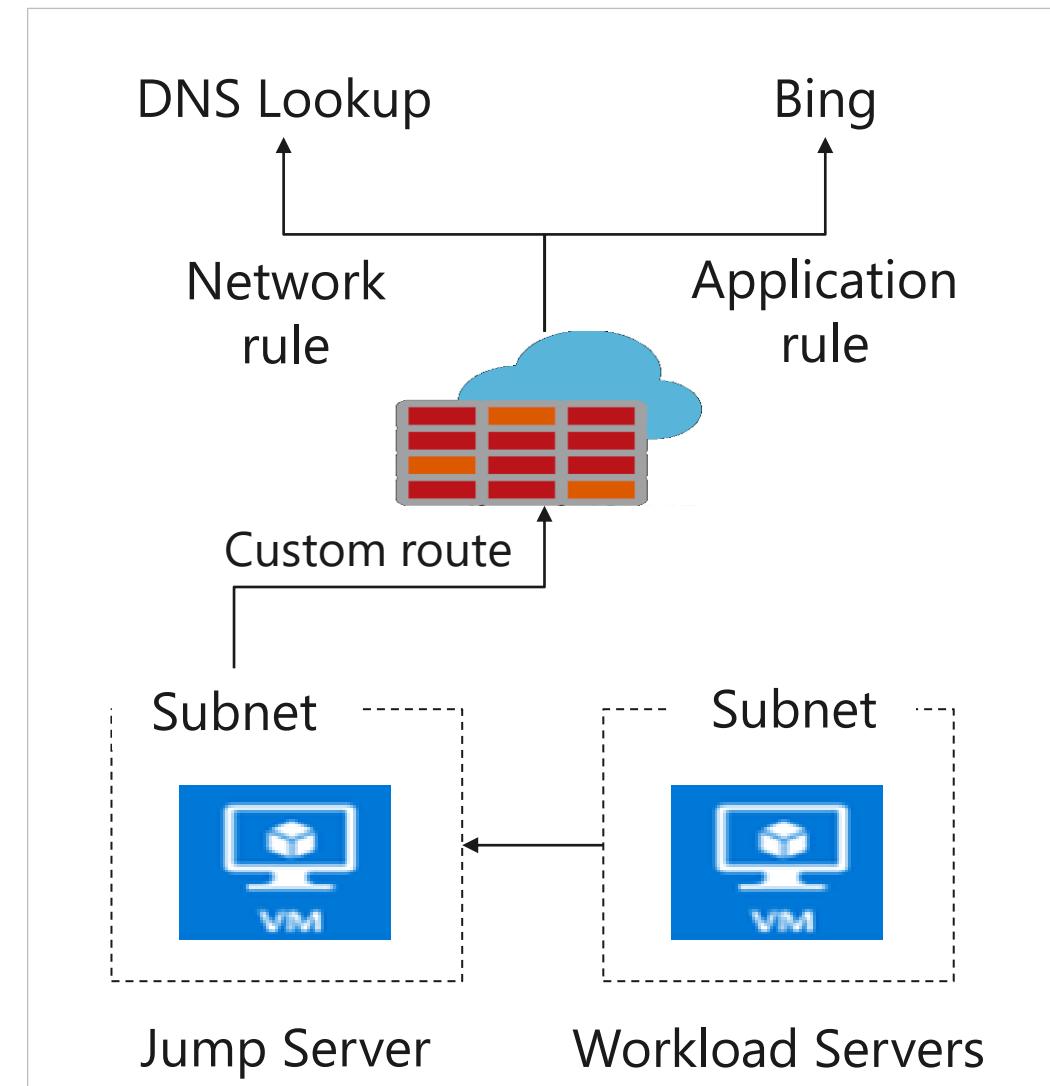
Lab 08 – Azure Firewall

Create a Workload subnet and Jump subnet each with a virtual machine

Create a custom route to ensure outbound traffic from the workload subnet goes to the firewall

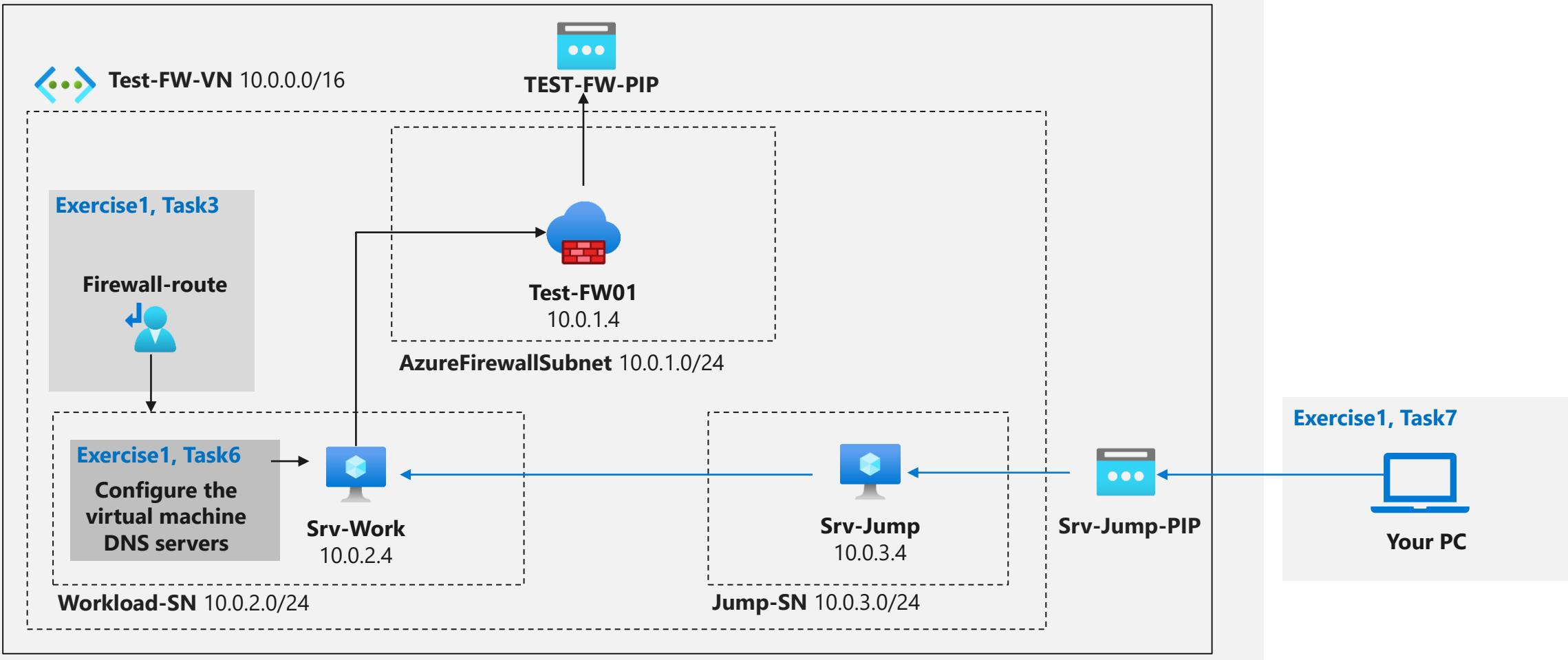
Create firewall application rules to allow traffic to Bing

Create firewall network rules to allow traffic to DNS lookup servers



Lab 08 – Azure Firewall

Exercise1, Task1



Lab 09 – Configuring and Securing ACR and AKS

Create an Azure Container Registry

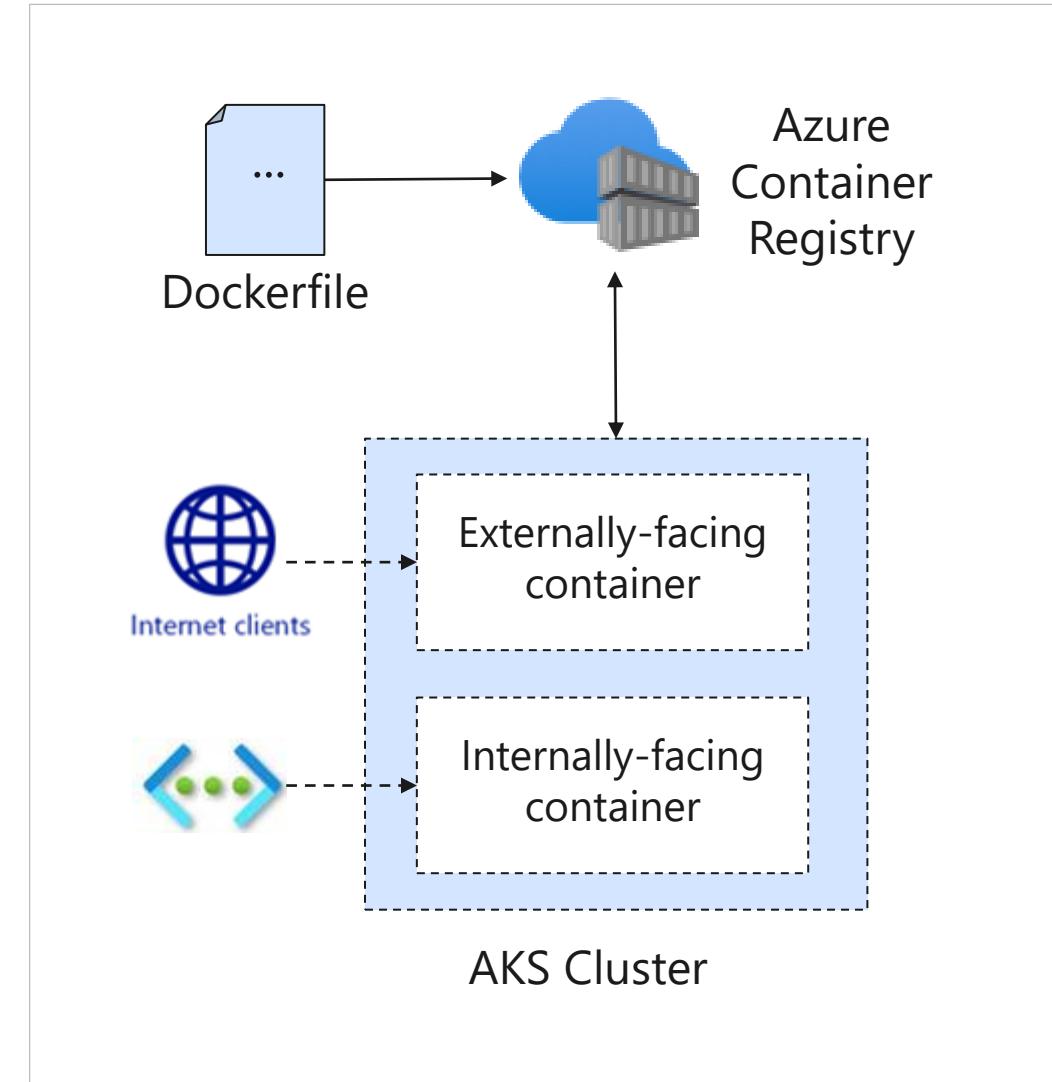
Create a Dockerfile, build a container and push it to ACR

Create an Azure Kubernetes Service

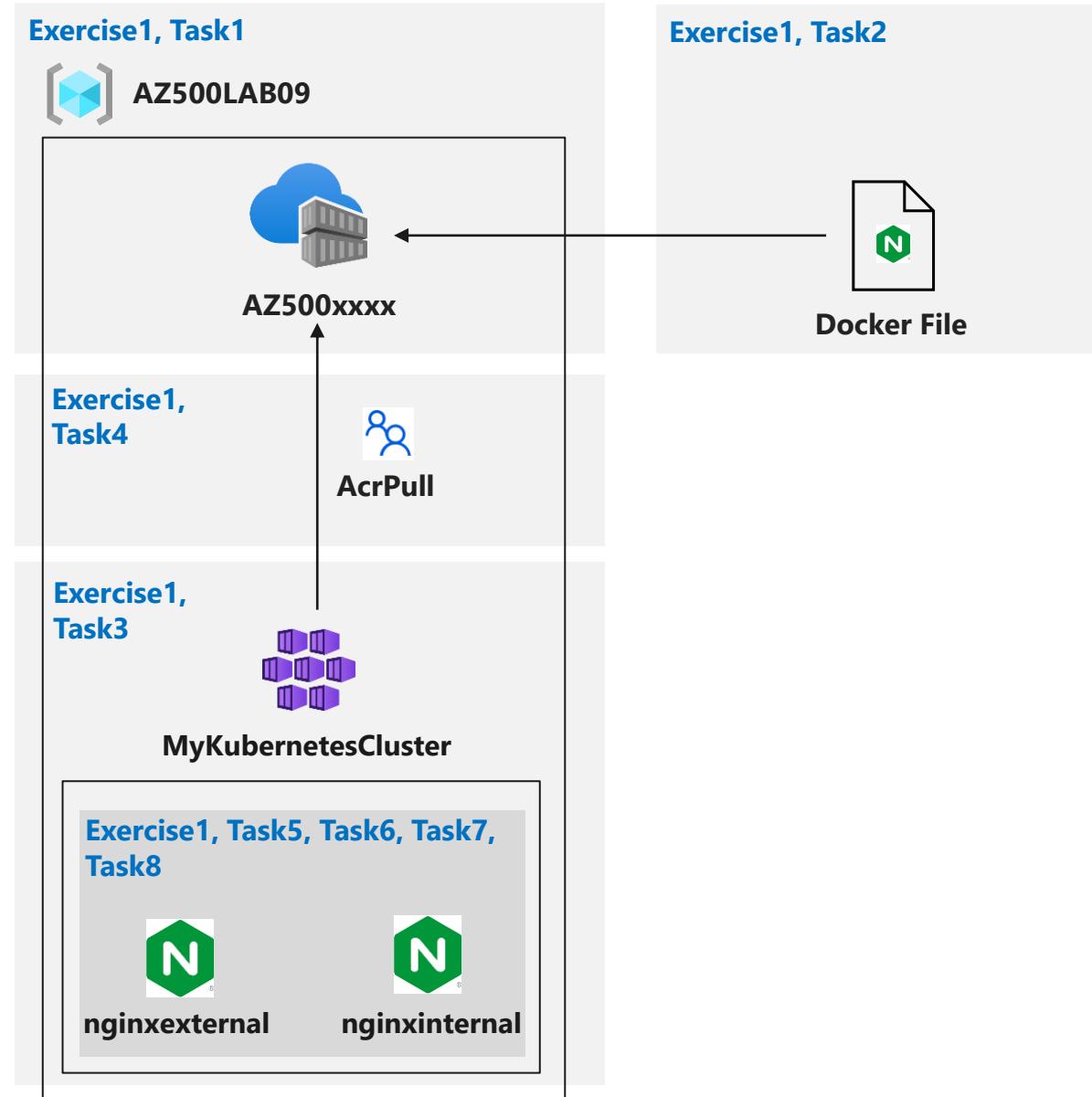
Give AKS permission to access the ACR

Deploy an external facing container and test

Deploy an internal facing container and test



Lab 09 – Configuring and Securing ACR and AKS



End of presentation