WELCOME to Today’s Session

- Sit tight. We will start shortly.
- Mute your phone.
- Register your Attendance via link in chat window.
- Prepare to participate via chat and annotations.

AZ-301 TSI Exam Preparation

MARK O'SHEA

MICROSOFT MVP, MCT

Today’s Session

There will be a 15-minute break 75-90 minutes into the session

At the end of each section I’ll review the questions/comments in chat before proceeding, and leave time for additional Q&A

If you have found resources that have helped you understand a topic, share them with others via chat

VM Scale Sets

Templated Infrastructure

While ARM templates are an excellent resource, for large scale deployments, other solutions are available:

VM Scale Sets allow true auto scaling to deploy big compute and big data solutions

Virtual Machine Scale Sets

Scale sets have a number of features:

- Deployable with JSON templates just like VMs
- Can use Azure Autoscale
- No requirement to pre-provision
- Load balancer creation
- NAT included

Virtual Machines vs. Virtual Machine Scale Sets

Scale Sets:

- Easy to grow and shrink on demand
- Easy to reimage
- Easy to overprovision
- Upgrade policies

VMs:

- Attach disks to VMs
- Attach non-empty disks
- Snapshot a VM
- Capture a VM Image
- Migrate from native to managed disks
- Assign IPv6 public IP addresses to individual VM NICs

Virtual Machine Scale Sets

- Connect to an Instance of a VM using RDP through the load balancer

- Use Continuous delivery to maintain an application in a VMSS with Visual Studio Team Services

- Using managed disks removes storage account considerations from Scale Set creation

Virtual Machine Scale Set Considerations

- Custom Extensions can be used to configure new VM instances when scaling – this can add time to the deployment

- Custom Images can be used to deploy all images to the scale set – this scales VMs in a ready to use state

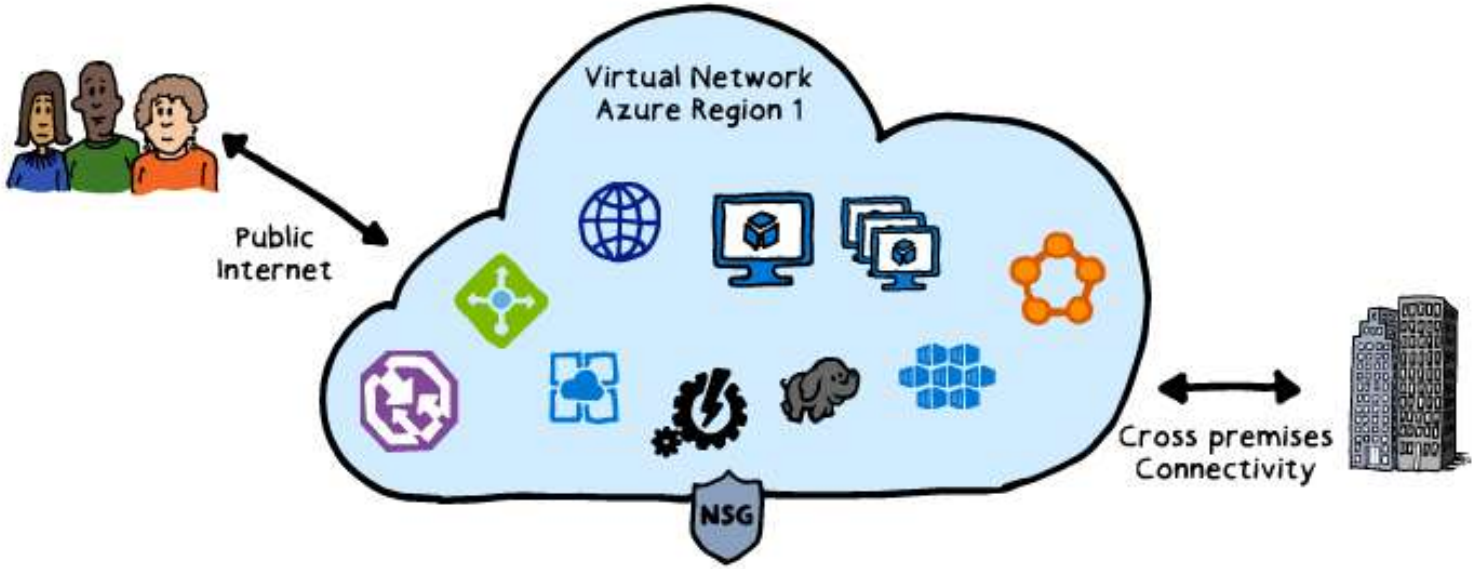
Considerations for “Large” VMSS

Large scale sets over 100 VMs use placement groups – these change load balancing and fault domain characteristics:

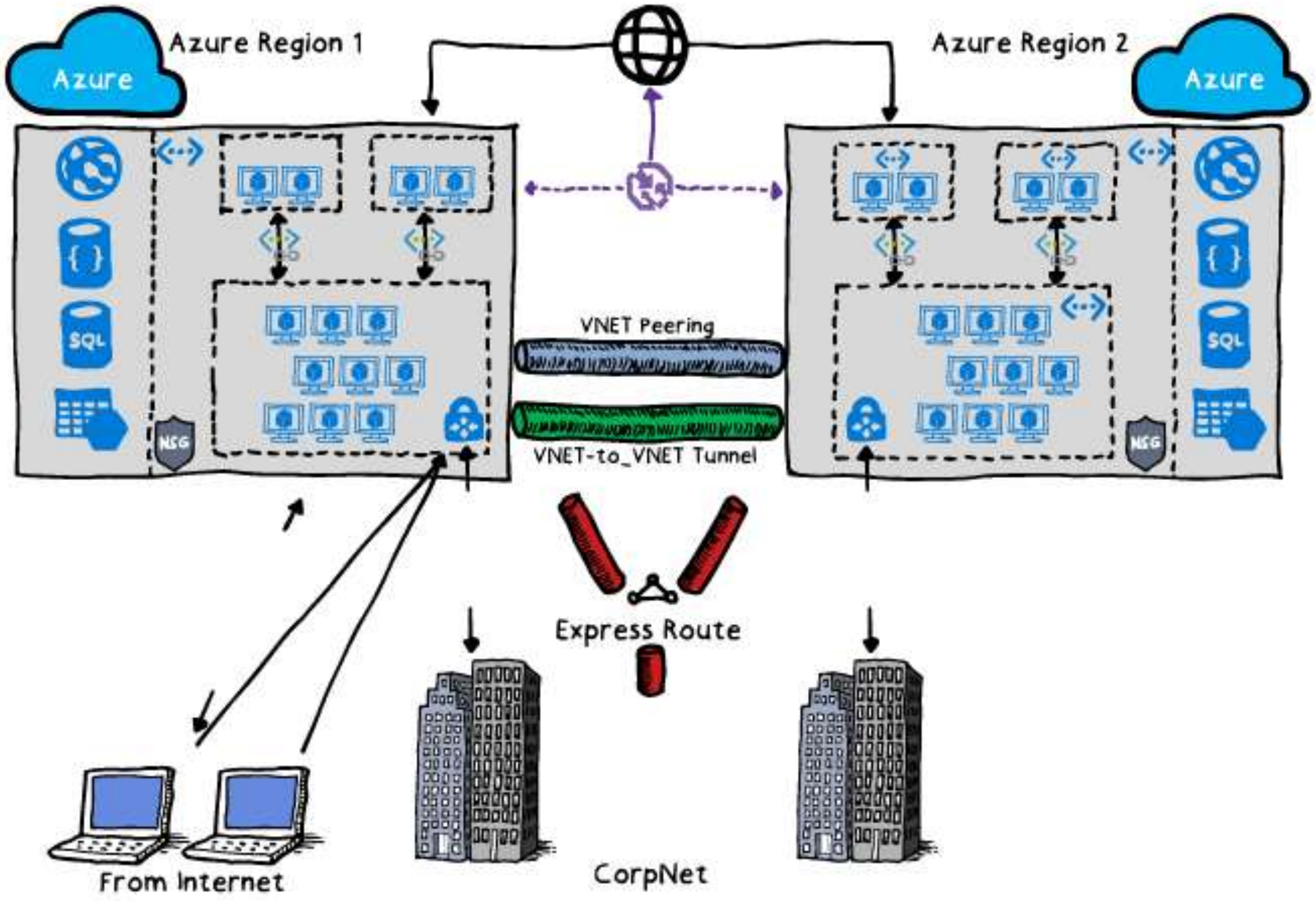
- Managed Disks
- Marketplace images scale to 1,000 VMs
- Custom images scale to 300 VMs
- Ensure available IP addresses in subnet
- Ensure your compute limits are high enough
- Fault Domains relate to a single placement group

Networking Azure Application Components

Azure Virtual Network (VNET) Architecture



Multi-Region Virtual Network Architecture



Multi-Region Virtual Network Architecture

- Traffic Manager provides DNS based traffic distribution & failover across Azure Regions
- IAAS & PAAS VNet inter-communication
- Isolate VM workloads in SubNets/Vnet
- ExpressRoute and/or S2S VPN for CorpNet connectivity or Azure-to-Azure Region traffic
- NSGs secure the in/outgoing traffic on VNet or NIC level

VNETs & Subnets

- Networking Topology:
  - Define 1 or more VNets within an Azure Region, and configure an address space for each
  - Define 1 or more SubNets within a VNet, and configure address space within the VNet range
  - VNets and SubNets are using CIDR notation (x.x.x.x/24, x.x.x.x/16,…)
  - Configure Network Security Group settings on VNet level
  - Attach a NIC to a SubNet

- SubNet IP Addressing:
  - IP-address gets allocated to a NIC during provisioning of the NIC
  - First available IP-address in a SubNet range is x.x.x.4
  - Azure SubNets support dynamic (=default) and static IP addressing

Public & Private IP-addressing

- Public IP-addressing:
  - Used for all public internet-facing communication
  - Required parameter when creating a VM from the portal

- Private IP-addressing:
  - Used for all inter-VNet communication
  - Used for all communication between an Azure VNet and an on-premises VNet

Azure DNS Resolving

- DNS Server settings are configured on VNET level
- Use Azure DNS (Default)
- Or use your custom DNS configuration:
  - Azure DNS Appliance (from Azure MarketPlace)
  - Azure VM (e.g. Windows ADDS with DNS)
  - On-premises DNS solution (requires connectivity)

- Public DNS names (available for VMs and App Services) must be unique across Azure regions:

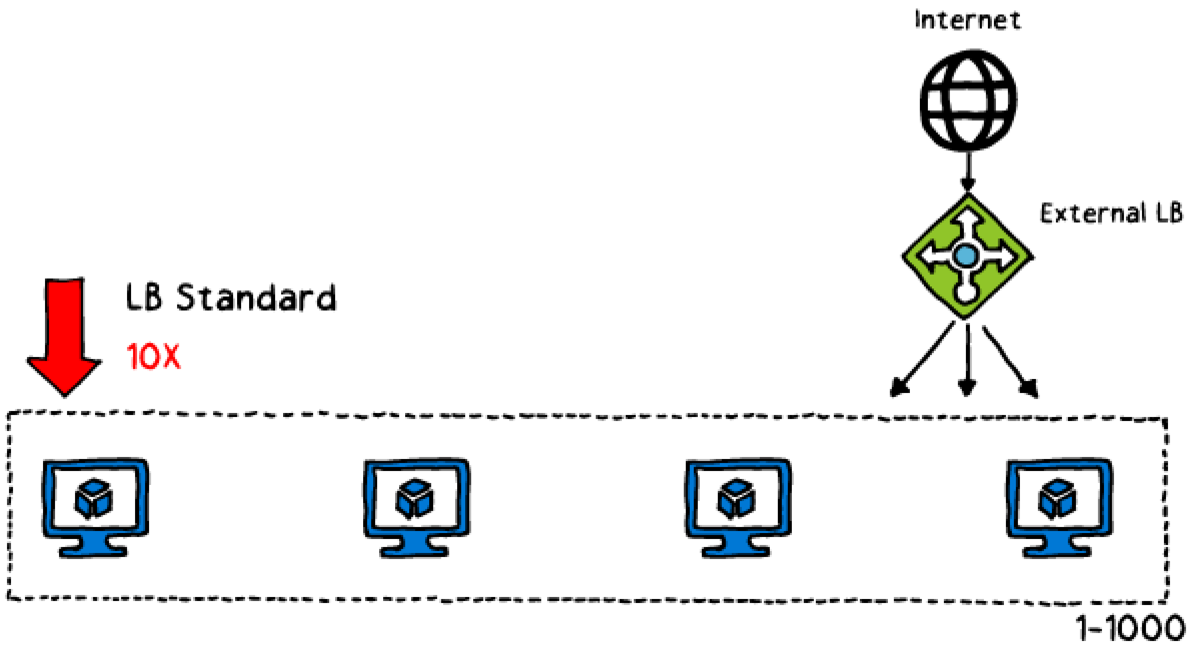
  <host.region.cloudapp.azure.com>

Load Balancing Solutions

- Azure Load Balancer (layer 4)
- Azure Application Gateway (layer 7)
- Azure MarketPlace Load Balancing Appliance (layer 7)
- Azure Traffic Manager (DNS-based)

Azure Load Balancer

- Load balancer with a Public IP-address, sending traffic along to the back-end pool servers
- TCP, UDP traffic
- Azure Platform management
- Support for Availability Sets



Load Balancer Basic

Load Balancer Basic can be used for most load balancing scenarios:

Basic
Up to 100 backend instances
Non-zonal frontend
Availability Set (single)
Basic NAT and Probe health status
NSG optional
Free

Load Balancer Standard

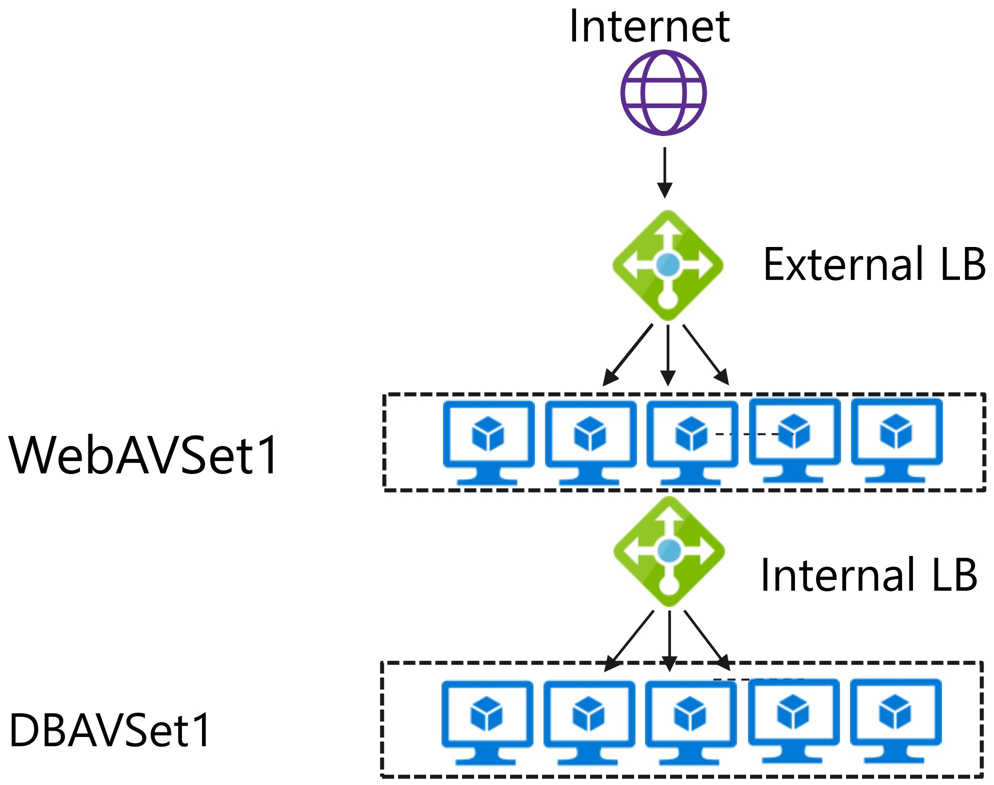
You can use Load Balancer Standard for TCP & UDP scenarios with:

- Larger scale
- Greater flexibility
- HA Ports
- New metrics
- Availability zones

Standard
Up to 1000 backend instances
Zone-redundant frontend Zonal frontend
Availability Sets not required and Availability Zones
Integrated Frontend and Backend health metrics
Supports HA Ports
NSG required

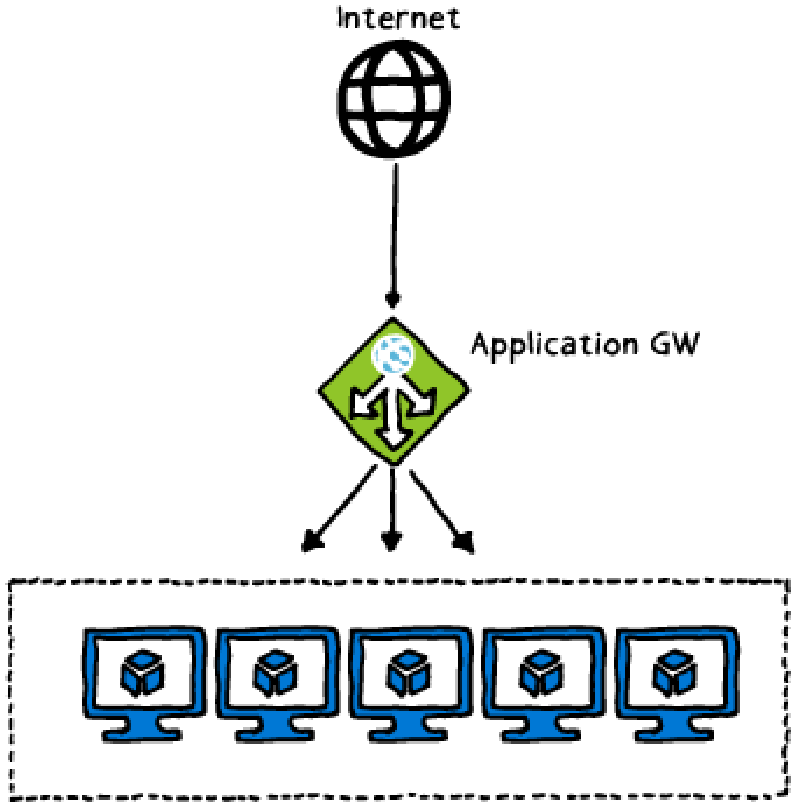
Internal Load Balancer

- Load balancer with a Private IP-address, sending traffic along to the back-end pool servers
- TCP, UDP traffic
- Azure Platform management

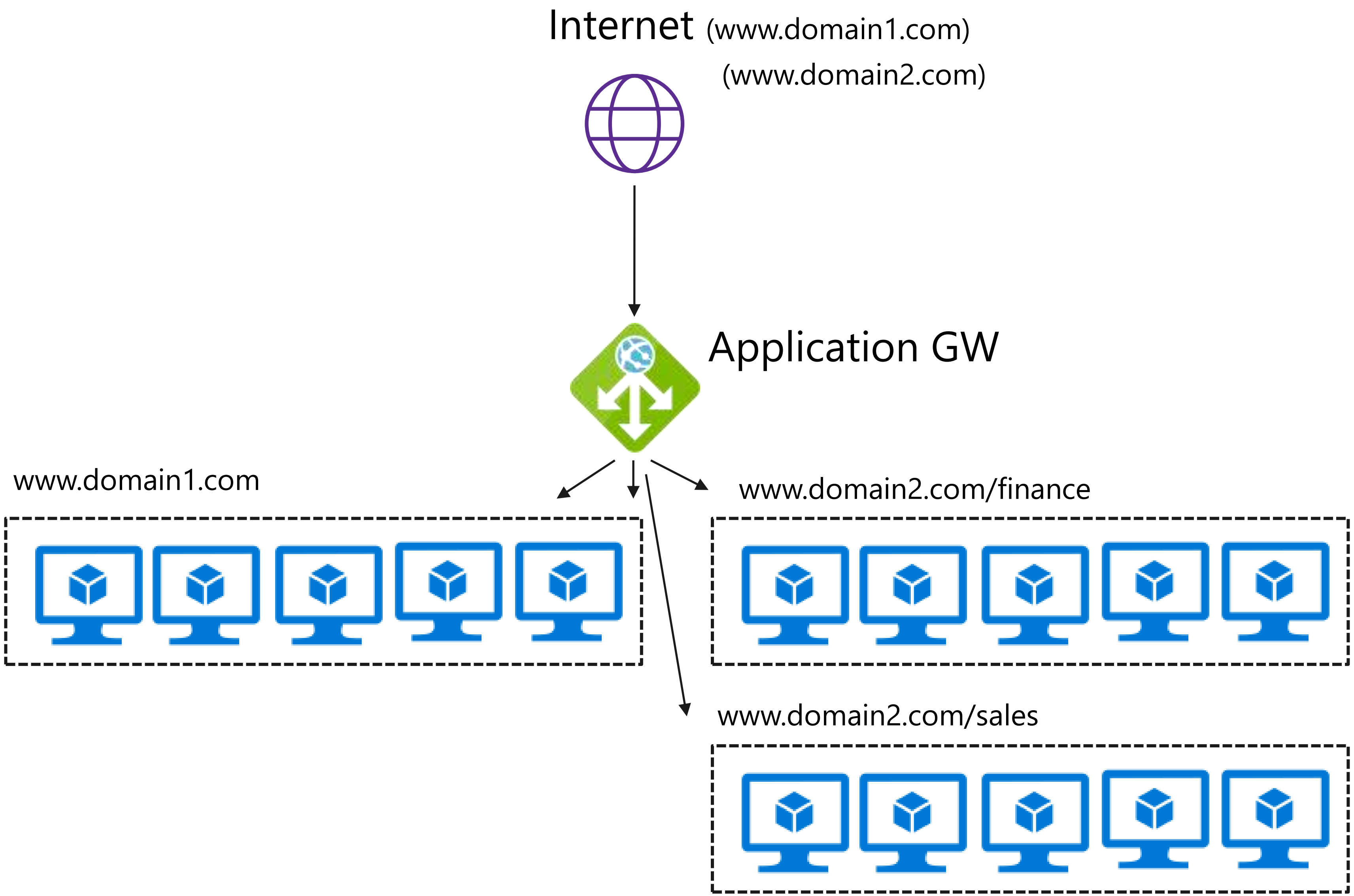


An Azure Load Balancer cannot both be external and internal

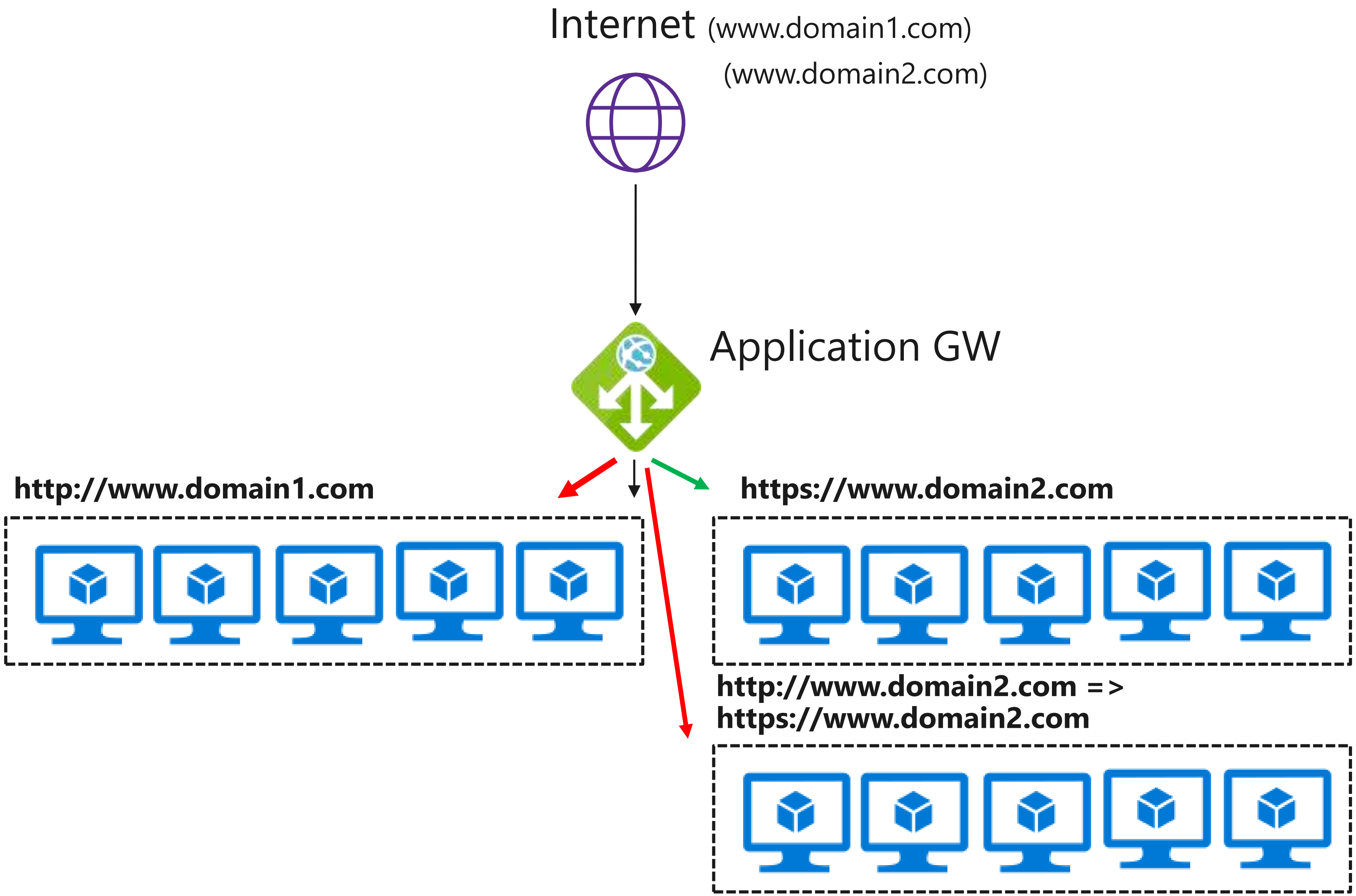
Azure Application Gateway



URL-based Routing



SSL Termination



Internet (www.domain1.com)

(www.domain2.com)

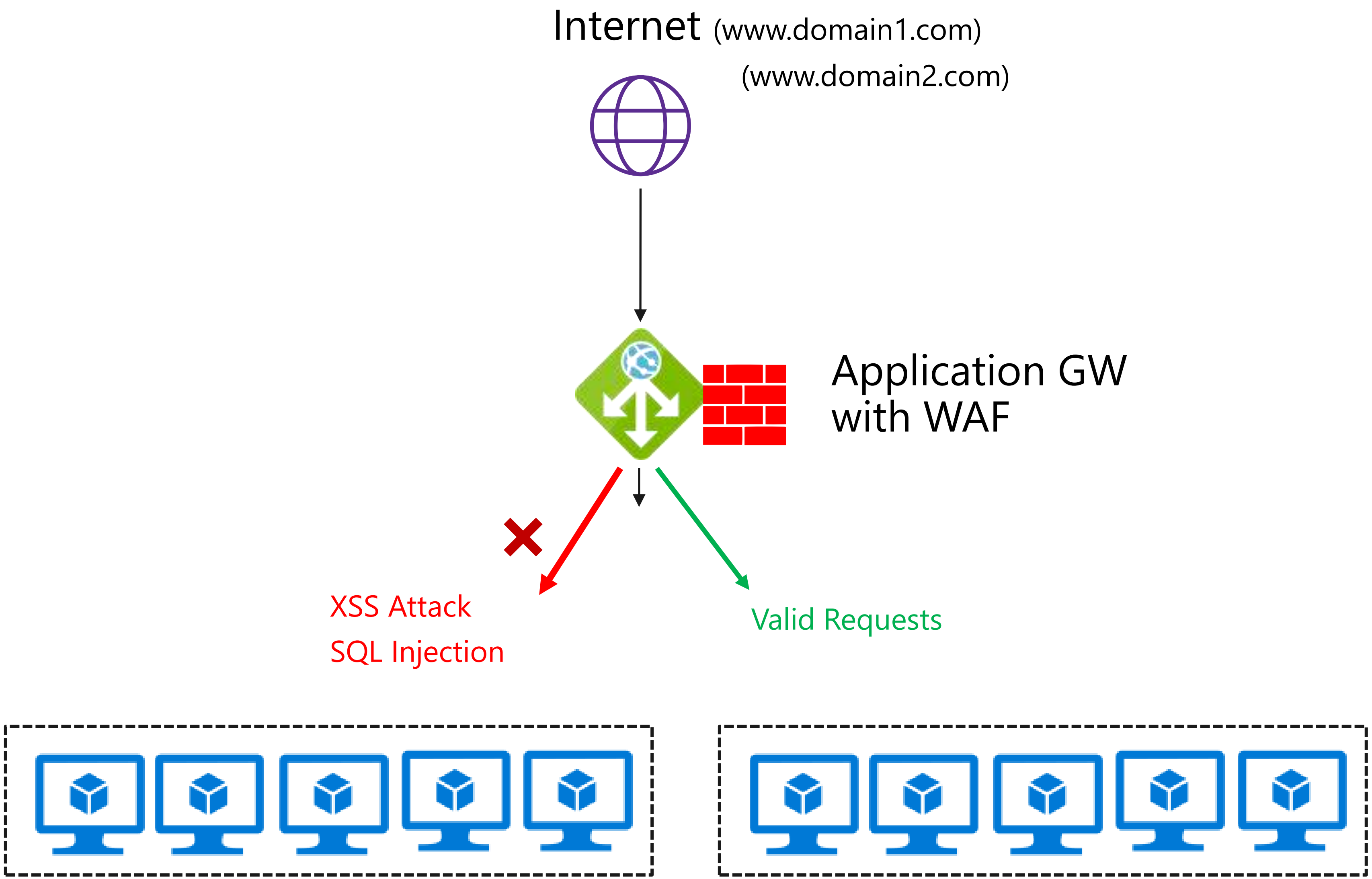
Application GW

http://www.domain1.com

https://www.domain2.com

http://www.domain2.com => https://www.domain2.com

Web Application Firewall (WAF)



Internet (www.domain1.com)

(www.domain2.com)

Application GW with WAF

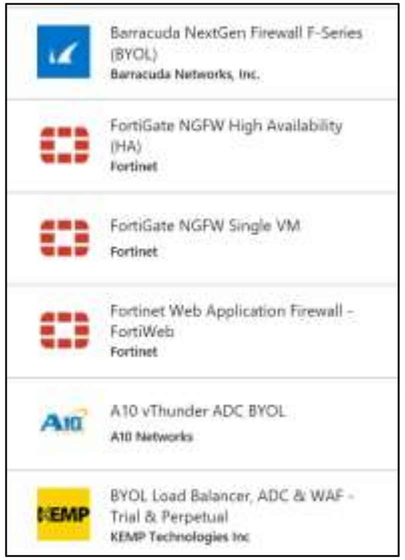
XSS Attack

SQL Injection

Valid Requests

Azure Load Balancing Marketplace Appliances

- Preconfigured vendor VM appliances, supported by Azure
- BYOL or Pay-per-use
- Can be an alternative for Azure Platform provided options



Barracuda NextGen Firewall F-Series (BYOL)
Barracuda Networks, Inc.

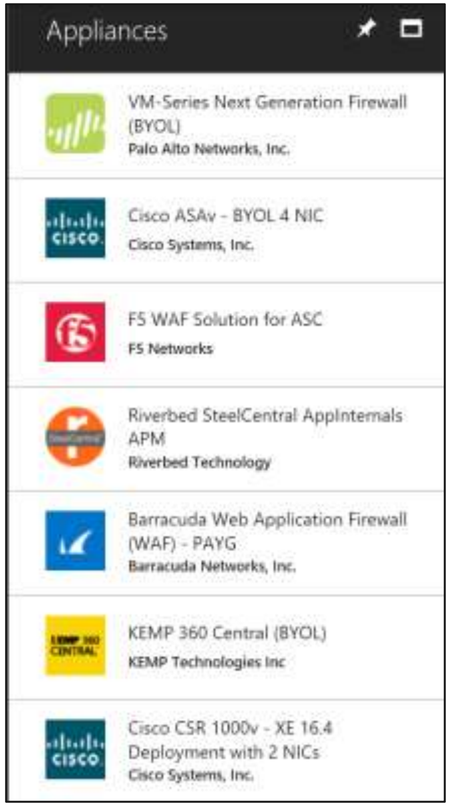
FortiGate NGFW High Availability (HA)
Fortinet

FortiGate NGFW Single VM
Fortinet

Fortinet Web Application Firewall - FortiWeb
Fortinet

A10 vThunder ADC BYOL
A10 Networks

BYOL Load Balancer, ADC & WAF - Trial & Perpetual
KEMP Technologies Inc



Appliances

VM-Series Next Generation Firewall (BYOL)
Palo Alto Networks, Inc.

Cisco ASAv - BYOL 4 NIC
Cisco Systems, Inc.

F5 WAF Solution for ASC
F5 Networks

Riverbed SteelCentral AppInternals APM
Riverbed Technology

Barracuda Web Application Firewall (WAF) - PAYG
Barracuda Networks, Inc.

KEMP 360 Central (BYOL)
KEMP Technologies Inc

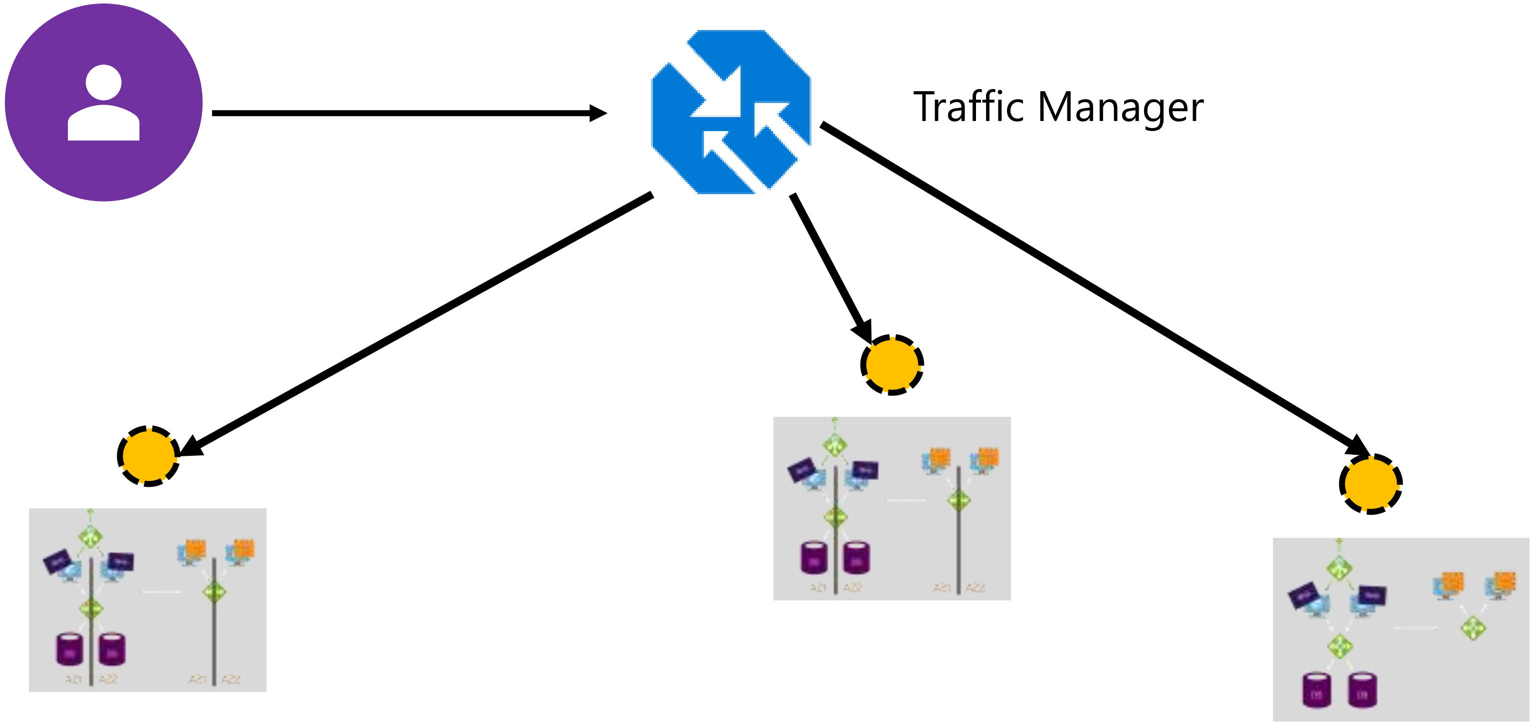
Cisco CSR 1000v - XE 16.4 Deployment with 2 NICs
Cisco Systems, Inc.

Azure Traffic Manager

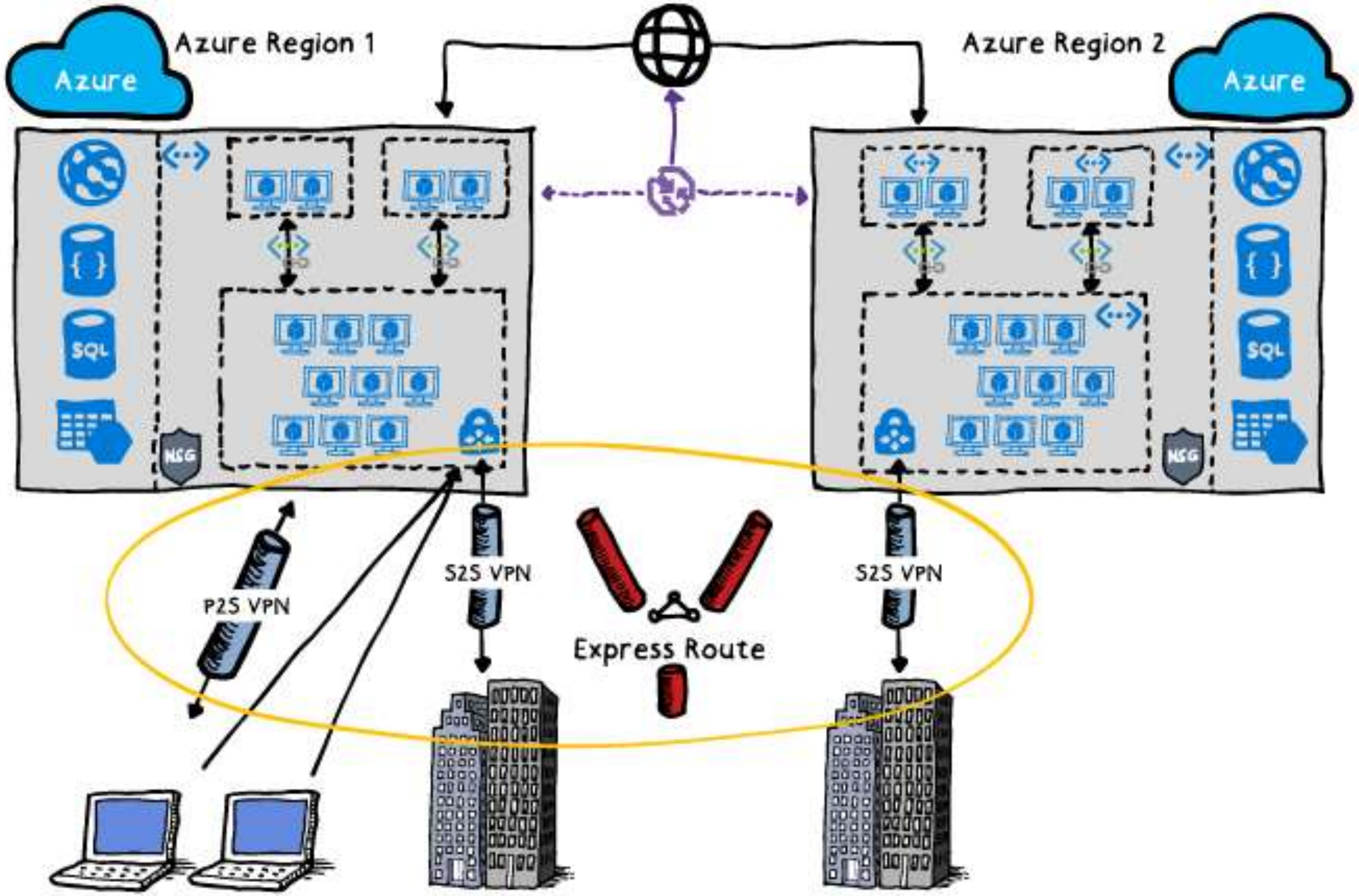
Global Resiliency and Performance, based on DNS

4 Load Balancing options:

- Priority
- Weighted Round Robin
- Geographical
- Performance



On-Premises to Azure Connectivity



Connectivity Options

Connectivity	Benefits
ExpressRoute	• ExpressRoute as primary cross-premises connectivity • Multiple circuits for redundancy & better routing • ExpressRoute-VPN co-existence for highly available, redundant paths
Site-to-Site VPN	• S2S VPN over Internet for remote branch locations • BGP & active-active configuration for HA and transit
Point-to-Site VPN	• P2S VPN for mobile users & developers to connect from anywhere with macOS & Windows • AD/radius authentication for enterprise grade security

High-Performance VPN Gateway SKUs

Scenarios:

- High throughput, hybrid workload over VPN tunnels
- Failover from ExpressRoute circuits to S2S VPN tunnels
- P2S for dev/test connectivity from anywhere

SKU	Workload	Throughput	S2S/V2V	P2S	SLA
VpnGw1	Production	650 Mbps	Max. 30	128	99.95%
VpnGw2	Production	1 Gbps	Max. 30	128	99.95%
VpnGw3	Production	1.25 Gbps	Max. 30	128	99.95%
Basic	Dev/Test	100 Mbps	Max. 10	128	99.9%

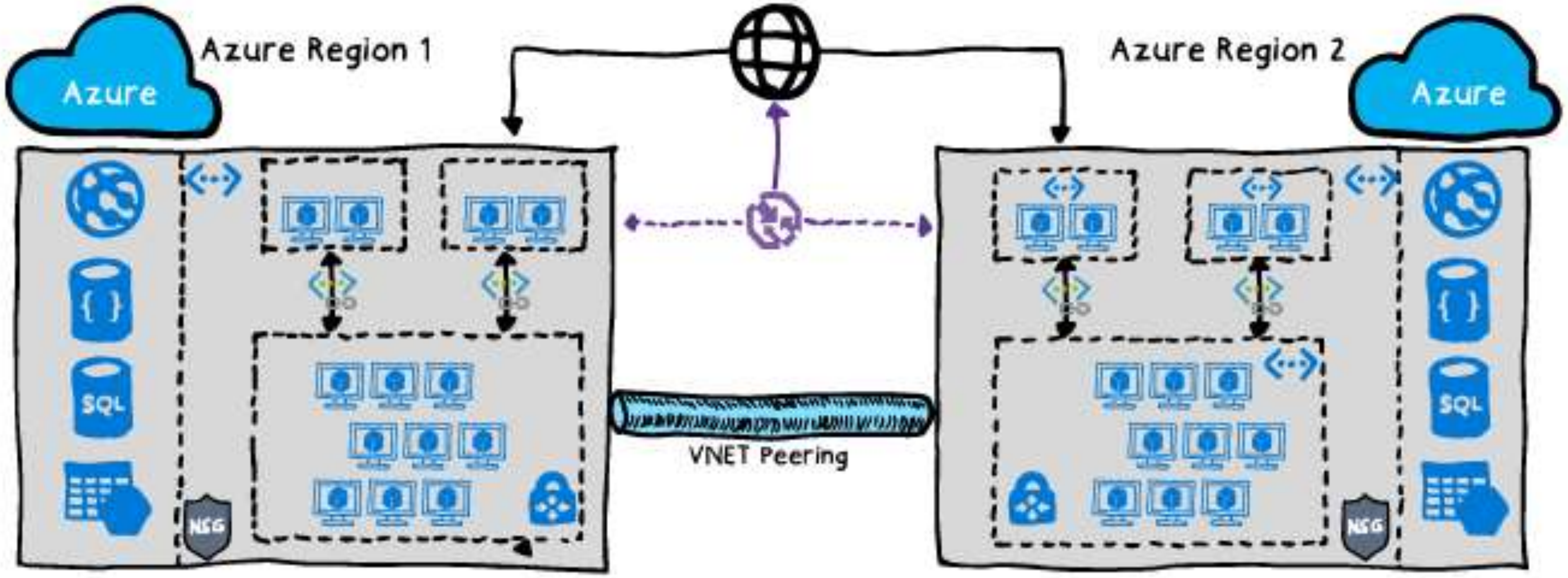
VNET Peering

- VNET Peering allows you to interconnect 2 Azure VNETs, as if they are 1 large VNET

- VNET Peering is possible within the same Azure region, or across Azure regions (using MS Backbone, no public internet)

- VNET Peering is supported to interconnect an Azure Classic VNET with an ARM VNET (e.g., for migrating workloads)

VNet Peering

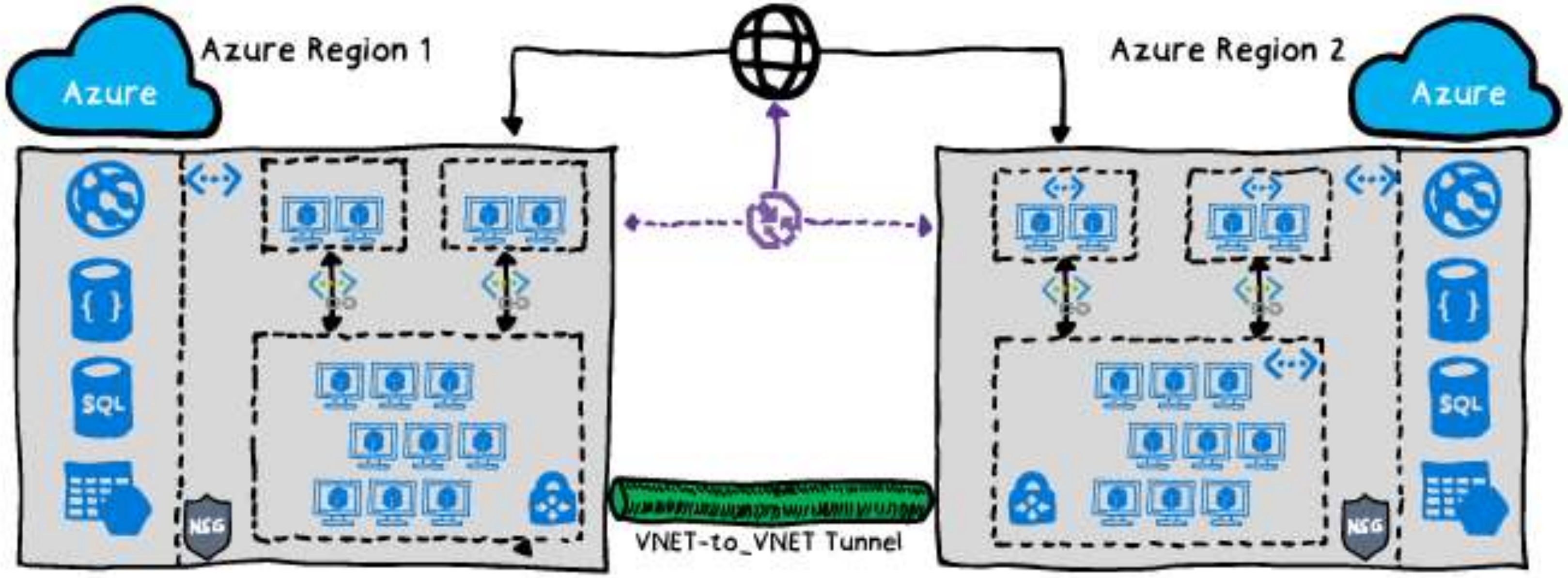


Multi-Region VPN Connectivity

- Before Vnet Peering, the only possible way to interconnect 2 Azure Regions, was Site-to-Site VPN Gateway tunneling

- This is still a valid option, if your traffic between both Azure regions must be encrypted (outside of the already encrypted Microsoft Backbone, no public internet)

Multi-Region VPN Connectivity

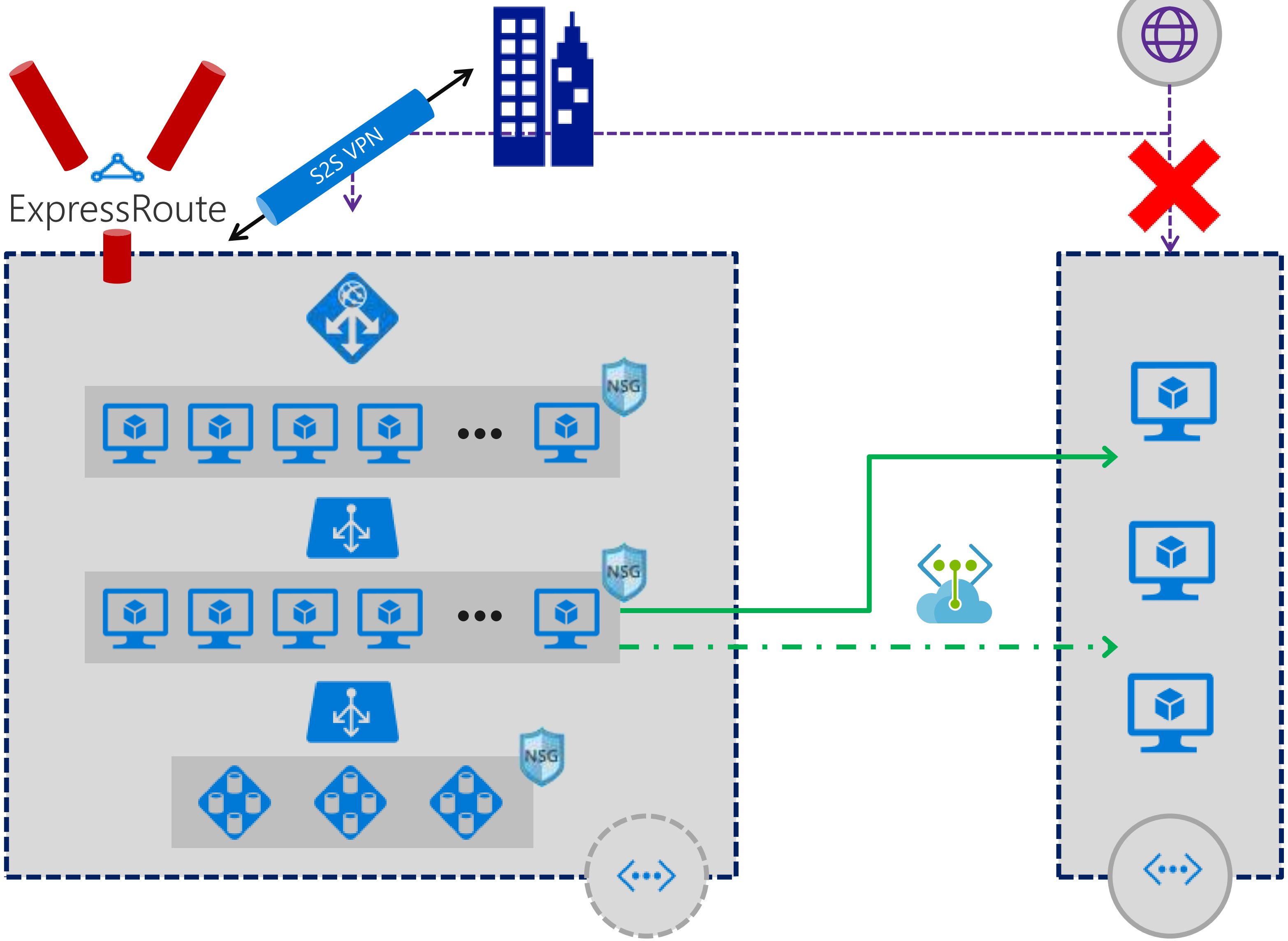


Forced Tunneling

- Challenges:
  - IaaS services accessible through internet
  - Customers may require their VMs to be only accessed from on-premises VNET

- Solution—Forced Tunneling:
  - IaaS services only accessible from a VNET
  - Site-to-Site VPN
  - Or ExpressRoute

Forced Tunneling

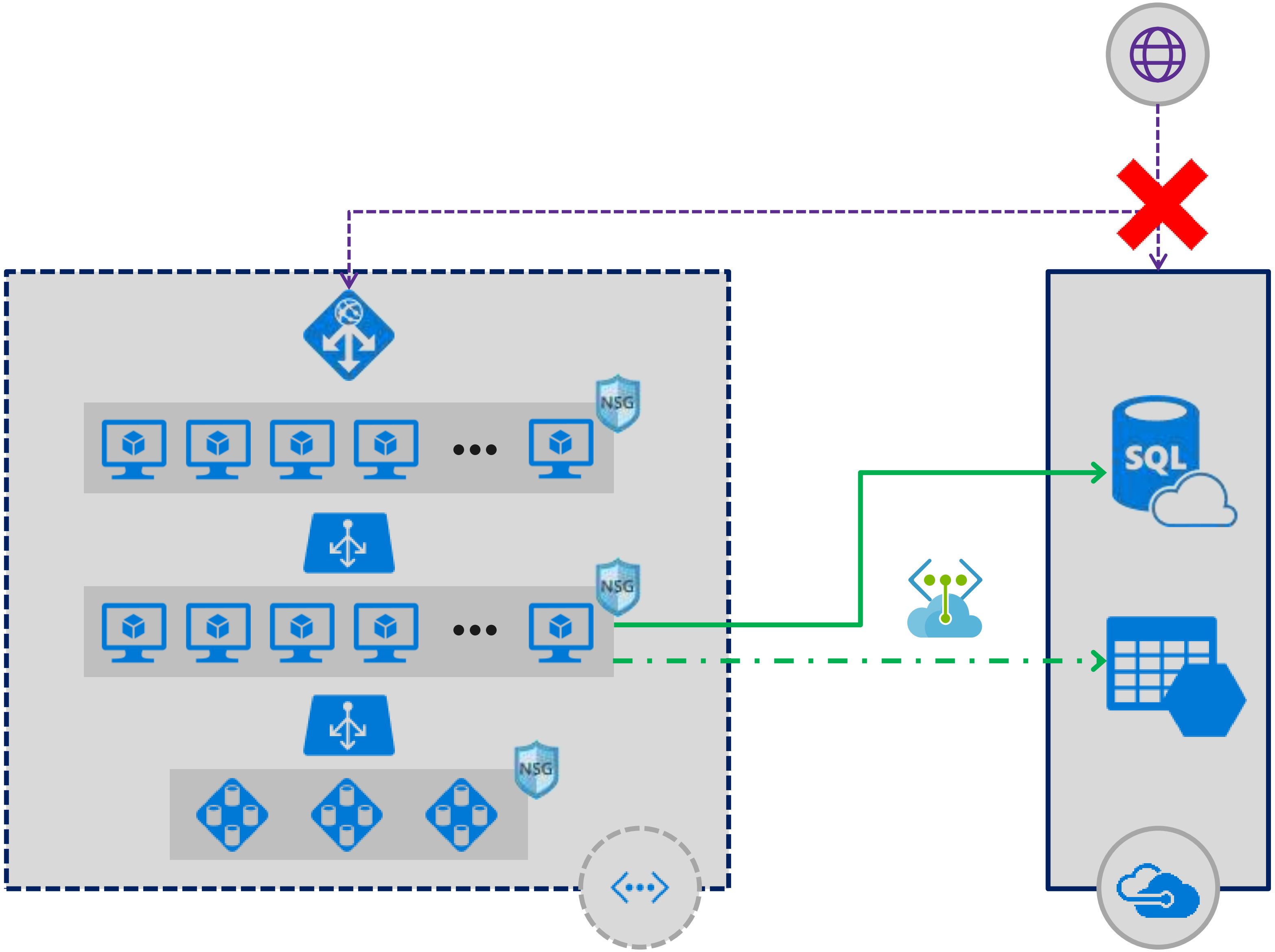


Securing Access to PaaS Services

- Challenges:
  - PaaS services accessible through internet
  - Customers may require their services endpoints to be only accessed from their VNETs

- Solution—VNEt Service Endpoints:
  - PaaS services only accessible from a VNET
  - Available now for Storage and SQL DB
  - Will roll out to other PaaS services in the future

Securing Access to PaaS Services



Network Security Groups

- A network security group (NSG) is a top level object that is associated to your subscription:
  - It can be used to control traffic to one or more virtual machine (VM) instances in your virtual network
  - An NSG contains access control rules that allow or deny traffic to VM instances
  - The rules of an NSG can be changed at any time, and changes are applied to all associated instances

Default Inbound Rules

NAME	PRIORITY	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	PROTOCOL	ACCESS
ALLOW VNET INBOUND	65000	VIRTUAL_NETWORK	*	VIRTUAL_NETWORK	*	*	ALLOW
ALLOW AZURE LOAD BALANCER INBOUND	65001	AZURE_LOADBALANCER	*	*	*	*	ALLOW
DENY ALL INBOUND	65500	*	*	*	*	*	DENY

Default Outbound Rules

NAME	PRIORITY	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	PROTOCOL	ACCESS
ALLOW VNET OUTBOUND	65000	VIRTUAL_ NETWORK	*	VIRTUAL_ NETWORK	*	*	ALLOW
ALLOW INTERNET OUTBOUND	65001	*	*	INTERNET	*	*	ALLOW
DENY ALL OUTBOUND	65500	*	*	*	*	*	DENY

Backing Azure Solutions With Azure Storage

Azure Storage

Azure provides a variety of storage features

Storage, like other services is provided in differing performance and cost levels. In addition, storage is broken down into four discrete services provided within Storage Accounts:

- Blobs
- Tables
- Queues
- Files

Azure Storage Accounts

Storage accounts are further split into General Purpose and Blob Storage

Type of Account	General Purpose Standard	General Purpose Premium	Blob Storage (hot and cool access tiers)
Services Supported	Blob, File, Queue services	Blob service	Blob service
Types of Blobs supported	Block blobs, Page blobs and Append blobs	Page blobs	Block blobs and Append blobs

Storage Account Security

Storage accounts can be secured by Azure AD or by Shared Access Signatures:

- Azure AD RBAC controls management functions when applied to a Storage Account
- Azure AD RBAC can be used to read data objects when applied to storage account keys
- Shared Access Signatures and Stored Access Polices further secures data objects to dates times and permissions
- Azure Storage can be accessed by any HTTP/HTTPS requests and has multiple storage libraries for popular languages

Storage Account Replication

Storage account replication can be changed after creation except for Zone Redundant Storage (ZRS)

Replication	LRS	ZRS	GRS	RA-GRS
Data stored in multiple datacenters	No	Yes	Yes	Yes
Data read from secondary & primary location	No	No	No	Yes
No of copies of data stored in separate nodes	3	3	6	6

Data transfer costs my be incurred if you change from Locally redundant storage (LRS) to Geo redundant storage (GRS) - this would be a one time cost

Storage Performance & Pricing

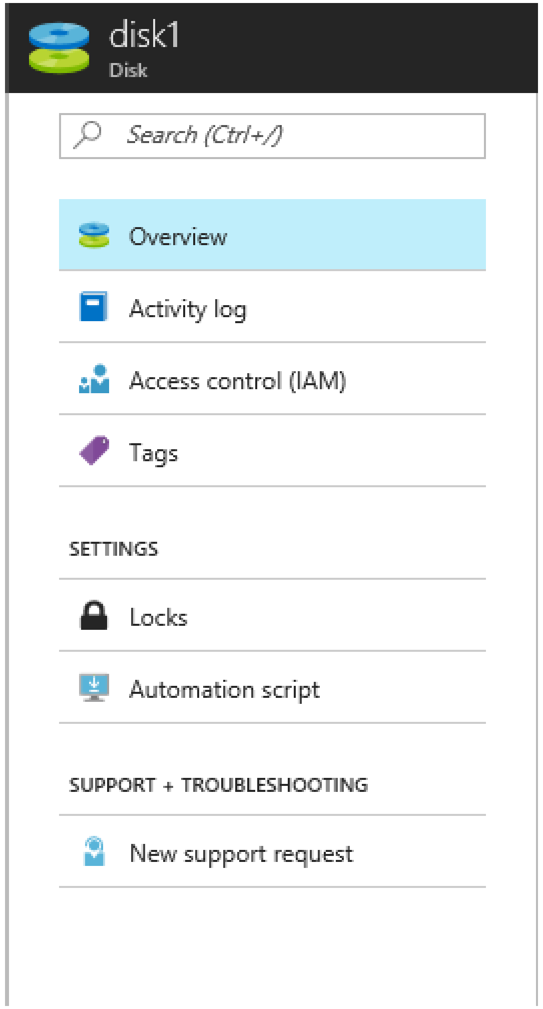
Premium Storage is:

- For page blobs and VM Disks
- Only available as a Locally Redundant storage account
- Only available for certain VM series

Blob Storage

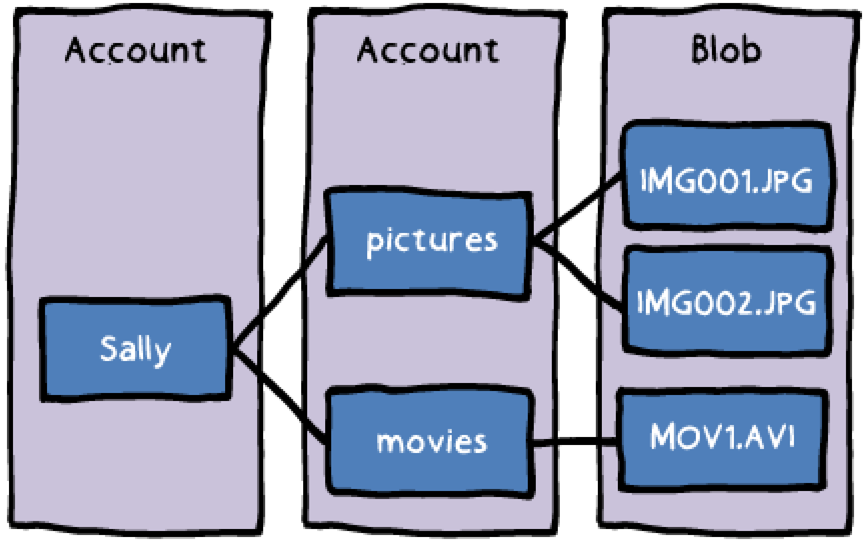
All VM Disks are stored within the Azure Blob Service:

- Unmanaged disks require the user to provision Storage Accounts and manage throughput
- Managed disks allow Azure to handle all storage and provisioning jobs and IOPs is not a consideration



Un-Managed Disks

- Require a storage account
- Management overhead
- Storage account IOPS limits
- Choose between Standard and Premium account at creation



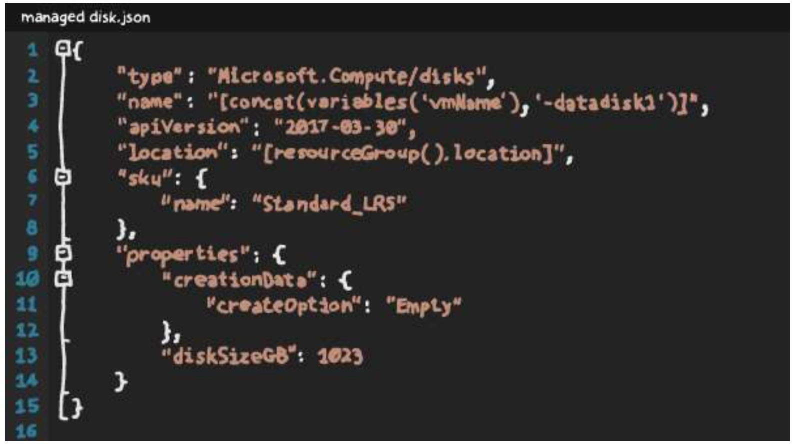
Managed Disks

- Standard and Premium disks at a disk level
- Azure handles storage account and limits
- Transaction billing (standard only)
- Snapshots
- Images

Deployment Considerations

Managed disks removes complexity from multiple disk VM deployments:

- Can deploy with templates
- Can manage with:
  - PowerShell
  - Azure CLI
  - Portal
- Easy snapshot creation and management
- Rapid performance changes



managed disk.json

```
{
    "type": "Microsoft.Compute/disks",
    "name": "[concat(variables('vmName'),'-datadisk1')]",
    "apiVersion": "2017-03-30",
    "location": "[resourceGroup().location]",
    "sku": {
        "name": "Standard_LRS"
    },
    "properties": {
        "creationData": {
            "createOption": "Empty"
        },
        "diskSizeGB": 1023
    }
}
```

Azure Files

An SMB 3.0 file service providing reliable network file shares without infrastructure:

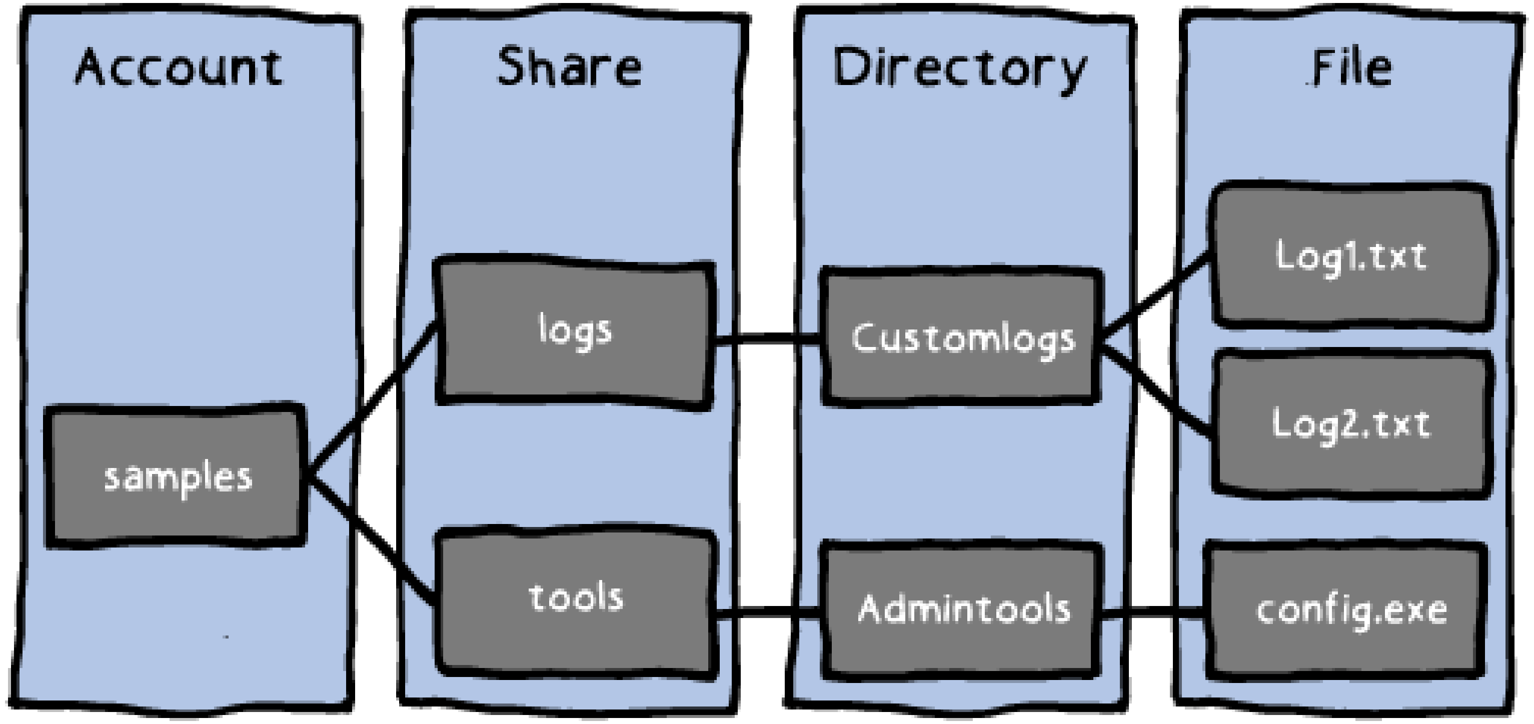
- File Shares
- File Sync
- IaaS File Shares

Sharing Files in Cloud Infrastructure

- Azure Files
- Azure IaaS VM File Share
- Azure File Sync for Hybrid and DR

Azure File Shares

Components



URL or server / application file share access

Azure File Sync

File Sync Service:

- NTFS volumes only
- Dedupe supported (not with Cloud Tiering)
- Cloud Tiering for cold files
- DR feature for failed servers

Azure IaaS File Sharing

Azure AD Domain Services integrates previously created Hybrid scenarios or works as a cloud only solution. The benefits are:

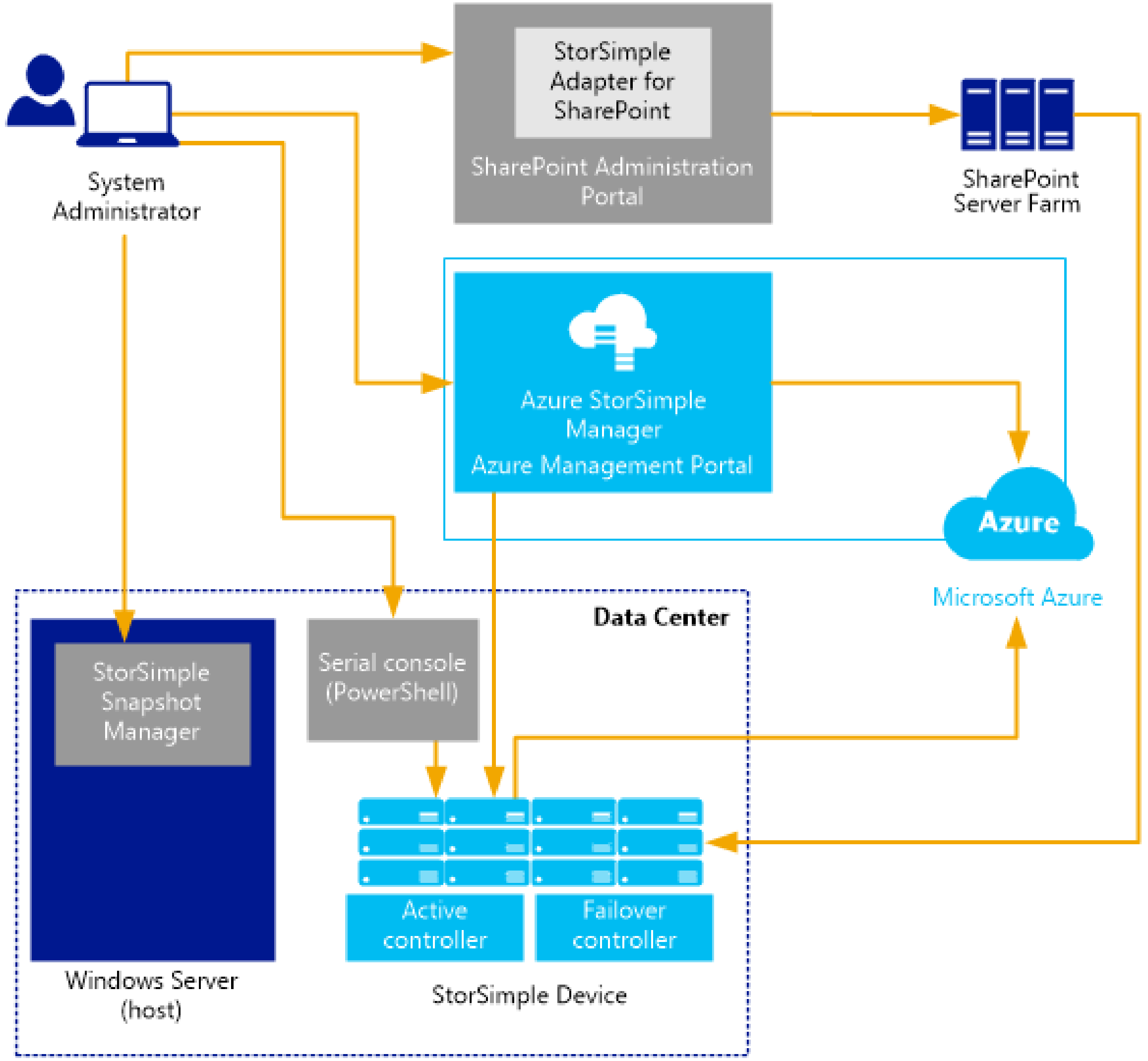
- Simplicity – few clicks to setup
- Integrated – deep Azure AD integration
- Compatible – Windows Server AD
- Cost-effective – no infrastructure burden

StorSimple

Hybrid file storage solution:

- Cost saving solution
- Accelerate Disaster Recovery
- Automate Data Management

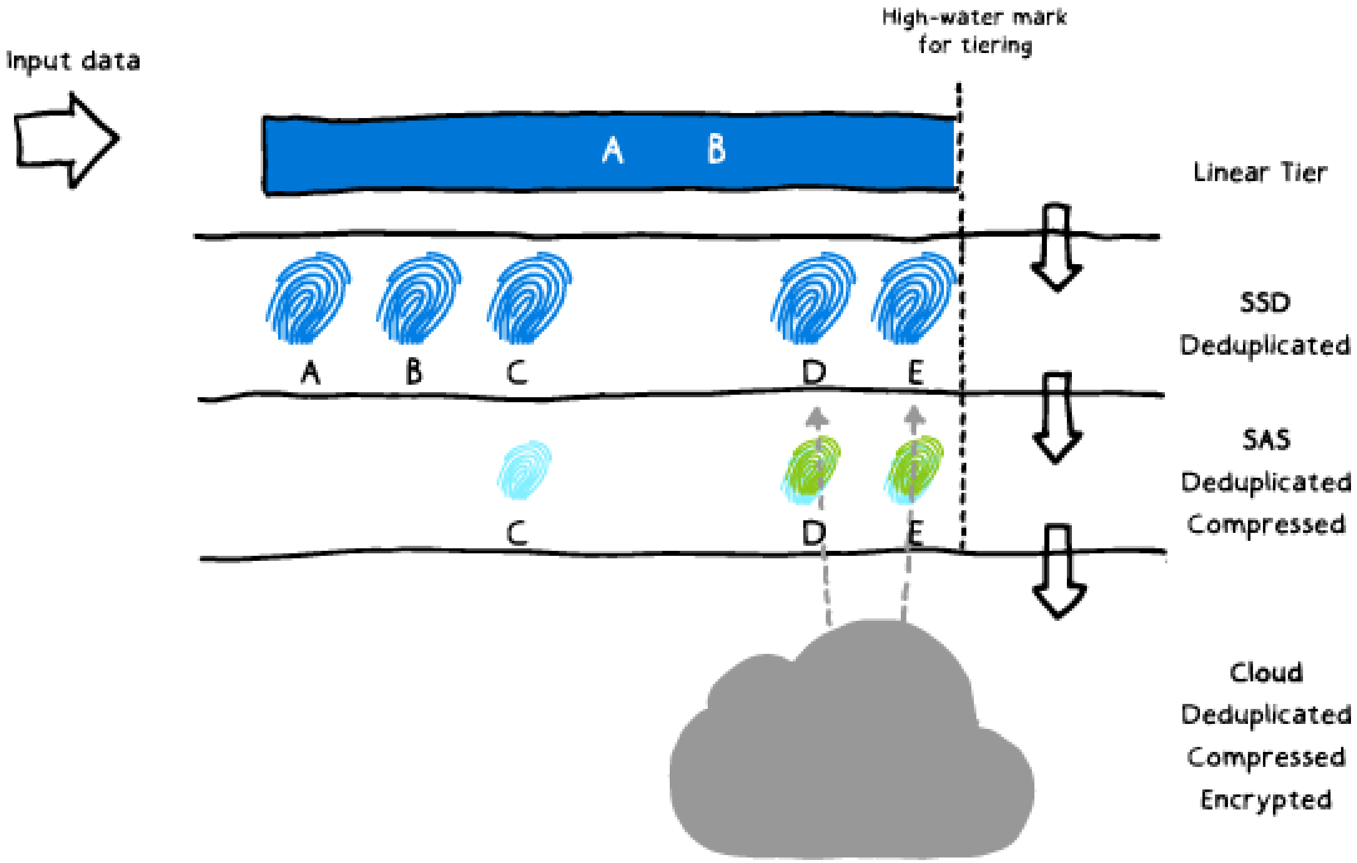
Architecture



Features

- Transparent integration – iSCSI protocol to invisibly link data storage facilities
- Reduced storage costs – Allocates sufficient local or cloud storage to meet demands, extends cloud storage when necessary
- Simplified storage management – standard tools
- Improved disaster recovery and compliance – Restores data as it is needed
- Data mobility – Can be accessed from other sites for recovery and migration purposes

Data Tiering



Lab Exercises

- https://github.com/MicrosoftLearning/AZ-301-MicrosoftAzureArchitectDesign/blob/master/Instructions
- Deploying Network Infrastructure for Use in Azure Solutions
- Deploying Messaging components to facilitate communication between Azure resources

THANK YOU for Participating in Today’s Session

1 Register your attendance

1. Go to **Link** provided in **chat window**
2. Click **Register Now**
3. Click **Confirm**

2 We'd love your feedback!

Please provide your feedback by clicking on the “***short survey***” link in the “**Did your session make the grade?**” **email you** will soon **receive**