Microsoft Certified: Azure Solutions Architect Expert (AZ-305): Networking, File and Blob Storage Solutions

Mike Boorman

Author

Designing solutions with:

- Cloud networking
- Hybrid networking
- Distributing network traffic
- Securing network traffic
- File and blob storage technologies
- Storage access and security

By the end of this course

You will have the ability to describe the various components of Azure related to networking as well as file and blob storage.

Prerequisites

- Basic cloud concepts
- General understanding of Microsoft Azure
- Knowledge of Microsoft Azure technologies
- Comfortable navigating the Azure Portal

Cloud Network Connectivity

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Connecting On-Premises, Other Clouds, and VNets

Azure ExpressRoute

Dedicated high performance network edge connector

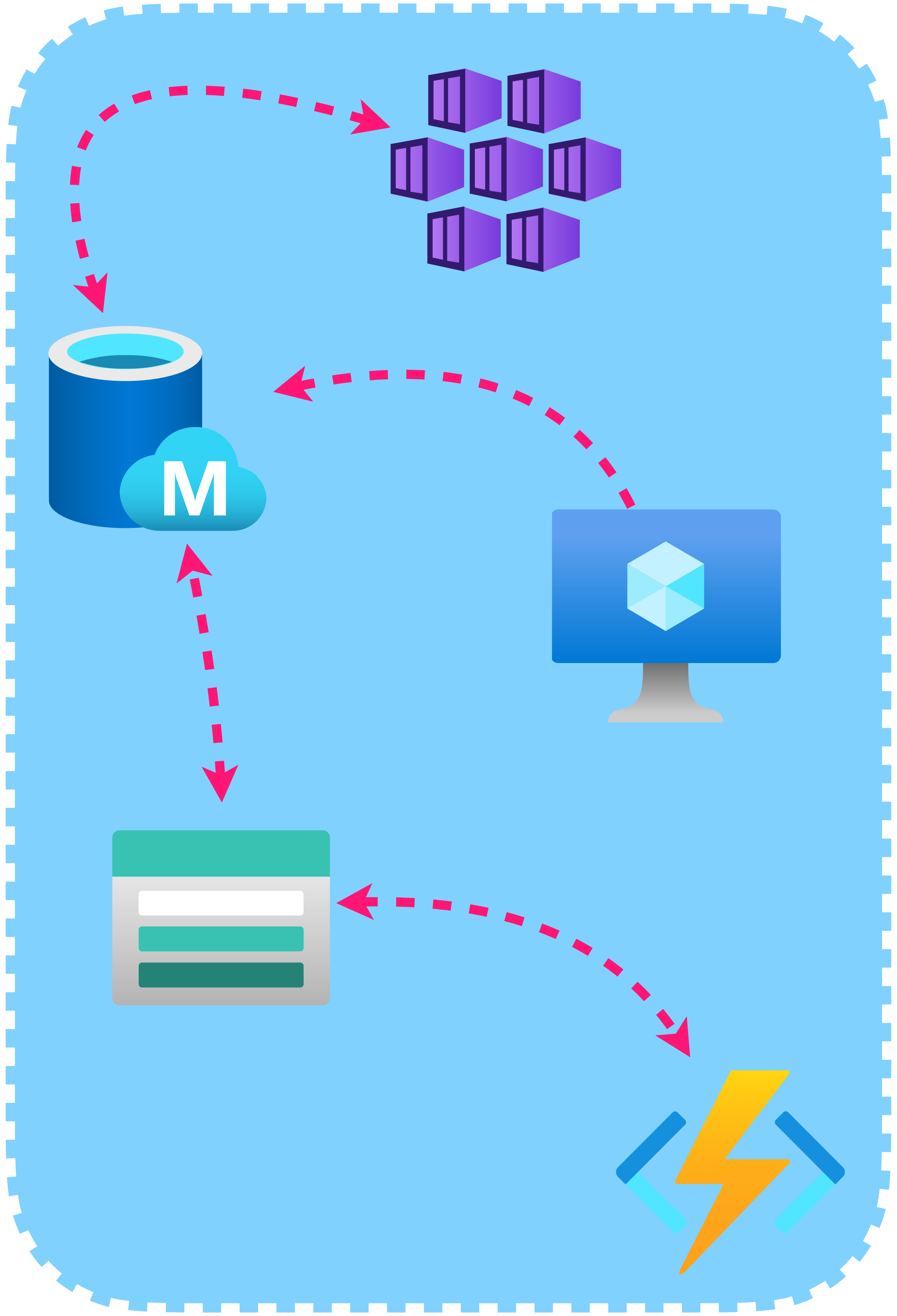
Azure VPN Gateway

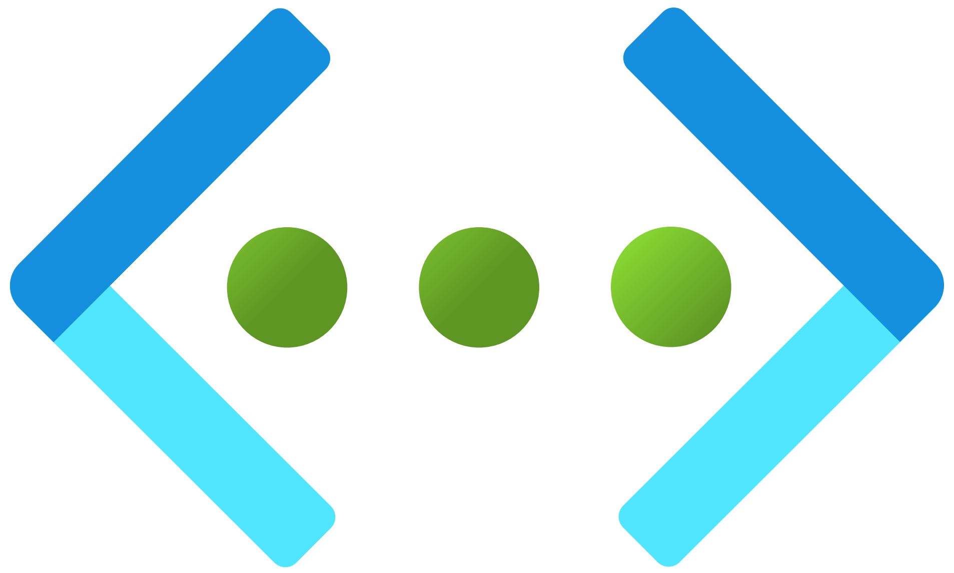
Site-to-Site VPN
Point-to-Site VPN

vNet Peering

Connecting vNets within Azure
Cross-region and subscription peering

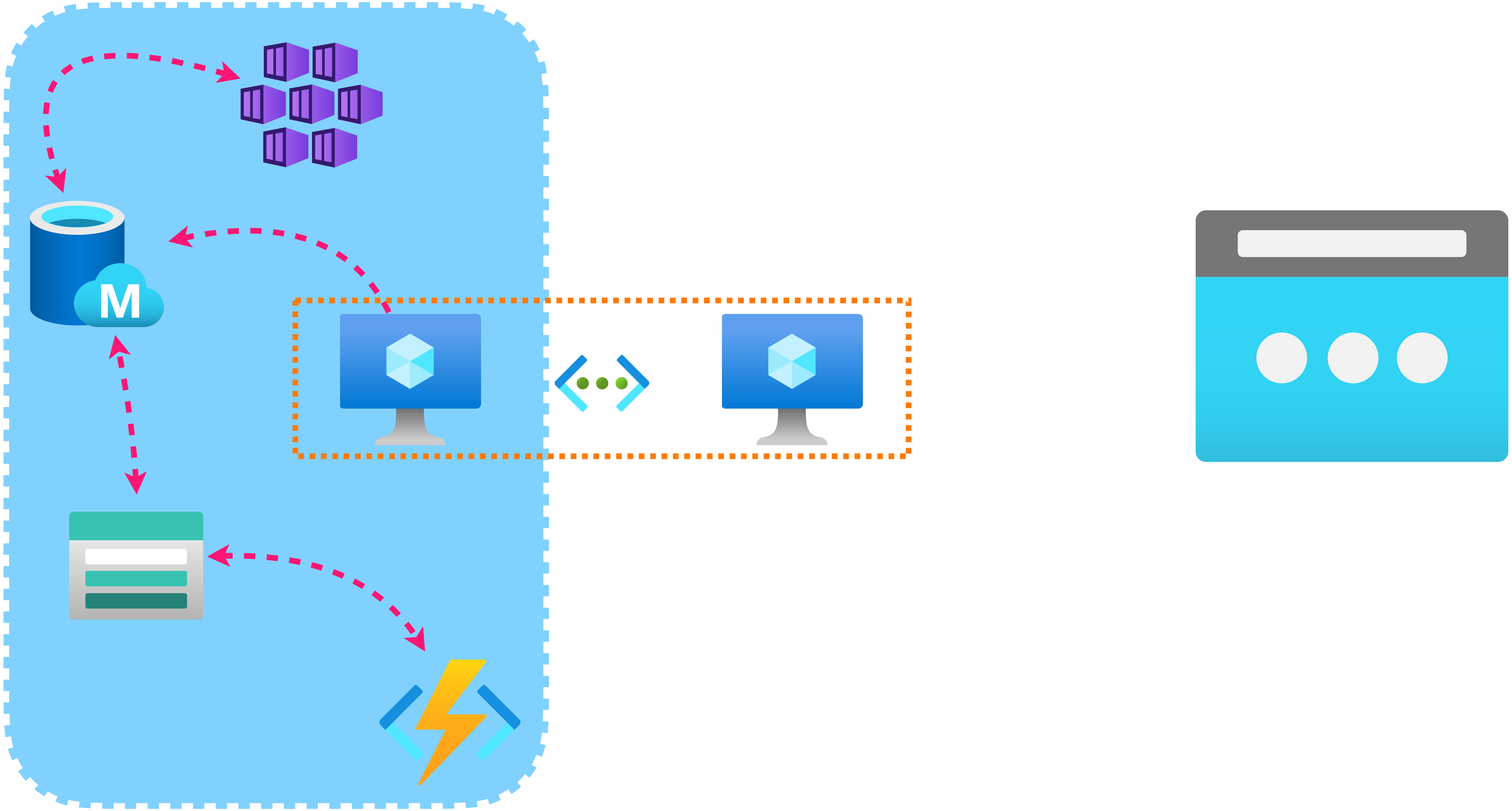
IP Addressing



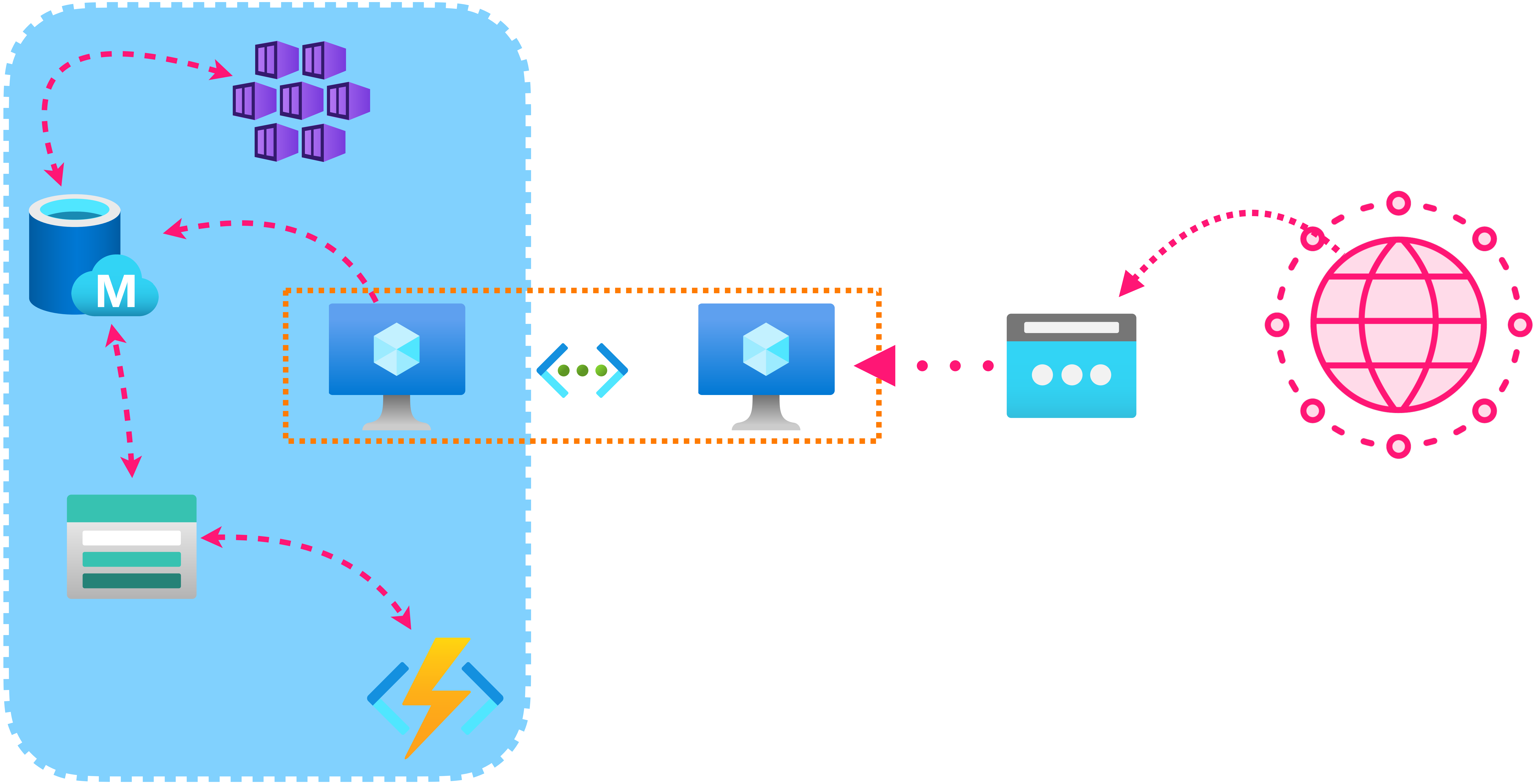


Virtual Network

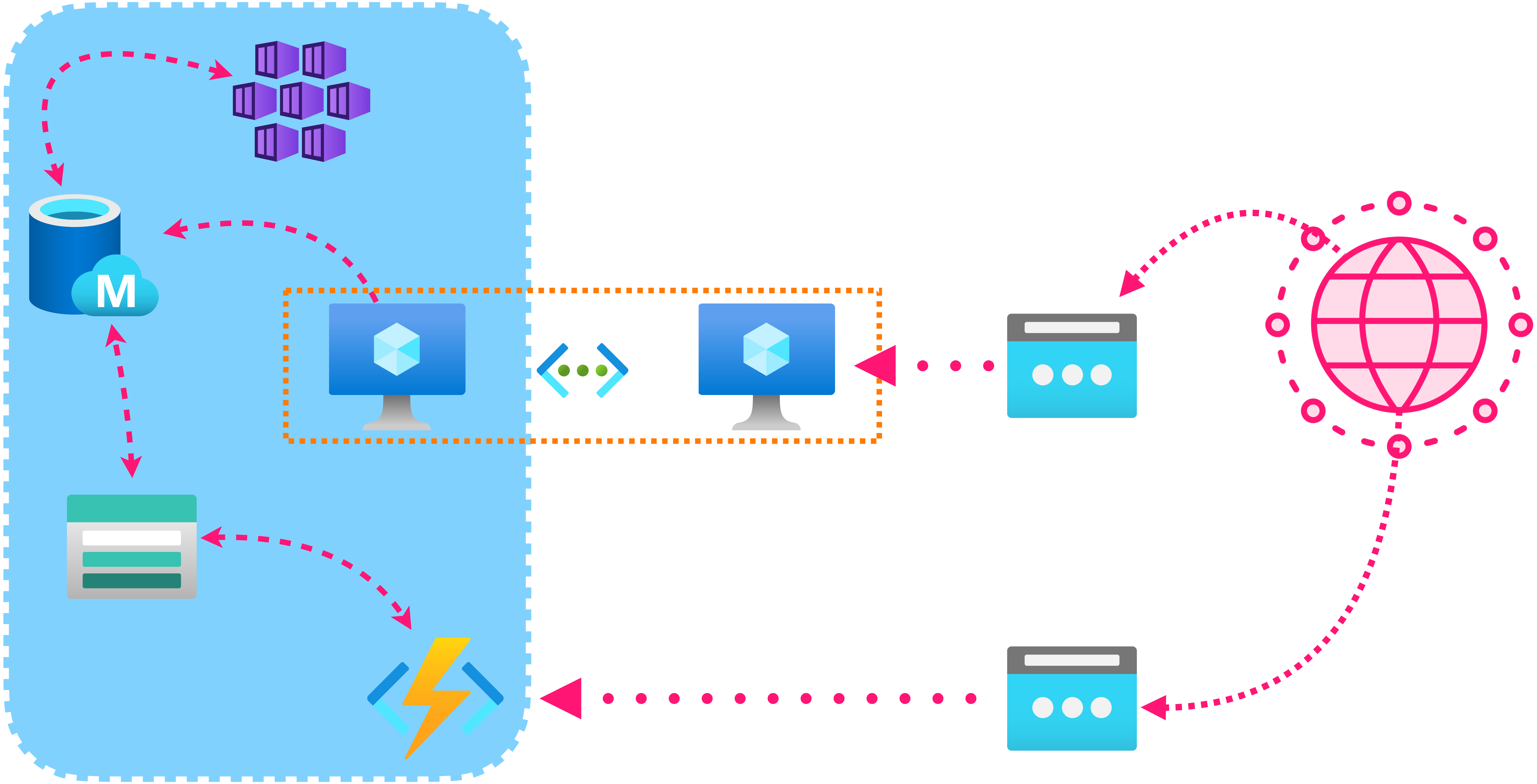
IP Addressing



IP Addressing

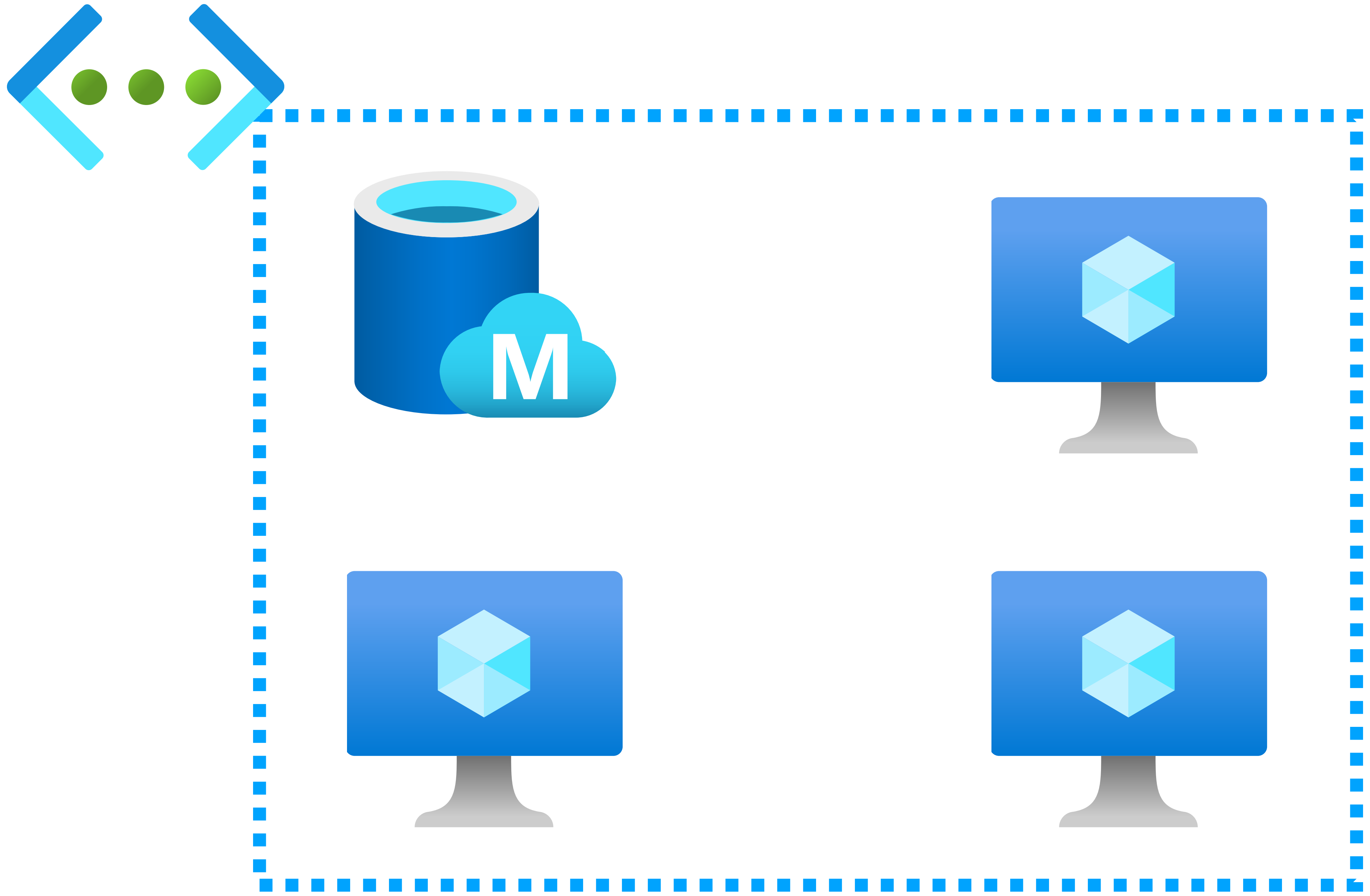


IP Addressing



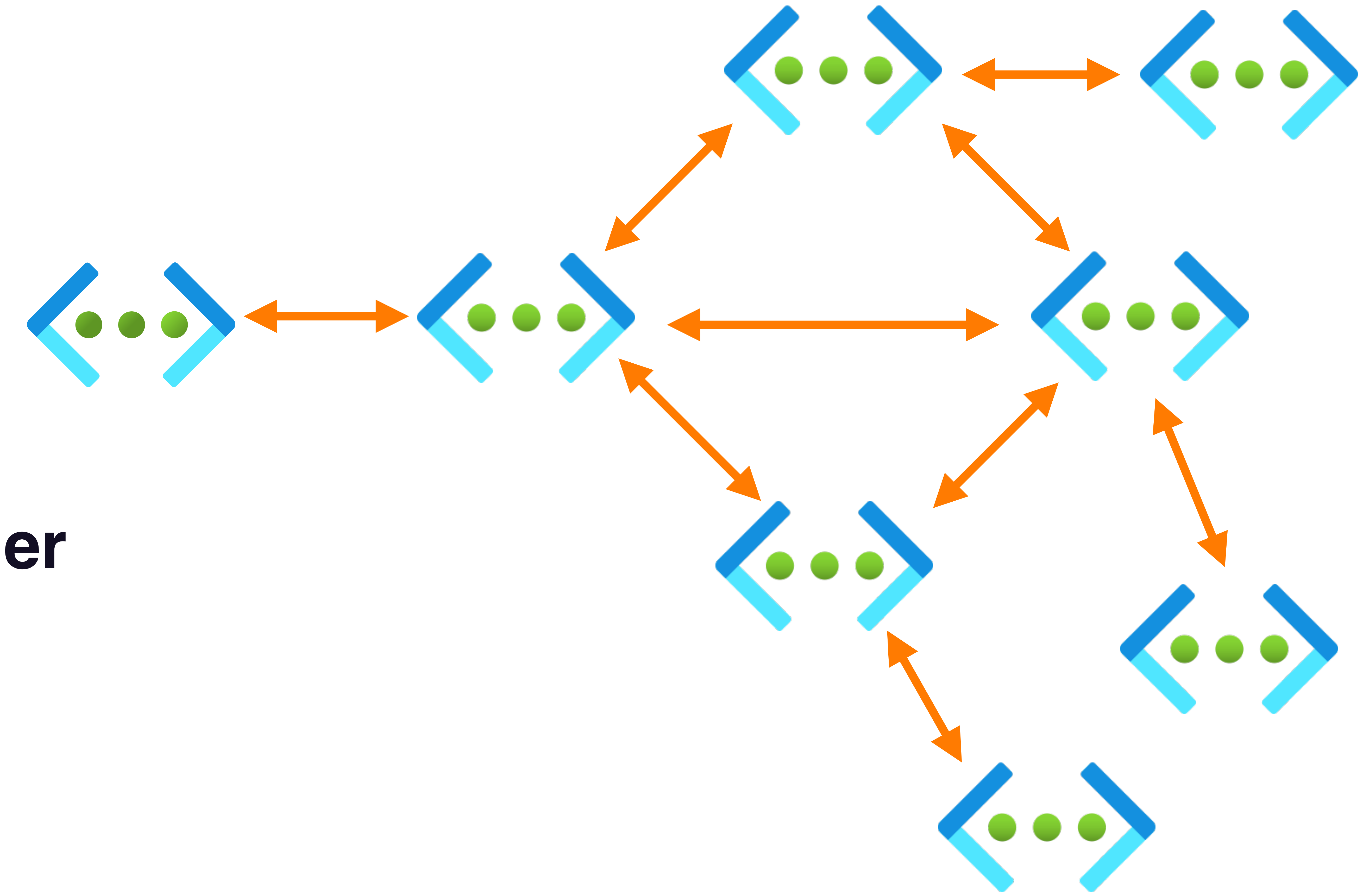
Network Topologies

Single



Network Topologies

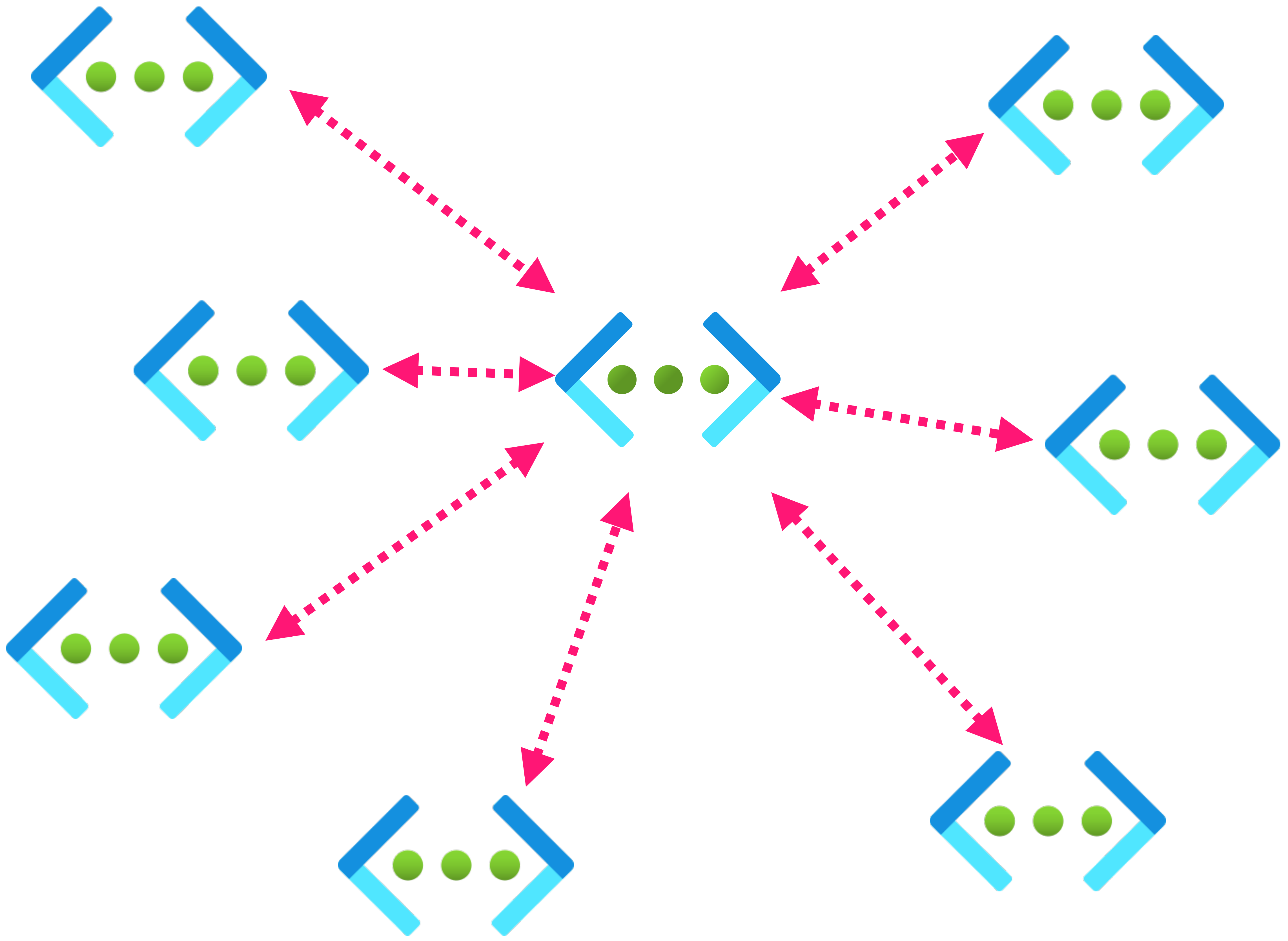
Multiple/Peering



Planning is critical with larger network implementations

Network Topologies

Hub and Spoke



Centralizes

- Traffic control

- Traffic monitoring

- Internal network security

- External network security

Network topology matters for on-premises, cloud, and hybrid environments.

Hybrid Network Connectivity

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

VPN, ExpressRoute, or Both

VPN

Secure, encrypted connection over the public internet

- Secure remote access for employees
- Low to moderate bandwidth requirements
- Cost-effective solution for small to medium deployments

VS

ExpressRoute

Dedicated, private connection with higher bandwidth and lower latency

- Mission-critical applications requiring high performance
- Large-scale data transfers and hybrid workloads
- Regulatory compliance and data sovereignty requirements

VPN, ExpressRoute, or Both

VPN

Secure, encrypted connection over the public internet

+

ExpressRoute

Dedicated, private connection with higher bandwidth and lower latency

VPN as a backup or failover for ExpressRoute

Segregating traffic based on security and performance needs

VPN Gateway

VPN gateway sizing and SKUs

- Gen 1: Basic, VpnGw1, VpnGw2, VpnGw3, VpnGw1-3AZ
- Gen 2: VpnGw2, VpnGw3, VpnGw4, VpnGw5, VpnGw2-5AZ

High availability and active-active configuration

- Deploying VPN gateways in active-active configuration
- Failover and redundancy for VPN connections

VPN gateway routing options

- Policy-based and route-based VPNs
- Dynamic routing with BGP (Border Gateway Protocol)

ExpressRoute

ExpressRoute Global Reach

- Connecting on-premises networks through Azure
- Enabling communication between on-premises locations using ExpressRoute

ExpressRoute FastPath

- Optimized data path for improved performance
- Reduced latency and higher throughput for specific workloads

Coexistence and migration

- Scenarios where using both VPN and ExpressRoute together is beneficial
- Migrating from VPN to ExpressRoute or vice versa

Virtual WAN

Virtual WAN

- Centralized network connectivity and management
- Connecting branch locations, remote users, and on-premises networks

Virtual WAN Components

- Virtual WAN Hub
- Virtual WAN VPN Gateway I ExpressRoute Gateway

Virtual WAN partner ecosystems and CPE devices

- Integration with third-party network providers and customer premises equipment (CPE)

Monitoring and troubleshooting Virtual WAN connections

- Built-in monitoring and diagnostics tools
- Troubleshooting common connectivity issues

weInvest is a global financial services company with multiple branch offices and a significant on-premises infrastructure. They are migrating their applications to Azure and need to establish secure and reliable connectivity between their on-premises datacenters and Azure.

Requirements:

- Secure and high-performance connectivity for mission-critical financial applications
- Ability to connect branch offices and remote users to Azure resources
- Compliance with regulatory requirements for data protection and privacy
- Scalability to accommodate future growth and expansion

Solution:

- Implement ExpressRoute for dedicated, high-bandwidth connectivity between on-premises datacenters and Azure
- Use Virtual WAN to connect branch offices and remote users to Azure, leveraging the Virtual WAN hub and VPN gateway
- Establish VPN connections as a backup and failover mechanism for ExpressRoute
- Leverage ExpressRoute Global Reach to enable communication between on-premises locations through Azure
- Implement network security best practices, such as Azure Firewall and Network Virtual Appliances (NVAs), to secure hybrid connectivity

Network Routing

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Why Modify Routing?

Scenarios for modifying routing

Custom network topologies

Traffic isolation and segmentation

Forced tunneling

Integration with on-premises networks

Benefits of modifying routing

Improved network performance

Enhanced security and control

Simplified network management

Routing Types in Azure

System Routes

Default routing provided by Azure

Automatically created and managed

User-Defined Routes

Custom routing rules defined by users

Override or augment system routes

Specify next hop for traffic

Border Gateway Protocol

Dynamic routing protocol

Exchange routing information between Azure and on-premises networks

Enables advanced routing scenario

Outbound Connectivity Options

- Load Balancer
- Azure NAT Gateway
- Azure Firewall
- Network Virtual Appliances

Scenario:

Reroute Media Group Inc. is migrating their application workloads to Azure. They have multiple virtual networks hosting different application tiers and need to ensure secure and efficient communication between them. Additionally, they require outbound internet connectivity for certain application components while maintaining security and control.

Requirements:

- Segregate traffic between application tiers
- Enable secure communication across virtual networks
- Allow outbound internet connectivity for specific resources
- Implement network security controls and filtering

Solution:

- **Use user-defined routes (UDRs) to control traffic flow between virtual networks and application tiers**
- **Implement a hub-and-spoke network topology with a central virtual network acting as a transit point**
- **Deploy Azure Firewall in the hub virtual network to control and filter outbound internet traffic**
- **Configure Virtual Network NAT Gateway for specific subnets requiring outbound internet connectivity**
- **Leverage BGP for dynamic routing between virtual networks and on-premises networks**

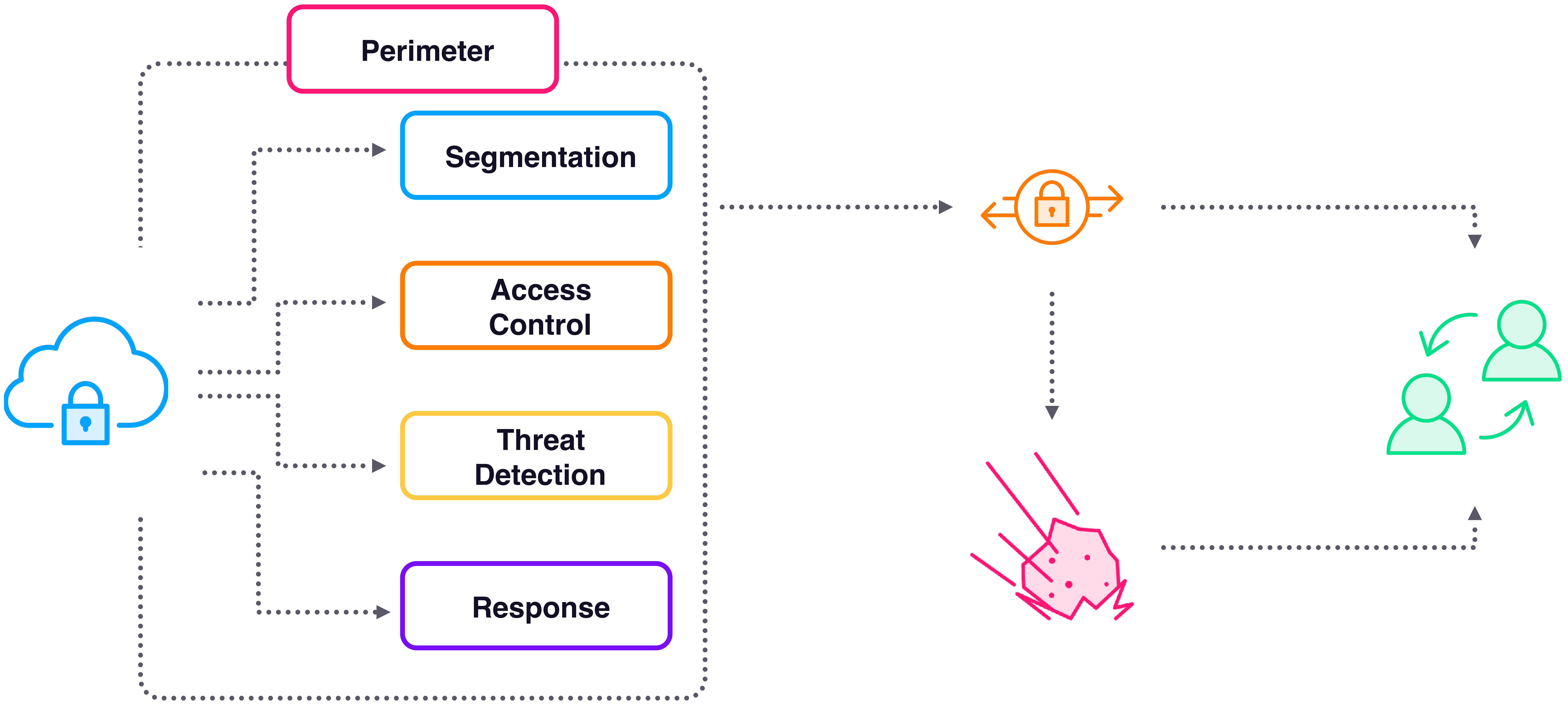
Securing External Network Traffic

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Defense in Depth



Traffic Filtering and Routing for Security

Network Security Groups (NSGs)

Stateful firewall

Filter traffic

User-Defined Routes (UDRs)

Control traffic flow

Route traffic

Application Security Groups (ASGs)

Group VMs

Apply NSG rules

Traffic Filtering and Routing for Security

Network Security Groups (NSGs)

User-Defined Routes (UDRs)

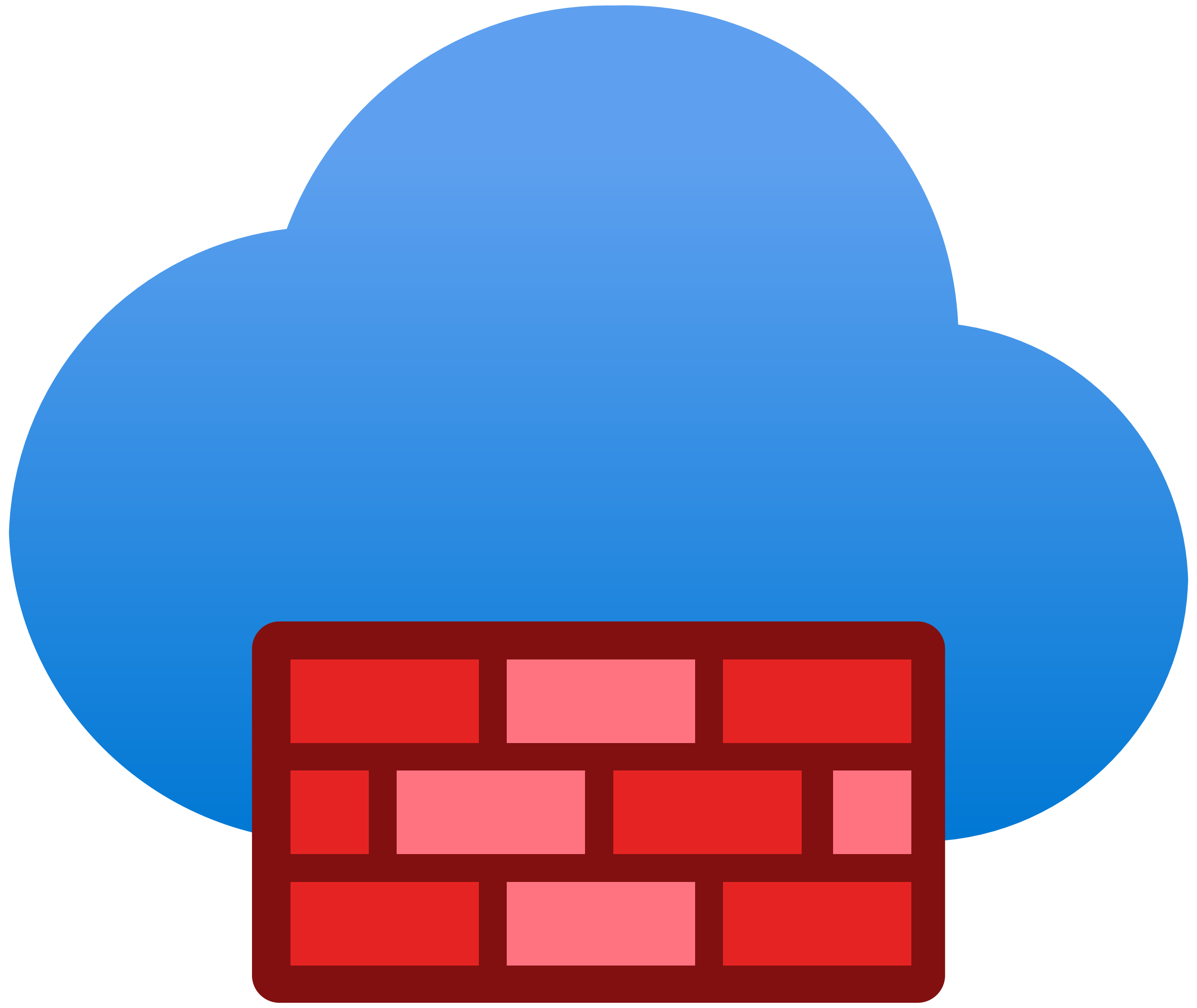
Application Security Groups (ASGs)

Implement least privilege access

Use a combination of NSGs, UDRs, and ASGs

Regularly review and update security rules

When to Use Azure Firewall



- Fully managed, cloud-native firewall service
- Stateful firewall, IDPS, and URL filtering

Scenarios for Azure Firewall

- Perimeter security for virtual networks
- Centralized control and logging
- Hybrid cloud environments
- Compliance requirements

Benefits of Azure Firewall

Highly available and scalable

Integrated with Azure management and security tools

Granular application and network-level control

Azure Firewall vs Network Virtual Appliance

Azure Firewall

Fully managed

Native Azure

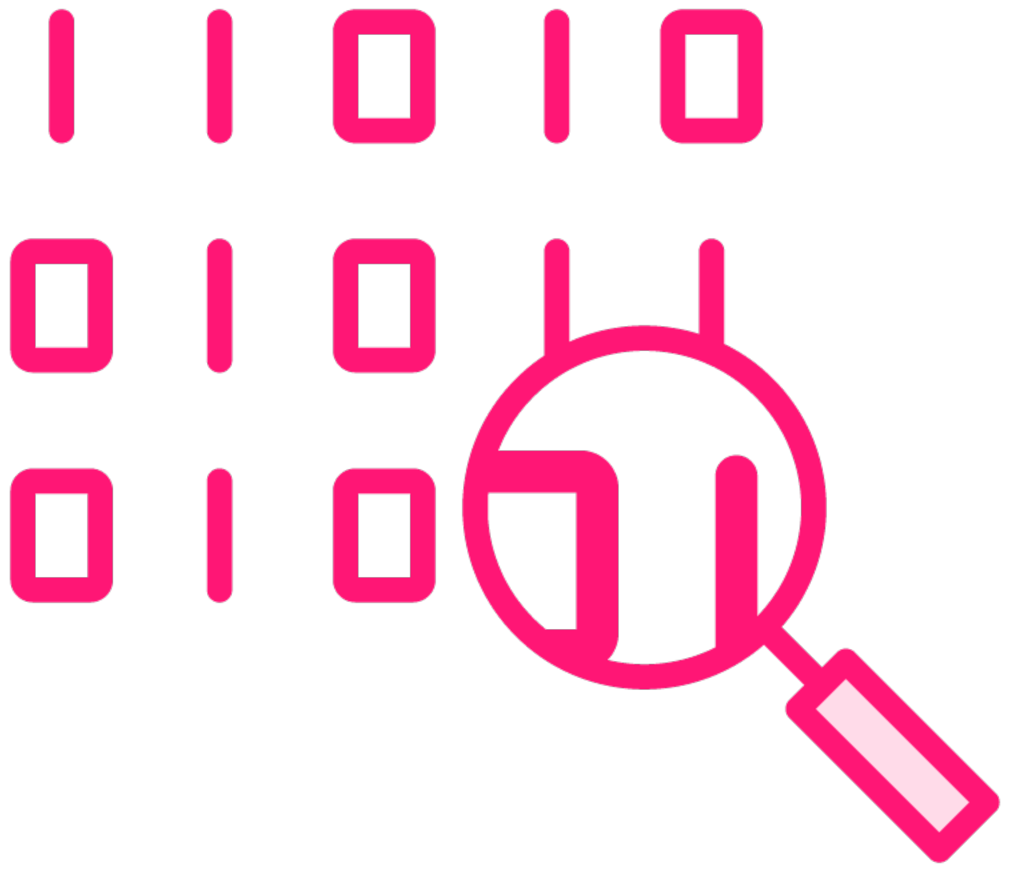
VS

Network Virtual Appliance

Self-managed

Third-Party Options

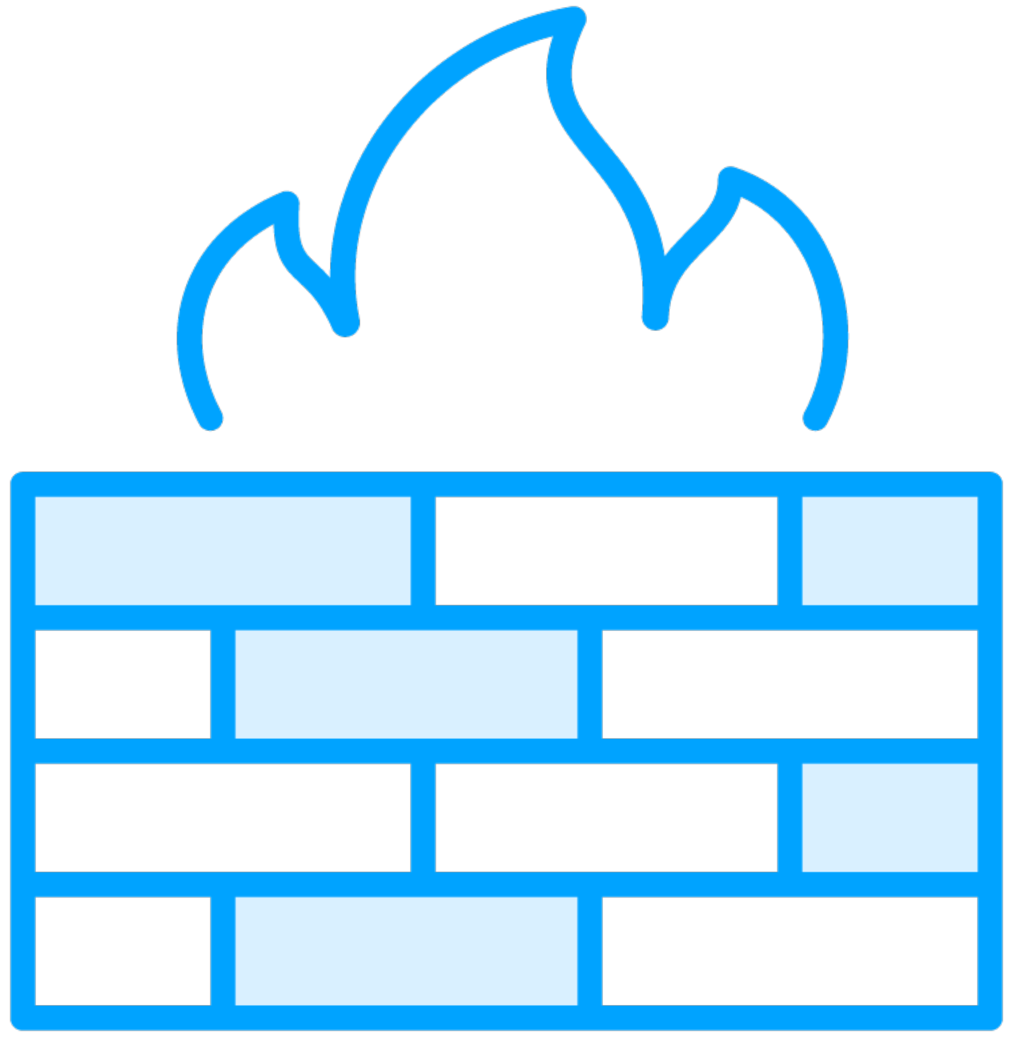
Data Residency and Public Endpoints



Data residency considerations

- Compliance with data localization regulations
- Choosing the appropriate Azure regions
- Azure Policy for enforcing data residency requirements

Public Endpoints and Service Firewall



- Exposing services to the internet
- Securing public endpoints with Service Firewall
- Configuration options for Service Firewall
- Integration with Azure Firewall and other security services

Data Residency and Public Endpoint Best Practices

Regularly assess compliance requirements

Use Azure Policy for enforcement

Implement least privilege for public endpoints

Monitor and audit access to public endpoints

Scenario: Investco Ltd. is a global financial services company that handles sensitive customer data. They are migrating their applications to Azure and need to ensure secure external network traffic while complying with data residency regulations.

Requirements:

- Implement a layered security approach
- Control inbound and outbound traffic at the network perimeter
- Ensure compliance with data residency regulations
- Secure public endpoints for customer-facing applications
- Centralized management and monitoring of network security

Solution:

- **Implement Defense in Depth using a combination of Azure services**
  - Azure Firewall for perimeter security and centralized control
  - Network Security Groups (NSGs) for subnet-level traffic filtering
  - User-Defined Routes (UDRs) for traffic routing through NVAs for additional inspection
  - Application Security Groups (ASGs) for granular access control between application tiers
- **Use Azure Policy to enforce data residency requirements and ensure data remains within specified regions**
- **Configure Service Firewall for public endpoints of customer-facing applications**
- **Integrate Azure Firewall with Azure Security Center for centralized management and monitoring**

Securing Internal Network Traffic

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Defense in Depth for Internal Networks

Layered security approach

Principle of least privilege

Segmentation and isolation

Defense in Depth for Internal Networks

Network segmentation

Access control and authentication

Encryption and data protection

Monitoring and logging

Network Security Groups (NSGs)

- Stateful firewall for inbound and outbound traffic
- Filter traffic based on IP addresses, ports, and protocols

Scenarios for Using Network Security Groups (NSGs)

Subnet-level traffic filtering

Isolating resources within a virtual network

Controlling access to specific services or ports

Implementing granular security policies

Best Practices for Using NSGs

Define clear and consistent naming conventions

Implement least privilege access

Regularly review and update NSG rules

Use NSGs in combination with other security controls

Network Segmentation and Isolation

Virtual Network (VNet)

Dividing VNets into subnets

Isolating resources based on application tiers or security zones

Network Security Groups (NSGs)

Applying NSGs to subnets or individual resources

Controlling traffic flow between segments

Application Security Groups (ASGs)

Grouping resources based on application roles

Applying NSG rules based on ASGs

Define clear segmentation boundaries
Implement least privilege access between segments
Regularly review and update segmentation policies

Service Endpoints and Private Endpoints

Service Endpoints

- Secure access to Azure services from a virtual network
- Extend virtual network identity to the service
- Supported services include Azure Storage, Azure SQL Database, and more

Secure access at the ***service*** level

Private Endpoints

- Private and secure connection to Azure services
- Expose services through a private IP address within a virtual network
- Ensures traffic remains within the Azure network

Secure access at the ***resource*** level

Scenario: myHealth Inc. is a healthcare organization that handles sensitive patient data. They are building a multi-tiered application in Azure and need to ensure secure internal network traffic between application components.

Requirements:

- Implement a Defense in Depth approach for internal networks
- Isolate application tiers and restrict inter-tier communication
- Control access to sensitive data stores and services
- Ensure compliance with healthcare regulations (e.g., HIPAA)
- Provide secure connectivity to Azure services

Solution:

- Implement network segmentation using Virtual Networks (VNets) and subnets
  - Create separate subnets for each application tier (web, application, database)
  - Apply Network Security Groups (NSGs) to subnets to control inter-tier communication
- Use Application Security Groups (ASGs) to group resources based on application roles
  - Apply NSG rules based on ASGs for granular access control
- Implement Private Endpoints for secure connectivity to Azure services (e.g., Azure Storage, Azure SQL Database)
  - Ensure sensitive data remains within the Azure network and is not exposed to the public internet
- Enable logging and monitoring for NSGs and Private Endpoints
  - Use Azure Network Watcher and Azure Monitor to detect and investigate security incidents
- Regularly review and update security policies and configurations
  - Conduct periodic security assessments and audits to ensure compliance with healthcare regulations

Distributing Regional Application Traffic

Mike Boorman

Author, Cloud

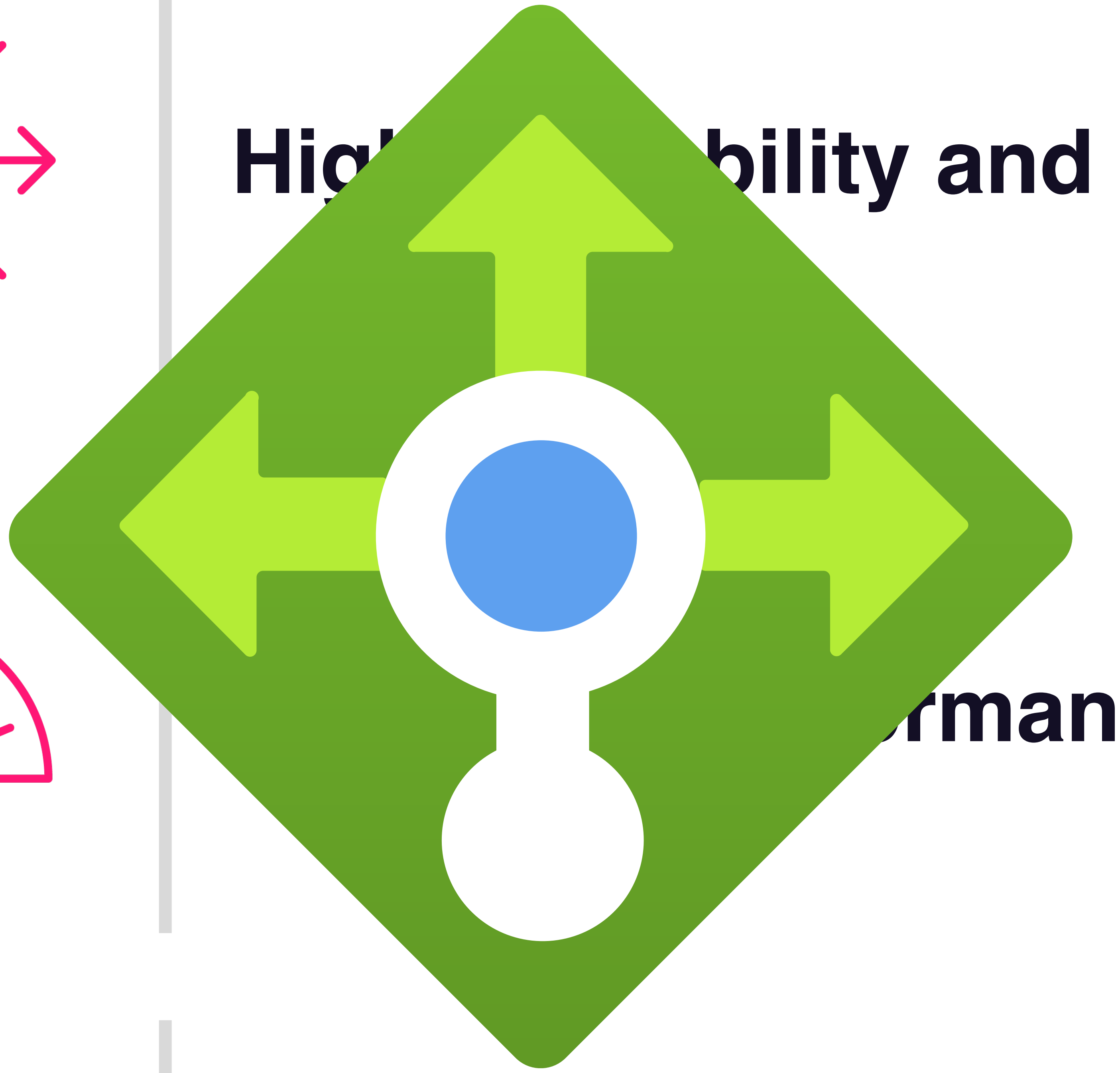
@pluralsight | www.pluralsight.com

Distributing Regional Application Traffic in Azure

Hig bility and fault tolerance

rmance and user experience

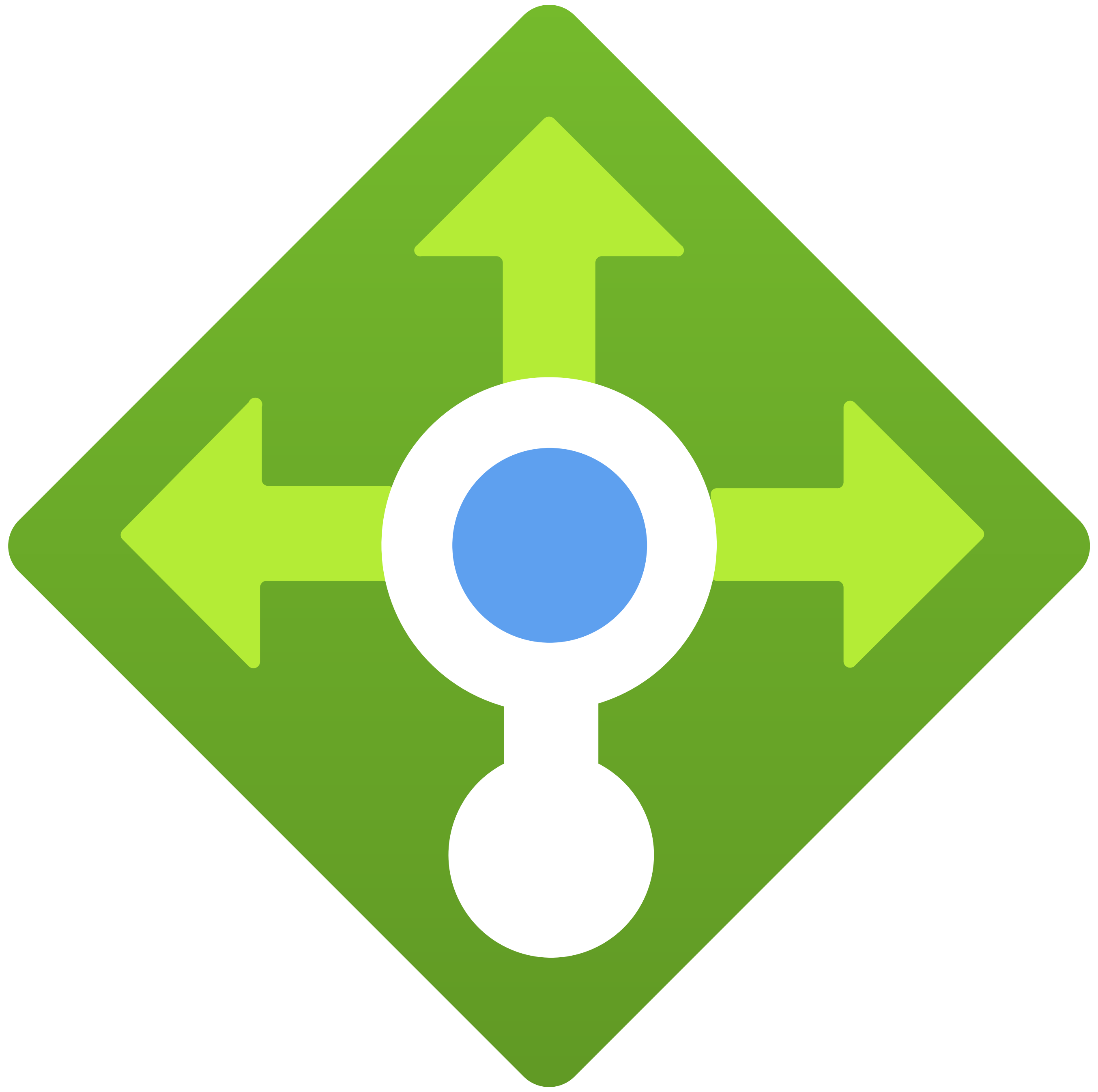
Efficient resource utilization



Load Balancer

Application Gateway

Azure Load Balancer



Overview

- Layer 4 (TCP/UDP) load balancing
- Distribution of incoming traffic across backend instances

Types

- Public Load Balancer
  - Distributes incoming internet traffic to backend instances
  - Provides a public IP address and DNS name
- Internal Load Balancer
  - Distributes traffic within a virtual network
  - Provides load balancing for internal services

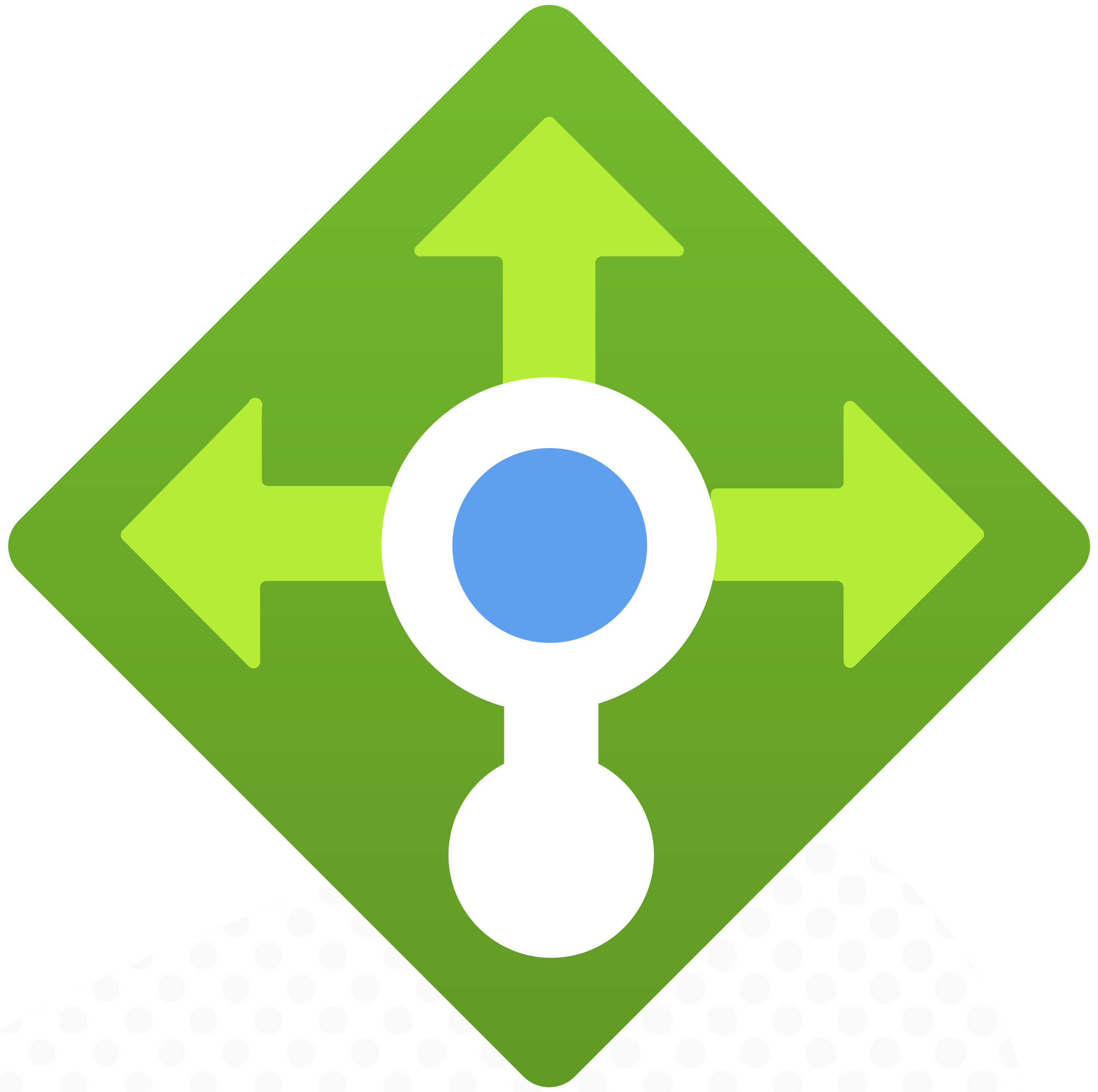
Azure Load Balancer

- Load Balancing Rules and Health Probes
  - Defining load balancing rules for traffic distribution
  - Configuring health probes to monitor backend instance health
- Use cases for Azure Load Balancer
  - Scalability and high availability for public-facing applications
  - Load balancing internal services within a virtual network

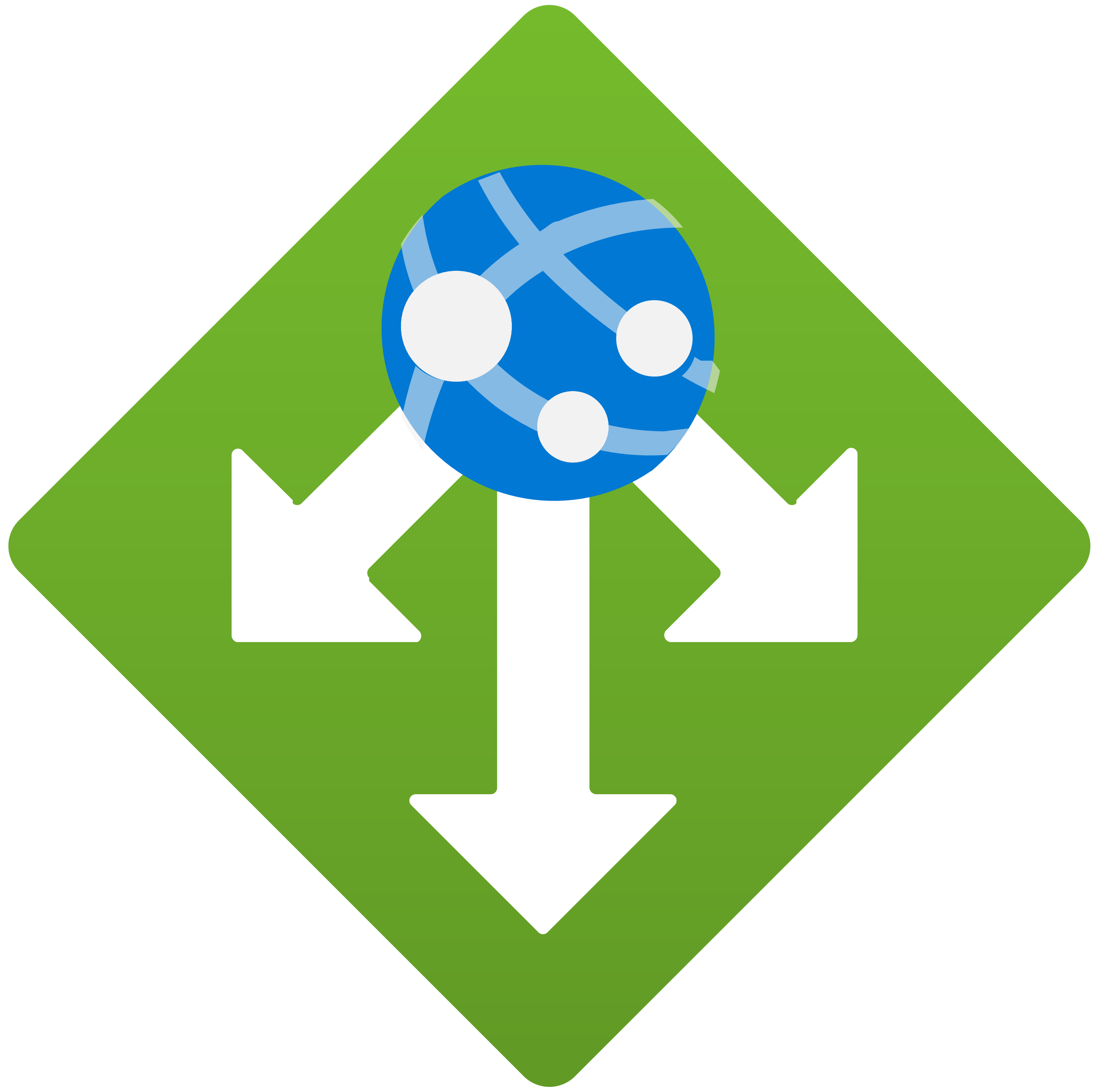
Azure Application Gateway

Layer 7 (HTTP/HTTPS) load balancing

Advanced routing and SSL termination

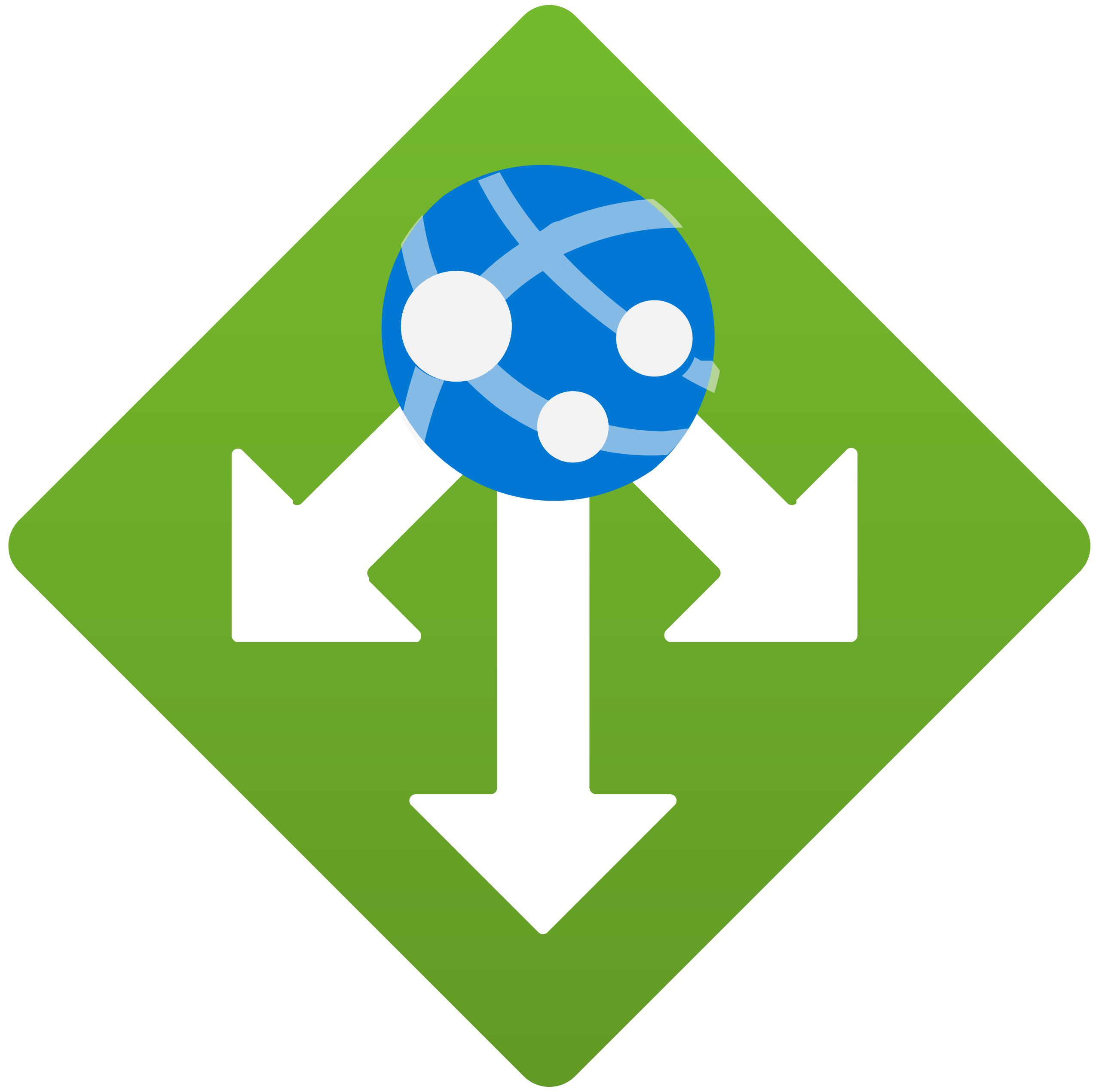


Azure Application Gateway Key Features



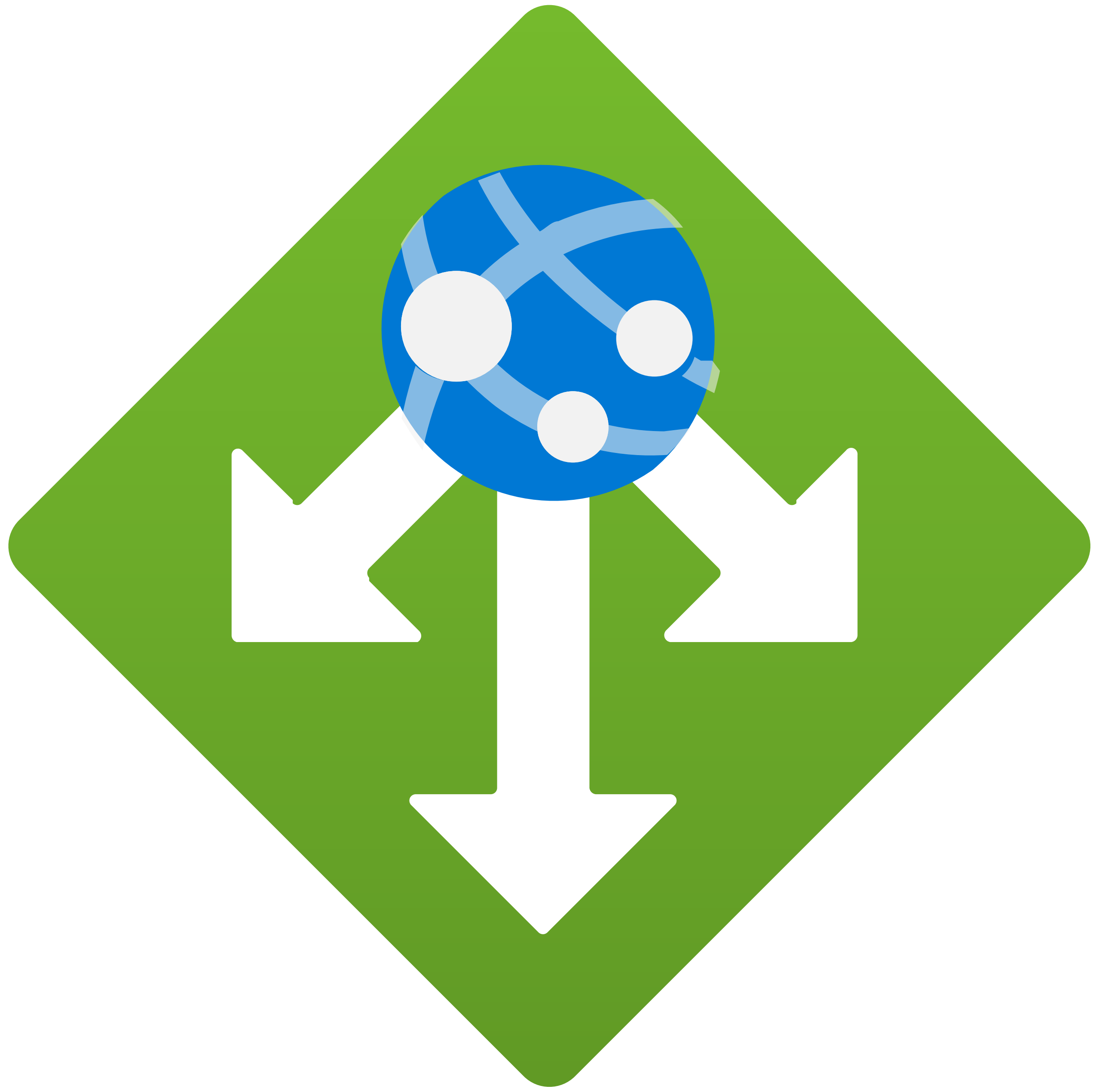
- URL-based routing
  - Routing requests based on URL paths
  - Enabling multiple applications on the same gateway
- SSL termination
  - Offloading SSL/TLS encryption and decryption
  - Improving application performance and reducing server load

Azure Application Gateway Key Features



- Web Application Firewall (WAF)
  - Built-in protection against common web vulnerabilities
  - Customizable rules and protection policies
- Autoscaling and high availability
  - Automatic scaling based on traffic load
  - Built-in redundancy and fault tolerance

Azure Application Gateway Use Cases



- Securing and load balancing web applications
- Hosting multiple websites on the same gateway
- Implementing advanced routing and SSL offloading

Choosing the Right Traffic Distribution Solution

Factors to Consider

- Application protocol (Layer 4 vs Layer 7)
- Routing requirements
- SSL termination needs
- Web application firewall (WAF) requirements
- Scalability and performance considerations

Best Practices

- Designing for high availability and fault tolerance
- Configuring health probes and monitoring
- Securing traffic with SSL/TLS encryption
- Regularly testing and validating the traffic distribution setup

Scenario: globalBuy Ltd. is a global e-commerce company that experiences high traffic volumes. They want to distribute their application traffic within each region to ensure high availability, scalability, and optimal performance.

Requirements:

- Handle both HTTP and HTTPS traffic
- Route requests based on URL paths to different backend services
- Offload SSL/TLS encryption and decryption
- Protect against common web vulnerabilities
- Automatically scale based on traffic load
- Ensure high availability and fault tolerance

Solution:

- **Implement Azure Application Gateway for regional traffic distribution**
  - Configure HTTP and HTTPS listeners to handle incoming traffic
  - Define URL-based routing rules to direct requests to appropriate backend services
  - Enable SSL termination to offload encryption and decryption
  - Activate the Web Application Firewall (WAF) to protect against common web vulnerabilities
  - Configure autoscaling to automatically adjust the number of instances based on traffic load
  - Deploy Application Gateway across multiple availability zones for high availability
- **Use Azure Load Balancer for distributing traffic to backend services within each availability zone**
  - Configure load balancing rules to distribute traffic evenly across backend instances
  - Define health probes to monitor the health of backend instances
  - Ensure that backend services are deployed across multiple instances for fault tolerance

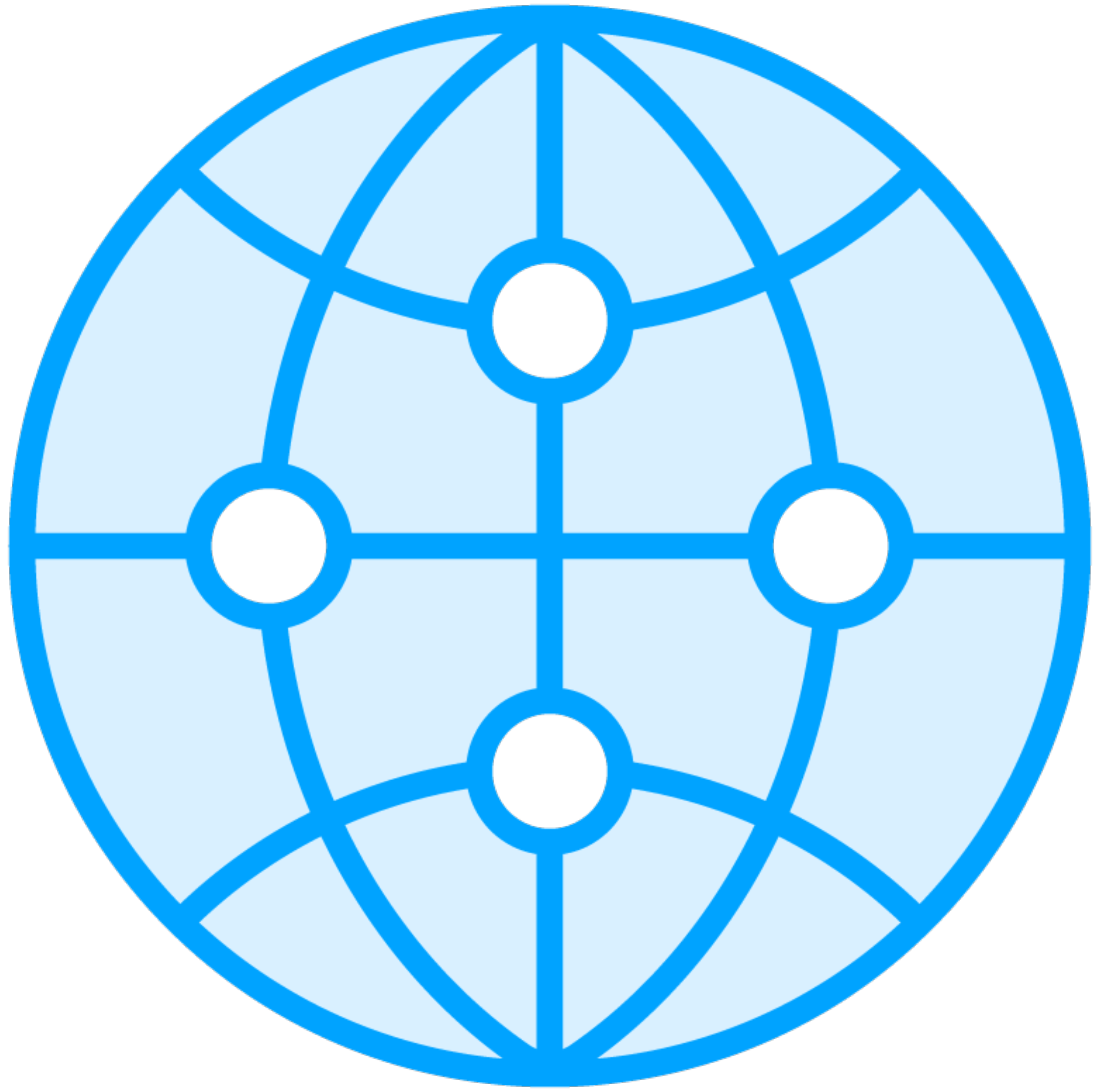
Distributing Global Application Traffic

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Why Distribute Globally?



- Improved performance and user experience
- Increased availability and reliability
- Efficient resource utilization across regions

Azure Front Door

Key features of Azure Front Door

- Anycast-based global load balancing
  - Distributing traffic to the nearest backend based on latency
- URL-based routing and path-based routing
  - Routing requests based on URL paths or patterns
- SSL offloading and end-to-end SSL
  - Offloading SSL/TLS encryption and decryption at the edge
- Custom domain support and SSL certificates
  - Using custom domain names and SSL certificates for branding

Overview of Azure Front Door

- Global HTTP load balancing and routing
- Accelerated application performance
- Integrated Web Application Firewall (WAF)

Azure Traffic Manager

DNS-based traffic routing

Global traffic distribution and failover

Configuring health probes to monitor backend health

Automatic failover to healthy backends

Azure Traffic Manager

Priority

Performance

Multivalue

Weighted

Geographic

Subnet

Azure Content Delivery Network (CDN)

Overview of Azure CDN

- Accelerating content delivery and reducing latency
- Caching static content at the edge

Azure CDN providers

- Microsoft
- Verizon
- Akamai

Key features of Azure CDN

- Global distribution and edge caching
- Serving content from the nearest edge server to users
- Dynamic site acceleration
- Compression and caching optimization
- Compressing content and optimizing caching settings

Choosing the Right Traffic Distribution System

Factors to Consider

- Application requirements and traffic patterns
- Performance and latency considerations
- Availability and failover needs
- Security and compliance requirements
- Integration with existing infrastructure

Comparing Solutions

- Routing capabilities and granularity
- Performance acceleration and caching
- Health monitoring and failover
- Security features and WAF integration

- Designing for high availability and geo-redundancy
- Optimizing performance with caching and content delivery
- Securing traffic with SSL/TLS and WAF

- Implementing proper health monitoring and failover mechanisms
- Regularly testing and monitoring the traffic distribution setup

Scenario: KnowNews Inc. is a global news and media company that serves millions of users worldwide. They want to distribute their application traffic globally to ensure high performance, availability, and efficient content delivery.

Solution:

- **Implement Azure Front Door for global HTTP load balancing and routing**
- **Leverage Azure Traffic Manager for global traffic routing and failover**
- **Use Azure Content Delivery Network (CDN) to accelerate static content delivery**

Requirements:

- Route users to the nearest application backend for optimal performance
- Accelerate delivery of static content, such as images and videos
- Ensure high availability and automatic failover in case of regional outages
- Protect against web vulnerabilities and DDoS attacks
- Integrate with their existing application infrastructure

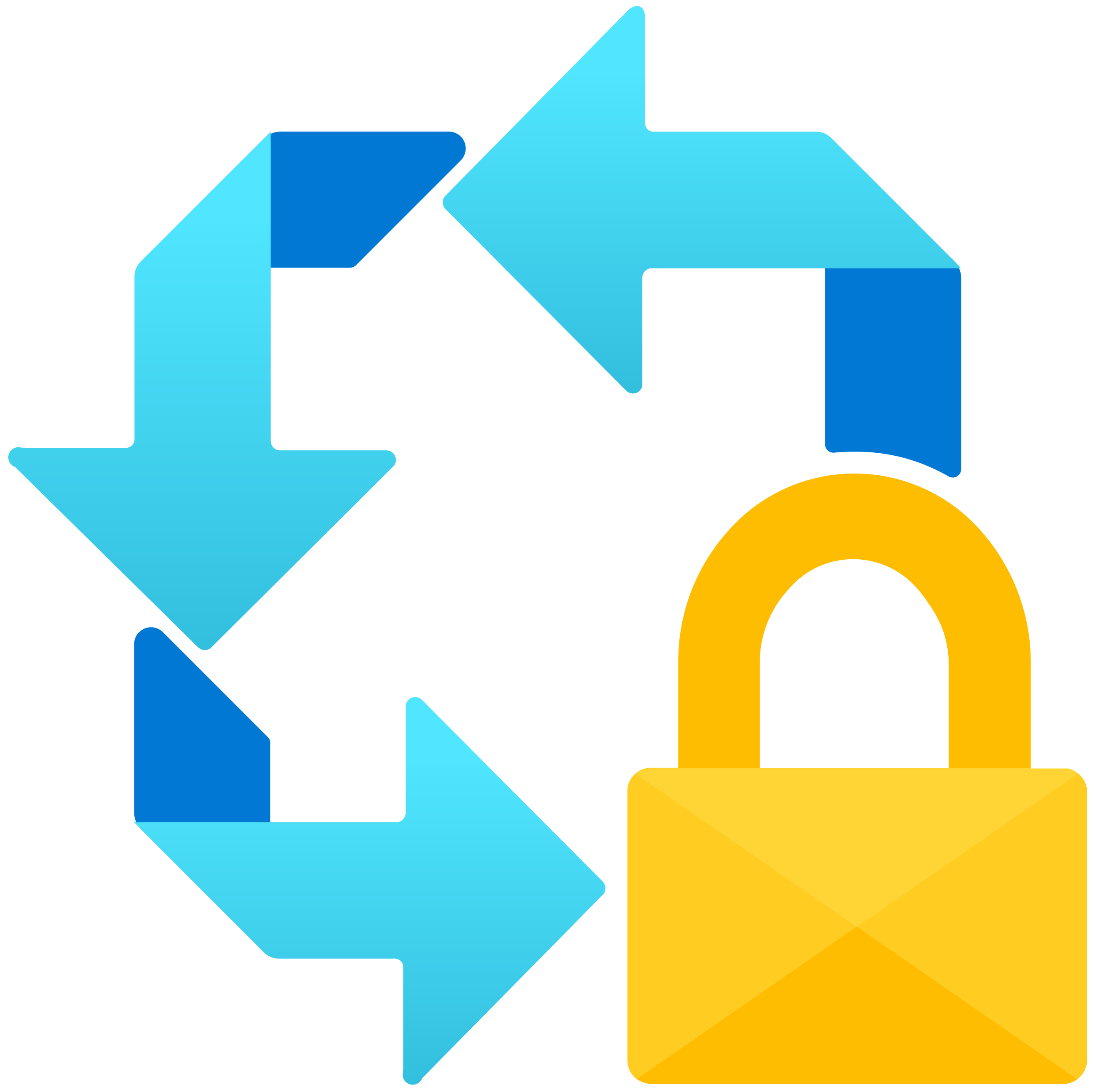
Securing Application Network Traffic

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Application Network Security



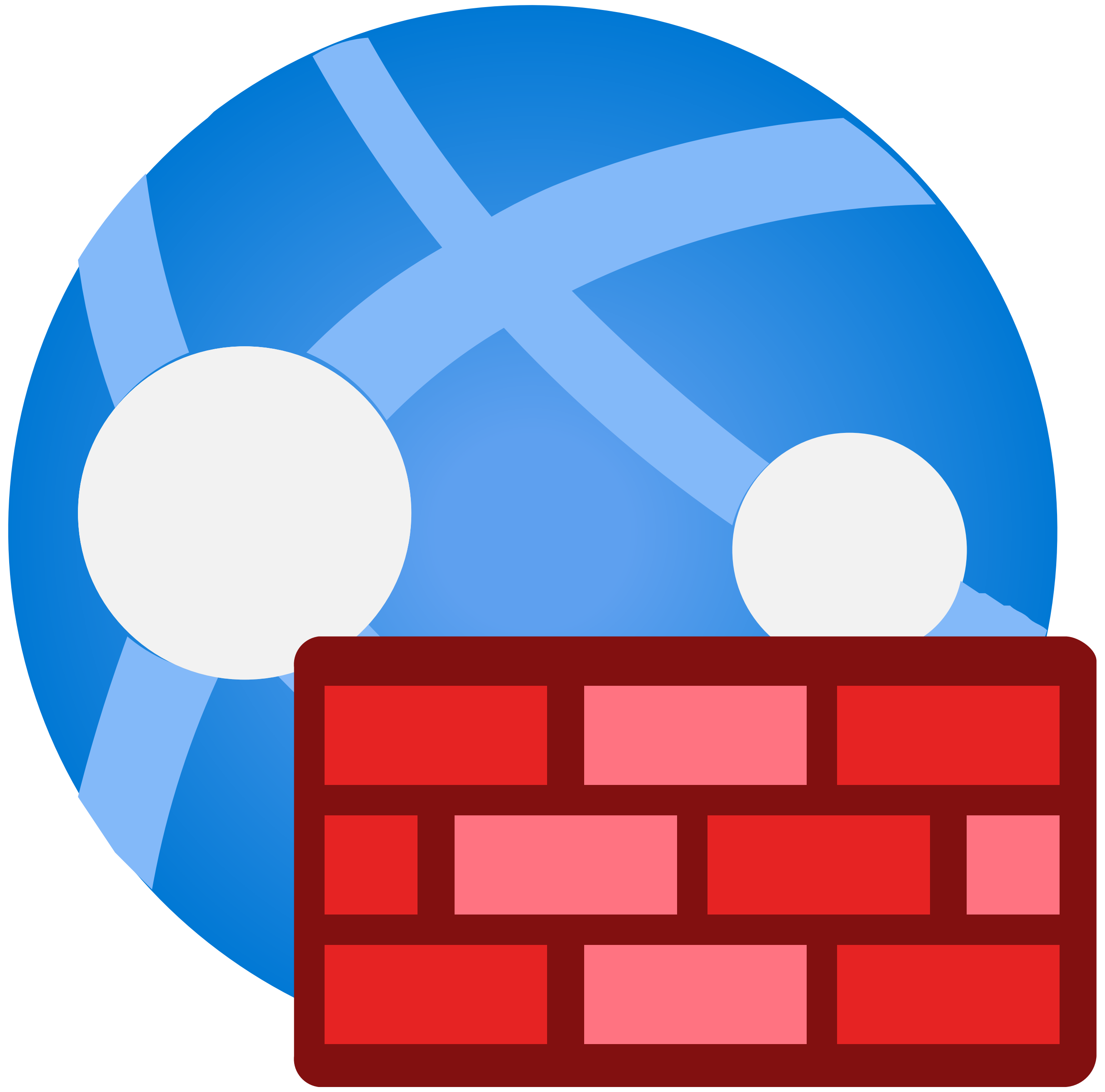
Common threats to application network traffic

- Web application vulnerabilities
- Distributed Denial of Service (DDoS) attacks

Azure services for application network security

- Azure Web Application Firewall (WAF)
- Azure DDoS Protection

Azure Web Application Firewall (WAF)



Key features of Azure WAF

- Protection against OWASP Top 10 vulnerabilities
  - SQL injection, cross-site scripting (XSS), etc.
- Customizable rules and rule groups
  - Defining custom rules based on specific application needs
- Integration with Azure services
  - Azure Application Gateway, Azure Front Door, Azure CDN
- Centralized monitoring and reporting
  - Logging and analytics for security events and trends

Overview of Azure Web Application Firewall (WAF)

- Protects web applications from common exploits and vulnerabilities
- Provides centralized protection for multiple web applications

When to use Azure WAF

- Protecting web applications from common vulnerabilities
- Compliance requirements (e.g., PCI DSS)
- Centralized security management for multiple web applications

Azure DDoS Protection

Key features of Azure DDoS Protection

- Always-on traffic monitoring
  - Continuous monitoring and real-time detection of DDoS attacks
- Adaptive tuning
  - Automatic tuning of application traffic patterns and behavior
- Scalable mitigation
  - Automatically scales to absorb and mitigate large-scale DDoS attacks
- Attack analytics and insights
  - Detailed telemetry and attack insights for post-attack analysis

When to use Azure DDoS Protection

- Protecting mission-critical applications and resources
- Ensuring high availability and business continuity
- Compliance requirements for DDoS protection
- Mitigating the impact of volumetric and protocol attacks

Overview of Azure DDoS Protection

- Protects Azure resources from Distributed Denial of Service (DDoS) attacks
- Provides network and application-level protection

Best Practices for Securing Application Network Traffic

- Implement a layered security approach
- Regular vulnerability assessments and penetration testing
- Keep WAF rules and signatures up to date
- Monitor and analyze security logs and metrics
- Implement security best practices for application development
- Educate and train employees on application security

Scenario: FairBank is a global financial institution that offers online banking services to its customers. They want to ensure the security of their web applications and protect against potential threats.

Requirements:

- Protect web applications from common vulnerabilities, such as SQL injection and cross-site scripting (XSS)
- Defend against DDoS attacks to ensure high availability and business continuity
- Comply with industry regulations and security standards
- Integrate security measures with their existing application infrastructure

Solution:

- **Implement Azure Web Application Firewall (WAF)**
- **Enable Azure DDoS Protection Standard**
- **Integrate with existing security solutions**

Case Study: Networking

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

GlobalTech Inc.

Company Background:

- Multinational technology company with offices in multiple regions
- Provides cloud-based software solutions to enterprise customers
- Experiencing rapid growth and expanding its Azure presence

Current Challenges:

- Inefficient network connectivity between on-premises data centers and Azure
- Lack of secure and scalable remote access for employees
- Inadequate protection against web application vulnerabilities and DDoS attacks
- Difficulty in managing and monitoring network traffic across regions

Goals:

- Establish secure and reliable connectivity between data centers and Azure
- Enable secure and scalable access to cloud resources for remote employees
- Enhance security posture for web applications and protect against DDoS attacks
- Simplify network management and monitoring across multiple regions

Proposed Azure Networking Solution

Hybrid connectivity

Remote access

Security enhancements

Regional traffic distribution

Monitoring and management

Proposed Azure Networking Solution

Hybrid connectivity

Remote access

Security enhancements

Proposed Azure Networking Solution

Implement Azure Traffic Manager

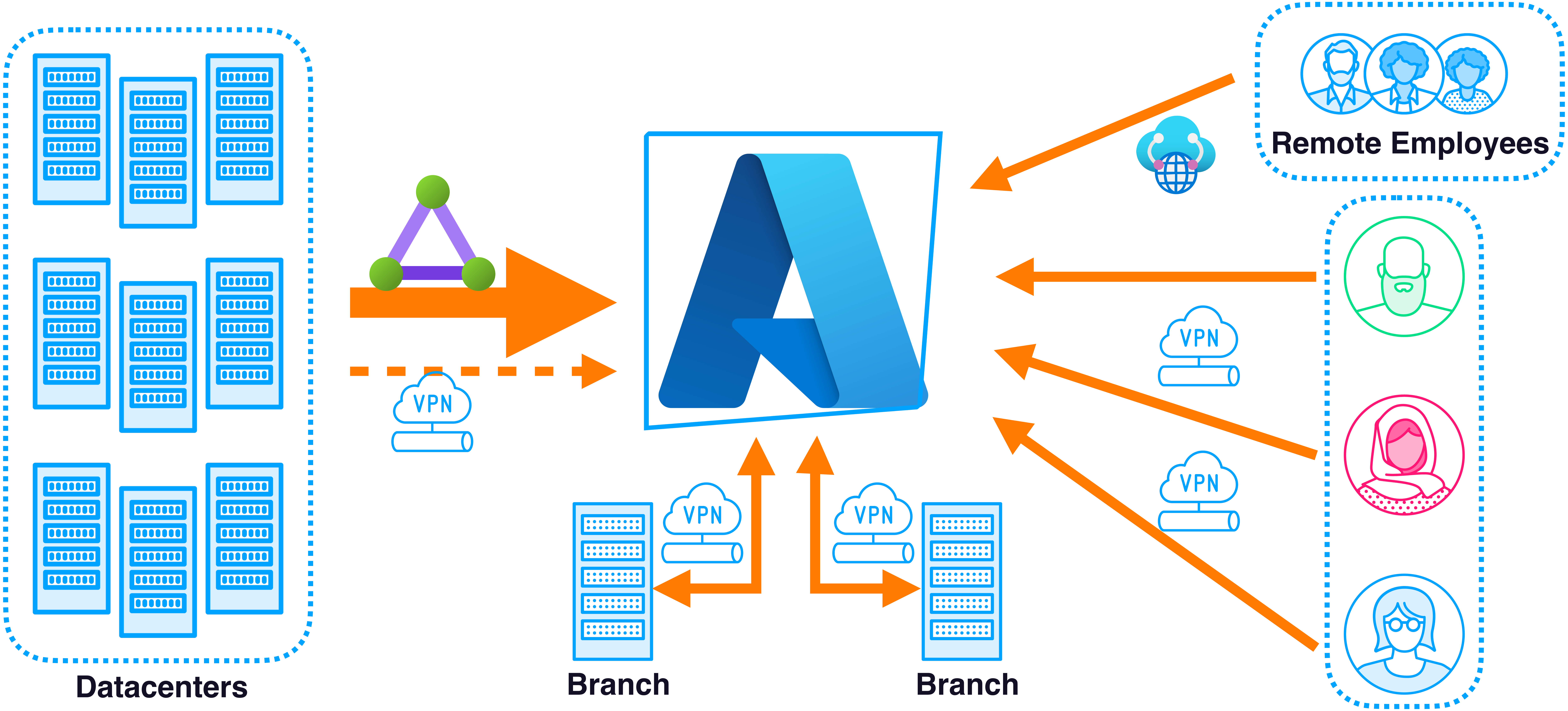
Implement Azure Front Door

Leverage Azure Network Watcher

Use Azure Monitor

Implement Azure Network Security Group (NSG)

Solution Architecture



Solution Architecture

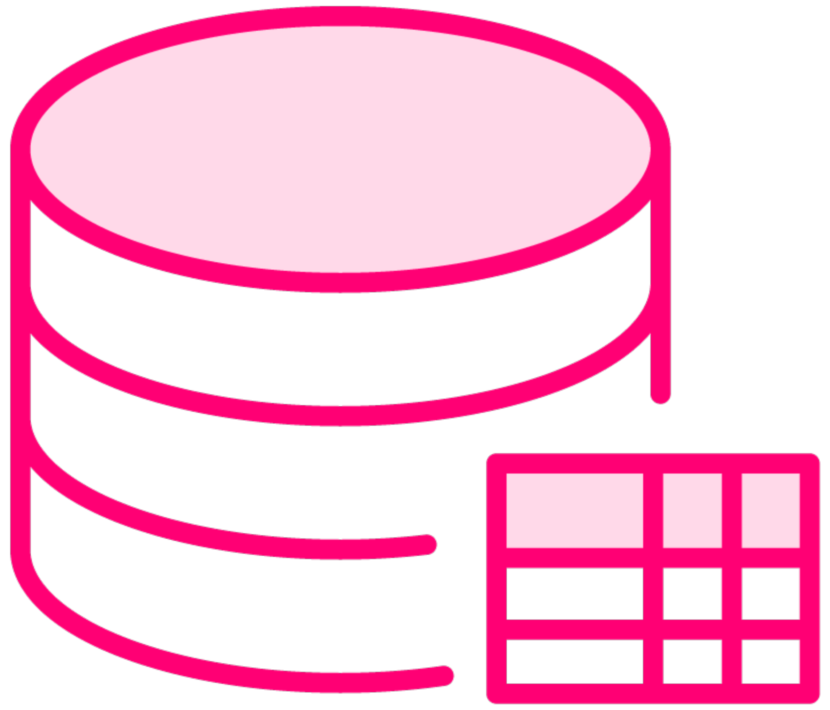
Storage Accounts

Mike Boorman

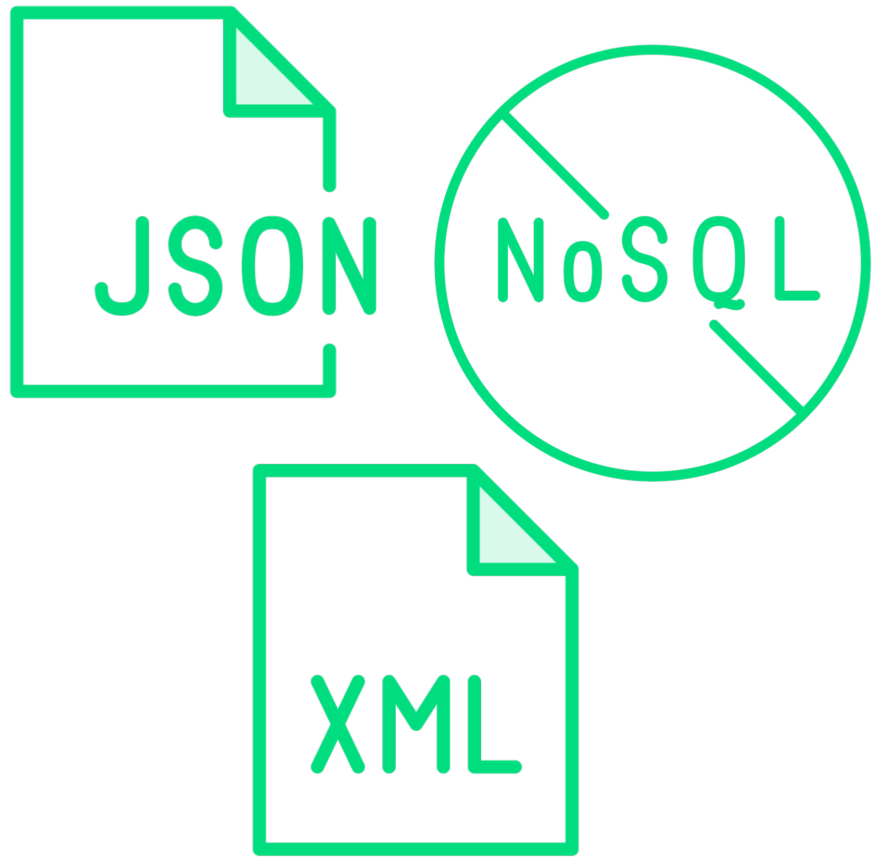
Author, Cloud

@pluralsight | www.pluralsight.com

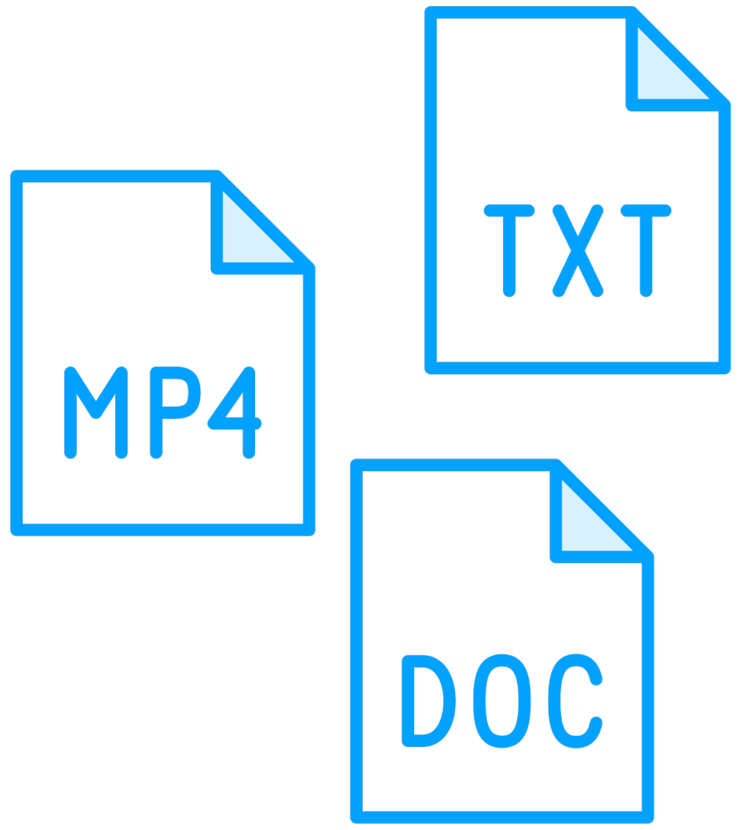
Overview of Data Structures



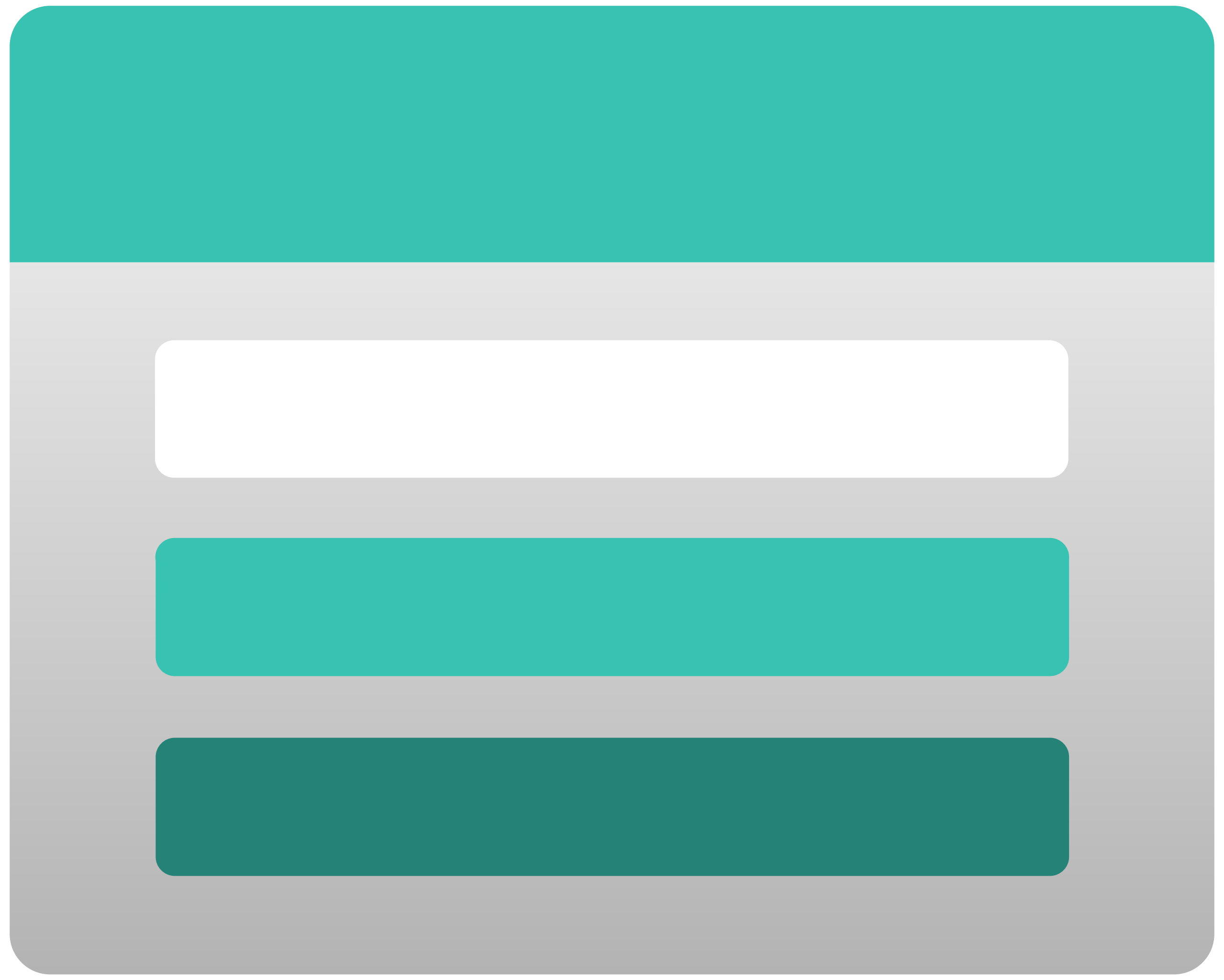
Structured Data
(SQL Databases)



Semi-structured Data



Unstructured Data
(Storage Accounts)



Storage Accounts

- Unique namespace accessible from anywhere
- Collection of settings about storage services
- Storage account types support different services

National and regulatory compliance and security considerations

Storage Account Types

Standard General Purpose v2

Premium Block Blobs

Premium File Shares

Premium Page Blobs

Storage Account Services

Blob Storage

Table Storage

Page Blobs

Queue Storage

Azure Files

Data Lake Storage

Storage Account Tiers

Access

Hot | Cool | Cold | Archive

Performance

Standard | Premium

Storage Account Redundancy

Local
(LRS)

Zone
(ZRS)

Geo
(GRS)

Read-access Geo
(RA-GRS)

Authentication and Authorization

Access Keys

Share Access Signatures (SAS)

Azure Role-Based Access Control (RBAC)

Encryption

Encryption at-rest

Encryption in-transit

Azure Key Vault Integration

Virtual Network Integration

Service endpoints

Private links

Firewall rules

Cost Optimization

Access Tier

Resiliency

Redundancy Implications

Object Lifecycle Management

Scenario 1 - File Storage for Corporate Shares

- Need to migrate 500 TB file shares from on-premises to cloud
- Shares accessed from multiple global office locations
- Infrequently accessed reference data

Solution: Azure File Storage, Standard Tier, Cool Access, Geo-redundant

Scenario 2 - Blob Storage for Video Content

- Storing media assets and video content
- Accessed frequently in region during editing, but rarely afterwards
- Total storage will reach 1 PB over next 3 years

Solution: Azure Blob Storage with Hot and Cool tiers, locally redundant storage, and either object lifecycle management or Archive tier to manage long-term costs.

Blob Storage

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Blob Storage Fundamentals

- Unstructured object storage in Azure
- Highly scalable and durable
- Accessed via HTTP/HTTPS

Blob Storage Types

Block Blobs

Append Blobs

Page Blobs

Blob Storage Tiers and Performance

Access

Hot | Cool | Cold | Archive

Performance

Standard | Premium

Blob Storage Security

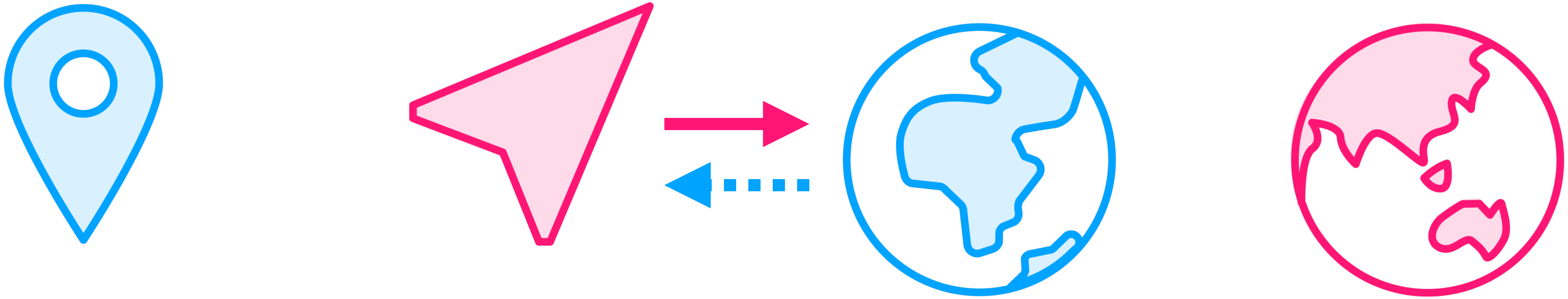
Authentication and Authorization

- Access Keys
- Share Access Signatures (SAS)

Encryption

- Encryption at-rest
- Encryption in-transit

Blob Storage Reliability and Disaster Recovery



Local
(LRS)

Zone
(ZRS)

Geo
(GRS)

Read-access Geo
(RA-GRS)

Blob Lifecycle Management

Automate Blob tiering and deletion

Reduce storage costs

Define rules based on Blob prefix, tags, or Blob index tags

Data Protection Strategies

- Soft delete for accidental or malicious deletion
- Versioning for maintaining previous versions
- Immutable storage for WORM compliance
- Point-in-time restore for block Blobs

Scenario - Design a Blob Storage Solution

- Customer needs to store application backups and logs
- Point-in-time restore required for up to 30 days
- Backups rarely accessed, but must be kept for 7 years

Solution: Use Blob Versioning and Soft Delete for point-in-time restore. Enable GRS for disaster recovery. Use Lifecycle Management to transition backups to Archive tier after 30 days. Configure immutable Blob policies for 7 year retention.

Data Security

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Classifying Data Sensitivity

- Public, Internal, Confidential, Restricted
- Use tags and metadata to classify blobs
- Apply appropriate security controls based on sensitivity

Blob Replication Options

Locally-redundant storage (LRS)

Zone-redundant storage (ZRS)

Geo-redundant storage (GRS)

Read-access geo-redundant storage (RA-GRS)

Understand replication for disaster recovery and high availability

Immutable Blob Storage

- Write Once, Read Many (WORM) policies
- Time-based retention and legal holds
- Ensure data integrity and compliance
- Understand immutability for regulatory requirements

Shared Access Signatures (SAS) Best Practices

- Use short expiration times
- Prefer stored access policies over ad hoc SAS
- Use minimum required permissions
- Enable HTTPS only
- Regenerate SAS keys periodically

Encryption for Blob Storage

Encryption at rest with Microsoft-managed or customer-managed keys

Encryption in transit with HTTPS

Understand encryption options and key management

Secure Transfer Required

- Enforce HTTPS for all API interactions
- Reject requests over HTTP
- Understand secure transfer options and configuration

Firewall and Virtual Network Rules

Allow or deny public access

Restrict access to specific virtual networks

Understand network-level security options

Firewall and Virtual Network Rules

Connect privately to Blob storage from VNets

Extend VNet security to storage

Understand private and service endpoint configuration and use cases

Scenario - Design Secure Blob Storage

- Customer needs to store sensitive financial data
- Data must be encrypted and accessible only from their VNet
- Accidental deletion must be prevented

Scenario - Design Secure Blob Storage

Solution:

- Use Blob Storage with private endpoints for VNet-only access.
- Enable encryption at rest with customer-managed keys.
- Configure immutable Blob policies to prevent deletion.
- Use RA-GRS for geo-redundancy and high availability.

File Storage

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Introduction to Azure File Storage

Azure Files

Azure File Sync

Azure NetApp Files

Azure Files

Managed file shares hosted in Azure Storage Accounts

Supports SMB 2.1, SMB 3.0, and NFS 4.1 protocols

Compatible with Windows, Linux, and macOS clients

Accessible via Azure portal, PowerShell, CLI, or REST API

Azure File Shares

Premium

Standard

Redundancy

Snapshots

Azure File Sync

Centralize on-premises file shares in Azure Files

Cache frequently accessed data on-premises

Synchronize across multiple servers and locations

Azure File Sync Deployment

- Install Storage Sync Service and agents
- Register servers and create sync groups
- Configure cloud tiering and offline data transfer

Azure NetApp Files

High-performance file storage for demanding workloads

Sub-millisecond latency and high throughput

Supports NFS, SMB, and dual-protocol access

Azure NetApp Files Use Cases

SAP and Oracle workloads

High-performance computing (HPC)

VDI and collaboration platforms

Security and Access Control

SMB and NFS authentication and authorization

RBAC for share-level access control

Encryption at rest and in transit

Backup and Disaster Recovery

Azure Backup integration for Azure Files

Cross-region replication with GRS and RA-GRS

NetApp Files cross-region replication and SnapMirror

Scenario - Design File Storage Solution

- Customer needs to migrate on-premises file servers to Azure
- Require sub-millisecond latency for database files
- Need to retain file share snapshots for 90 days

Scenario - Design File Storage Solution

Solution:

- Use Azure File Sync to migrate on-premises shares to Azure Files.
- Use Azure NetApp Files for database files requiring low latency.
- Configure Azure Files snapshots with 90-day retention.
- Use RA-GRS for disaster recovery.

File and Blob Data Protection

Mike Boorman

Author

@pluralsight | www.pluralsight.com

Blob Soft Delete

- Protects against accidental or malicious deletion of Blobs
- Provides a configurable retention period for deleted Blobs
- Permits restoration of whole containers

Point-in-Time Restore

Allows restoring Blobs to an earlier point in time

Useful for recovering from data corruption or application errors

Immutable Storage

- Ensures data cannot be modified or deleted for a specified period
- Helps comply with regulatory requirements and legal holds
  - Financial services, healthcare, and other regulated industries

Azure Files Backup and Recovery

Centralized backup management for Azure Files

Supports various backup scenarios (full, incremental, etc.)

Restore individual files or entire file shares

Scenario:

A financial institution needs to store and protect sensitive customer data in the cloud while ensuring compliance with regulatory requirements.

Solution:

- Use Azure Blob Storage with Soft Delete and Point in Time Restore enabled
- Configure immutable storage for Blobs containing sensitive data
- Implement Azure Backup and Recovery for Azure Files to protect and restore file shares

Migrating File and Blob Data

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Azure Migrate: Databox

- Secure, offline data transfer to Azure
  - Disk, Heavy, Edge
- Suitable for large data volumes (up to 80 TB)
  - Limited network bandwidth
  - Large initial volumes of data

Azure Storage Migration Service

Migrates on-premises file servers to Azure

Supports various migration scenarios (lift and shift, phased migration)

Assess, migrate, and cutover file servers to Azure

Minimize downtime during cloud migrations

Azure Import/Export Service

Securely transfer large amounts of data to Azure using physical disks

Suitable for one-time migrations or scenarios with limited network bandwidth

AzCopy Utility

Command-line utility for copying data to and from Azure Storage

Supports various data transfer scenarios (blob, file, table, queue)

High-performance data transfer with resume and sync capabilities

Service Comparison

Solution	Data Volume	Use Case	Transfer Method	Ongoing Sync
Azure Migrate: Databox	Up to 80 TB	Large one-time data migrations	Offline (hardware)	No
Azure File Sync	Varies	Hybrid file sharing and synchronization	Online (network)	Yes
Storage Migration Service	Varies	Migrating on-premises file servers to Azure	Online (network)	No
Import/Export Service	Up to 80 TB	Large one-time data migrations	Offline (disks)	No
AzCopy	Varies	Copying data to/from Azure Storage	Online (network)	No

Service Comparison

- **If large one-time data migration:**
  - If offline transfer is feasible: Azure Migrate: Databox or Import/Export Service
  - If online transfer is preferred: AzCopy or Storage Migration Service
- **If ongoing synchronization is needed:**
  - If hybrid file sharing: Azure File Sync
  - If migrating on-premises file servers: Storage Migration Service
- **If copying data to/from Azure Storage: AzCopy**

Case Study: File and Blob Storage

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Reroute Media Group

Company Background:

- Global marketing agency with offices in multiple countries
- Specializes in creating and managing digital marketing campaigns
- Handles large volumes of media files (images, videos, documents)

Current Challenges:

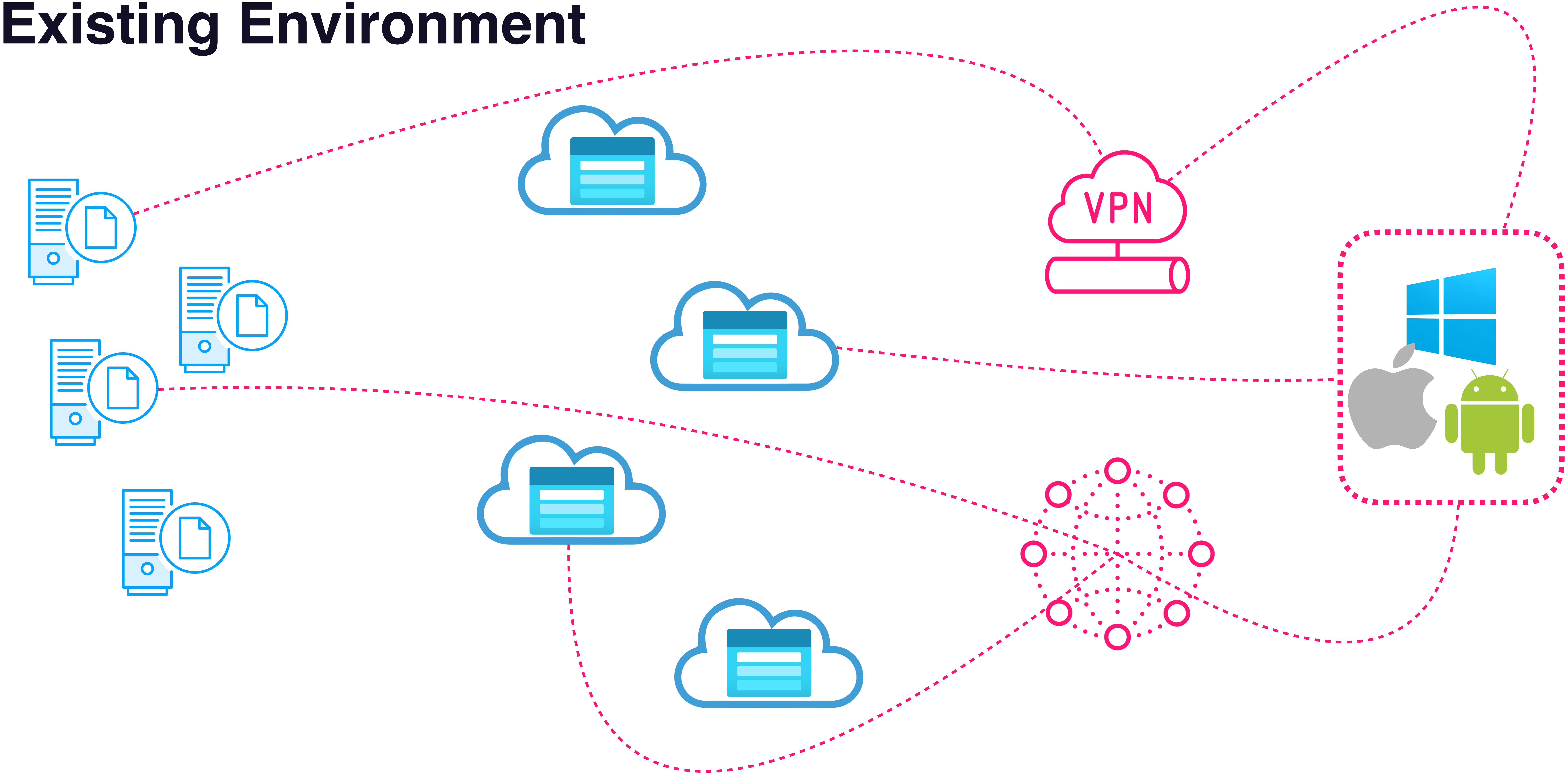
- Inefficient file sharing and collaboration across teams
- Inconsistent data storage and management practices
- Increasing storage costs and complexity

Reroute Media Group

Goals:

- Centralize file storage and improve collaboration
- Ensure data security and compliance
- Optimize storage costs and simplify management

Existing Environment



Requirements

Requirements

Centralized file storage:

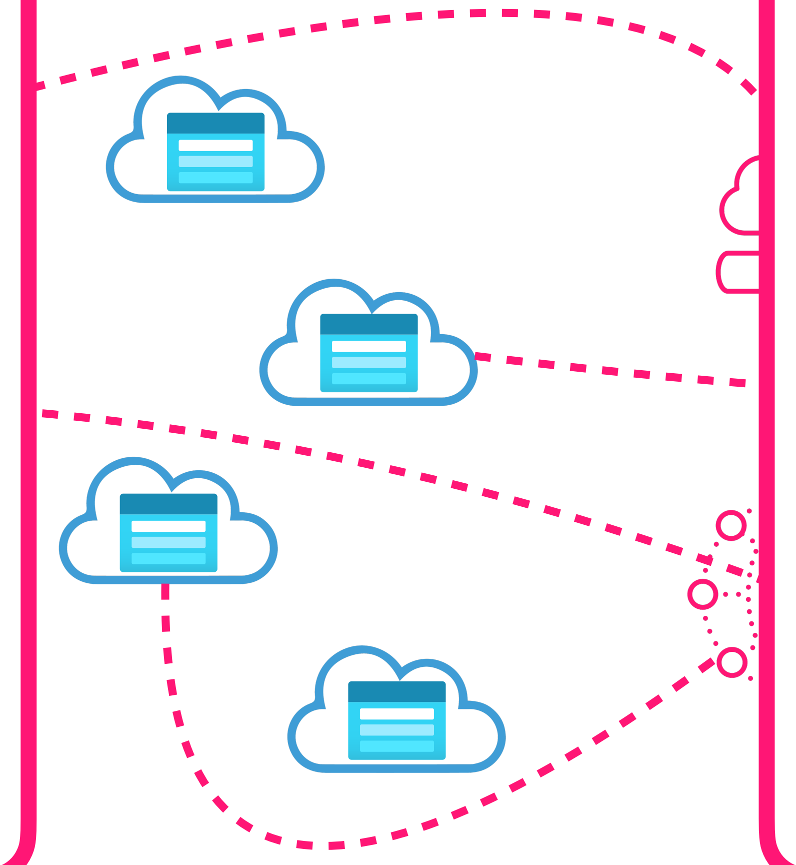
- Consolidate files into a single cloud-based storage solution
- Enable seamless file sharing and collaboration across teams

Scalability and performance:

- Accommodate growing data volumes without disruption
- Ensure fast and reliable access to files from anywhere

Security and compliance:

- Implement granular access controls and permissions
- Encrypt data at rest and in transit
- Meet regulatory requirements (e.g., GDPR, HIPAA)



Requirements

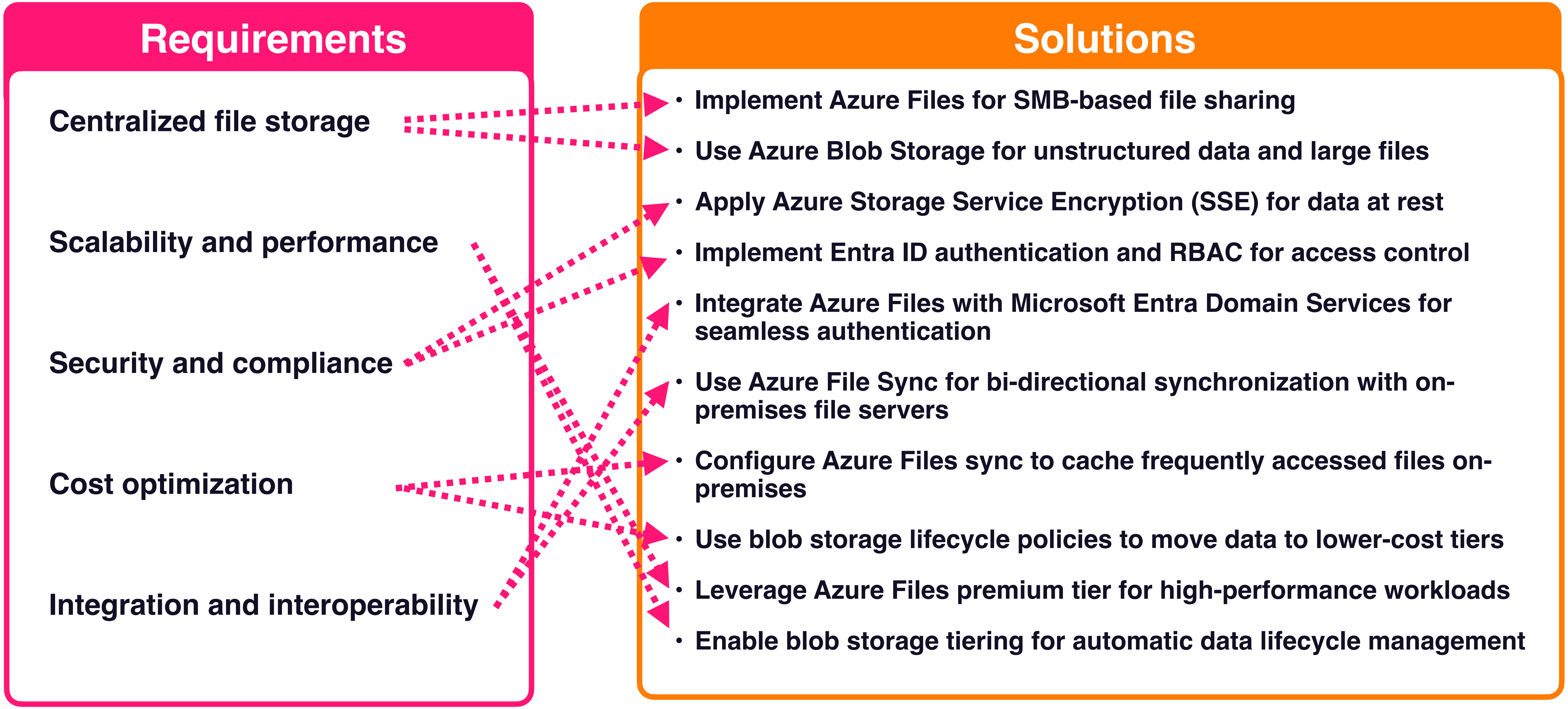
Cost optimization:

- Minimize storage costs while maintaining performance
- Implement lifecycle management policies for data archival

Integration and interoperability:

- Integrate with existing productivity tools and workflows
- Support access from various devices and platforms

Solutions



Requirements

Centralized file storage

Scalability and performance

Security and compliance

Cost optimization

Integration and interoperability

Solutions

- Implement Azure Files for SMB-based file sharing
- Use Azure Blob Storage for unstructured data and large files
- Apply Azure Storage Service Encryption (SSE) for data at rest
- Implement Entra ID authentication and RBAC for access control
- Integrate Azure Files with Microsoft Entra Domain Services for seamless authentication
- Use Azure File Sync for bi-directional synchronization with on-premises file servers
- Configure Azure Files sync to cache frequently accessed files on-premises
- Use blob storage lifecycle policies to move data to lower-cost tiers
- Leverage Azure Files premium tier for high-performance workloads
- Enable blob storage tiering for automatic data lifecycle management

Conclusion and Next Steps

Mike Boorman

Author, Cloud

@pluralsight | www.pluralsight.com

Cloud and Hybrid Network Connectivity

Securing External and Internal Network Traffic

Distributing Regional and Global Application Traffic

Securing Application Network Traffic

Being an Architect

Three Things That You Need to Know

1 Solution Architects map requirements to solutions.

2 Enable stakeholders to make informed decisions when trading off between requirements.

3 Follow-up.

Key Outcomes

Use all of the course content. Don’t skip the quizzes and hands-on labs.

WHATS NEXT

Follow the AZ-305 learning path to prepare for the exam.

Keep going on your cloud journey!