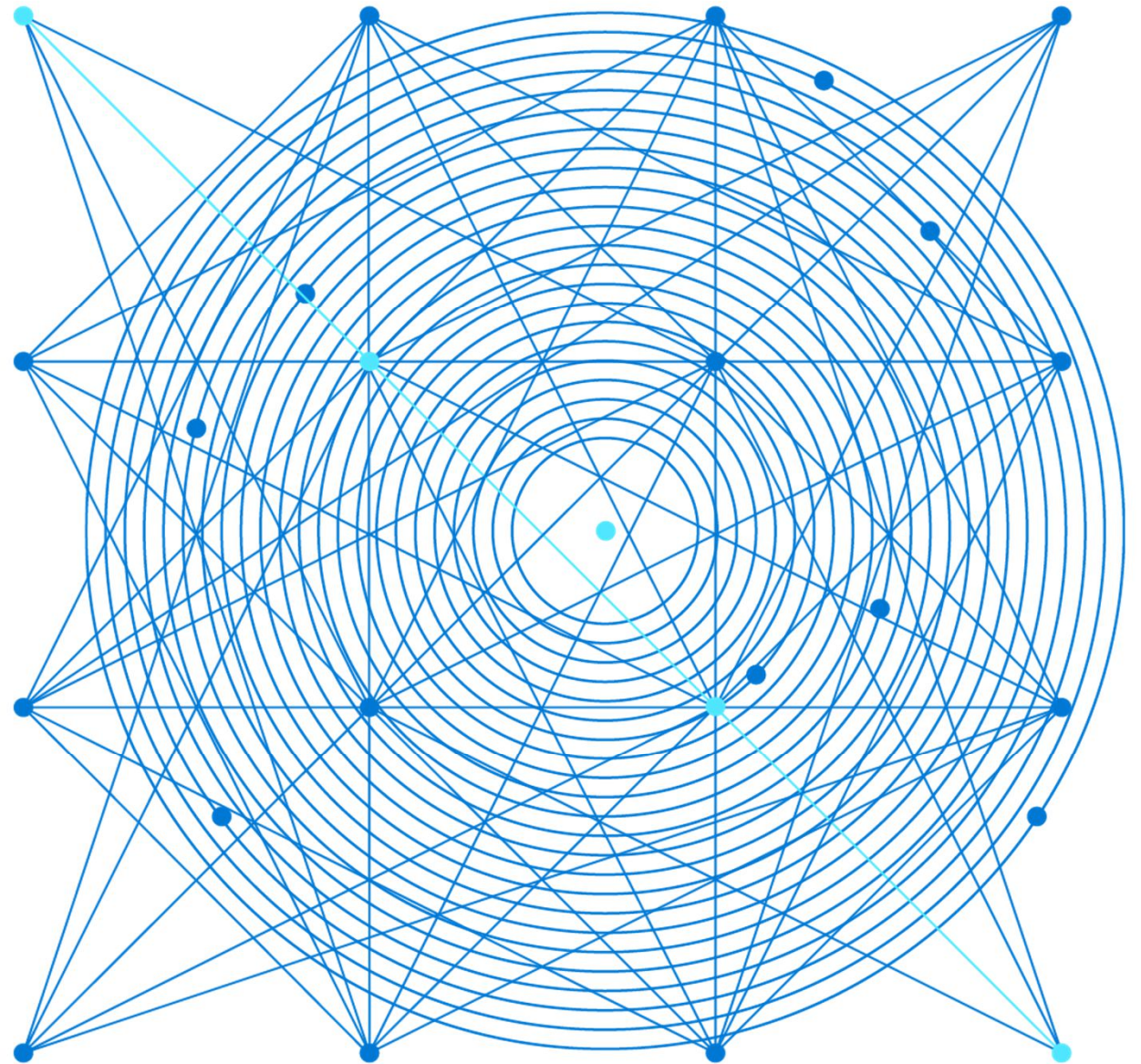


AZ-303: Microsoft Azure Architect Technologies



Module 5: Implement Load Balancing and Network Security

Azure Load Balancer, Application Gateway, Azure Firewall, and Azure Traffic Manager

Learning Objectives

You will learn the following:

- Implement Azure Load Balancer
- Implement an Application Gateway
- Web Application Firewall
- Implement Azure Firewall
- Implement Azure Front Door
- Implementing Azure Traffic Manager
- Implement Network Security Groups and Application Security Groups
- Implement Azure Bastion

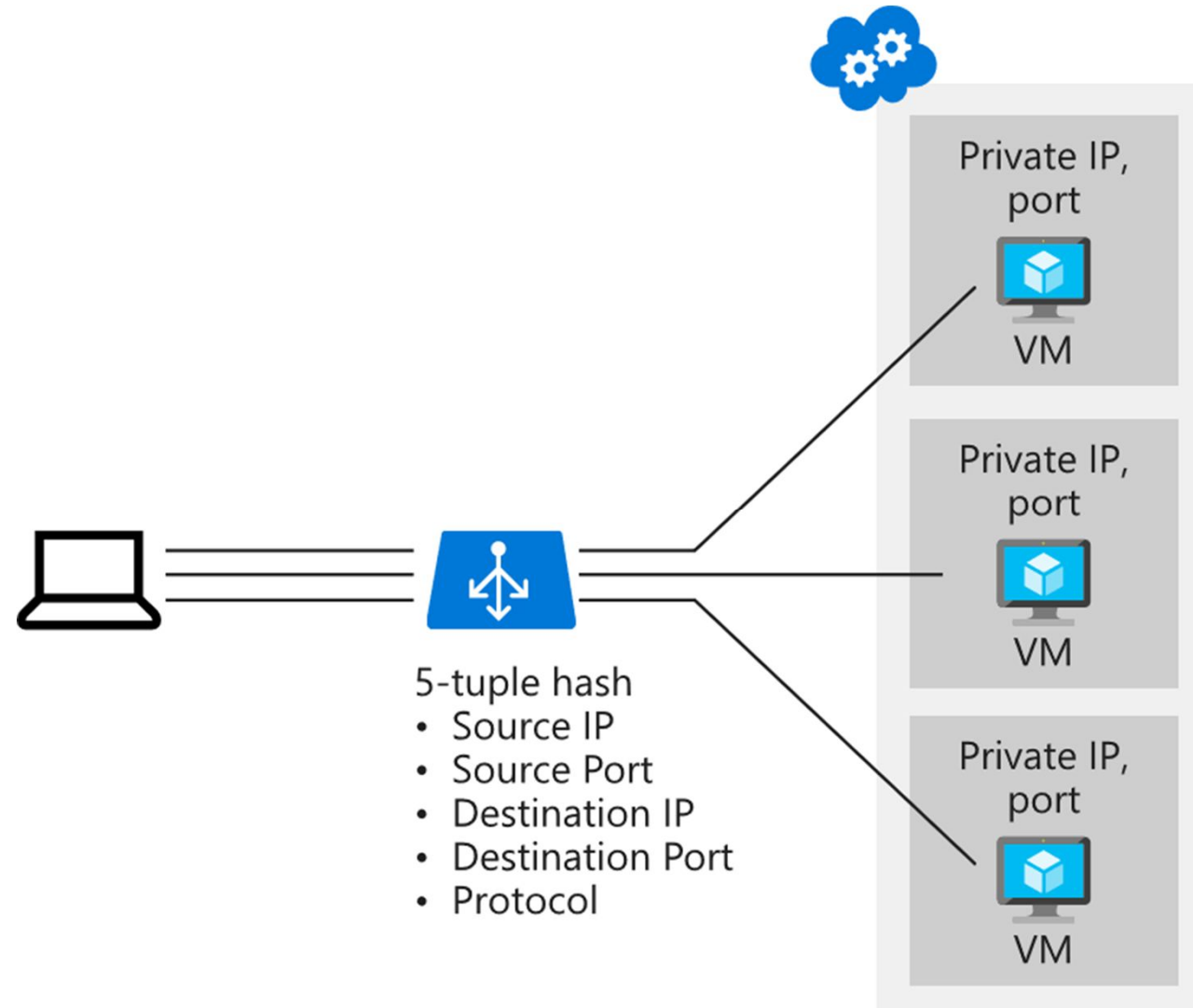


Implement Azure Load Balancer



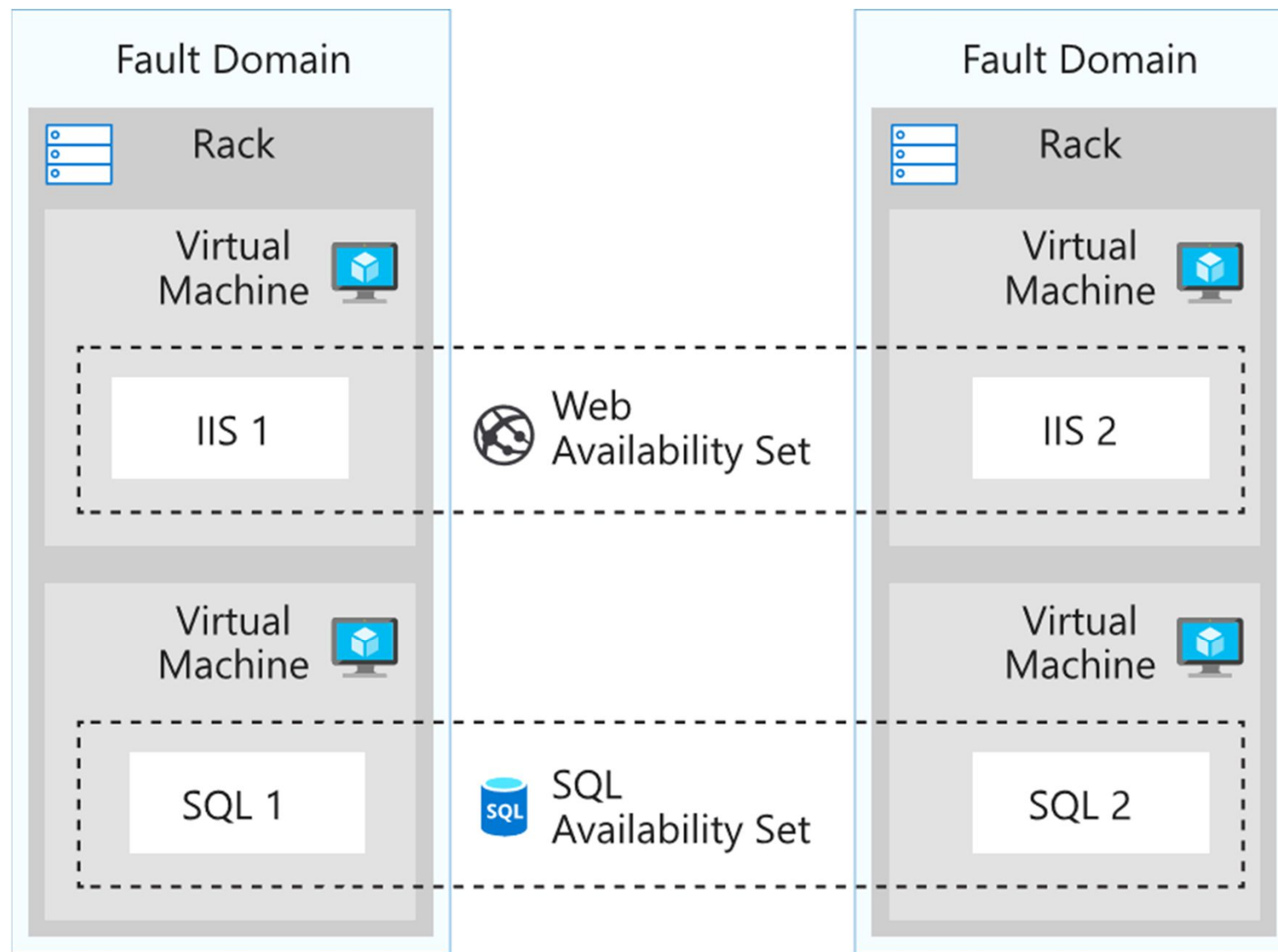
Distribute Traffic with Azure Load Balancer (1 of 3)

- Distribute traffic with Azure load balancer based on
 - Source IP
 - Source port
 - Destination IP
 - Destination port
 - Protocol type



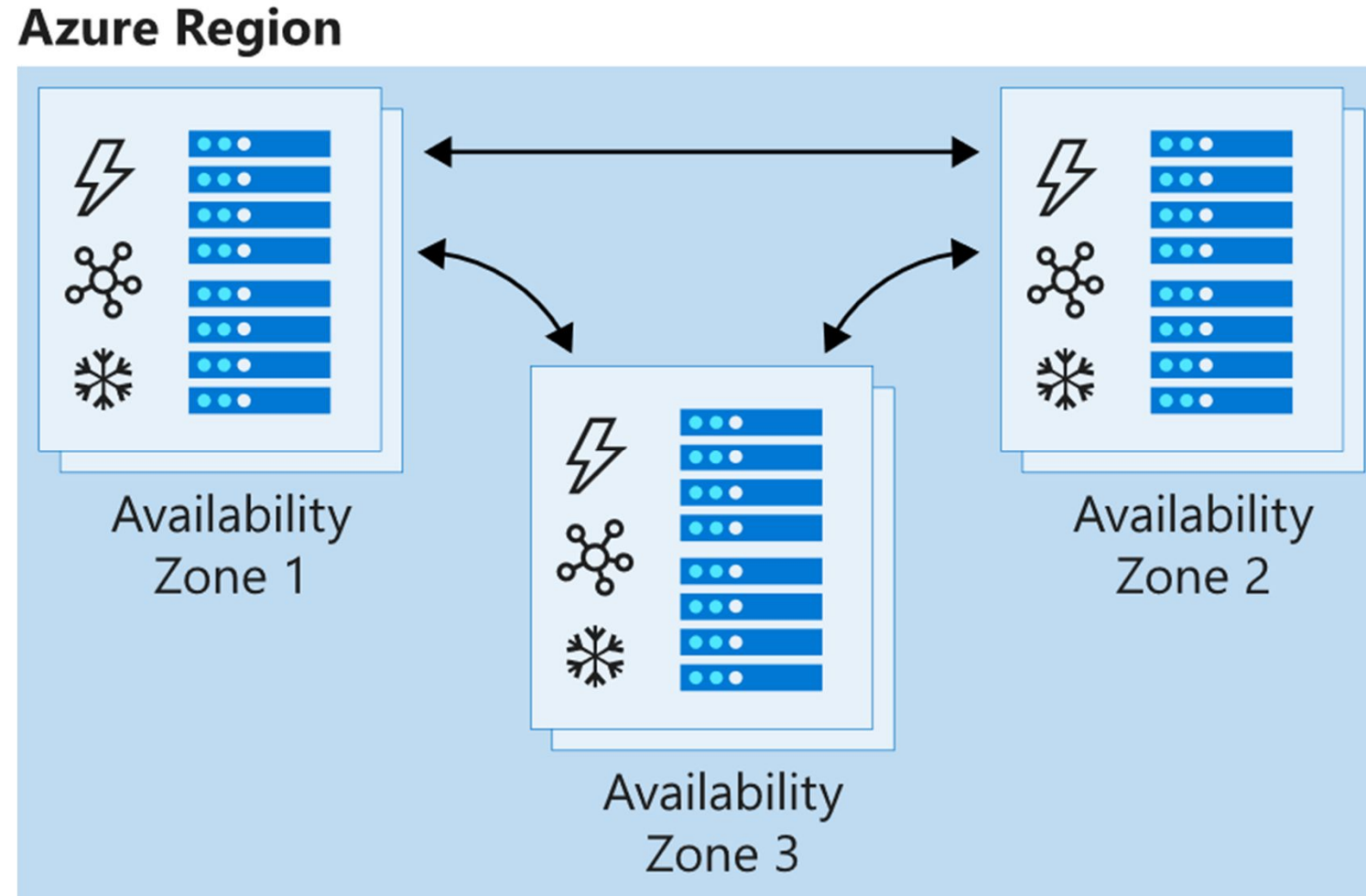
Distribute Traffic with Azure Load Balancer (2 of 3)

- Availability sets



Distribute Traffic with Azure Load Balancer (3 of 3)

- Availability zones



Select a Load Balancer Solution

Basic load balancers allow:

- Port forwarding
- Automatic reconfiguration
- Health probes
- Outbound connections through source network address translation (SNAT)
- Diagnostics through Azure Log Analytics for public-facing load balancers

Standard load balancers support all basic features and allow:

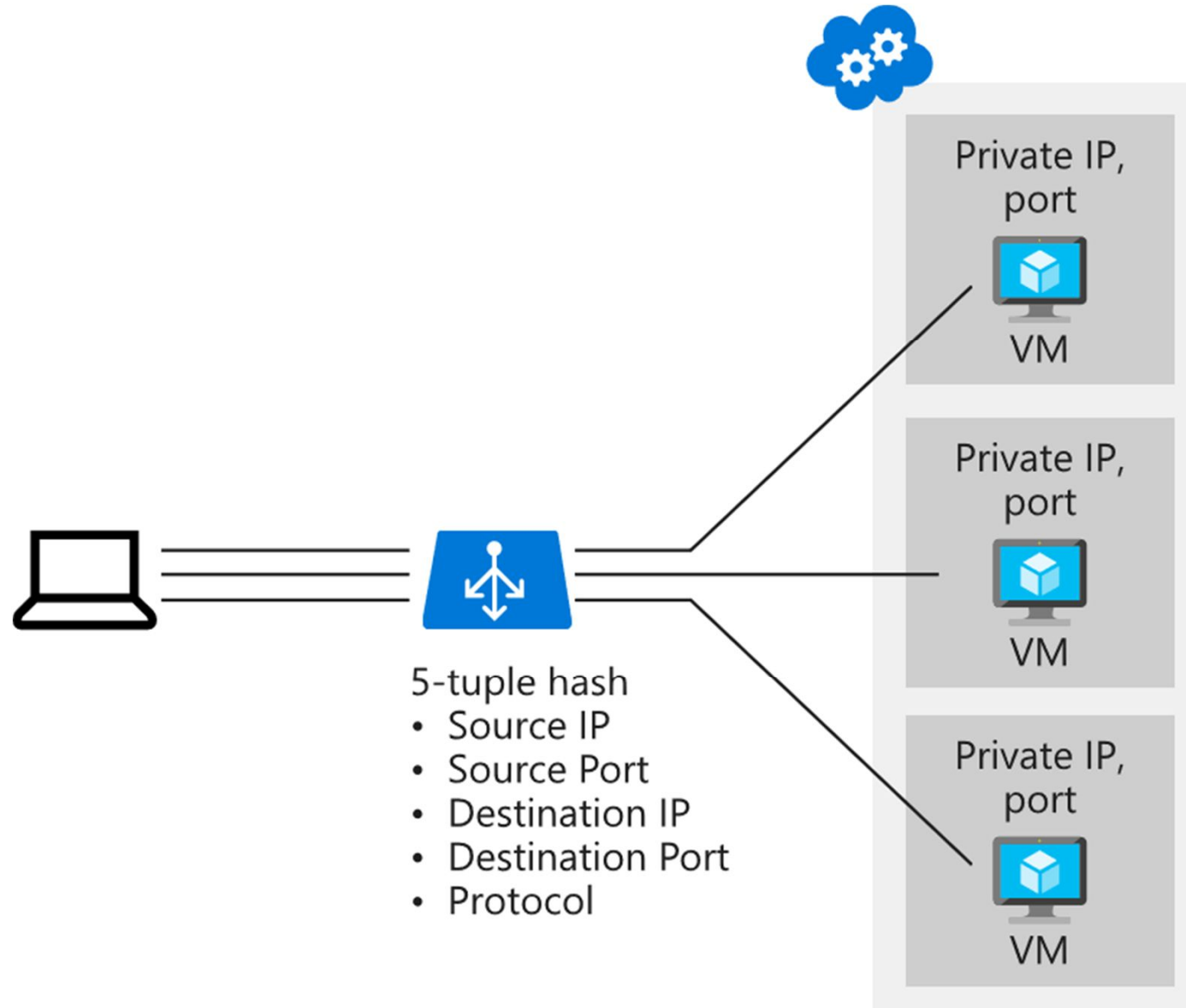
- HTTPS health probes
- Availability zones
- Diagnostics through Azure Monitor, for multidimensional metrics
- High availability (HA) ports
- Outbound rules
- A guaranteed SLA (99.99% for two or more virtual machines in different zones)



Configure a Public Load Balancer (1 of 3)

Distribution mode

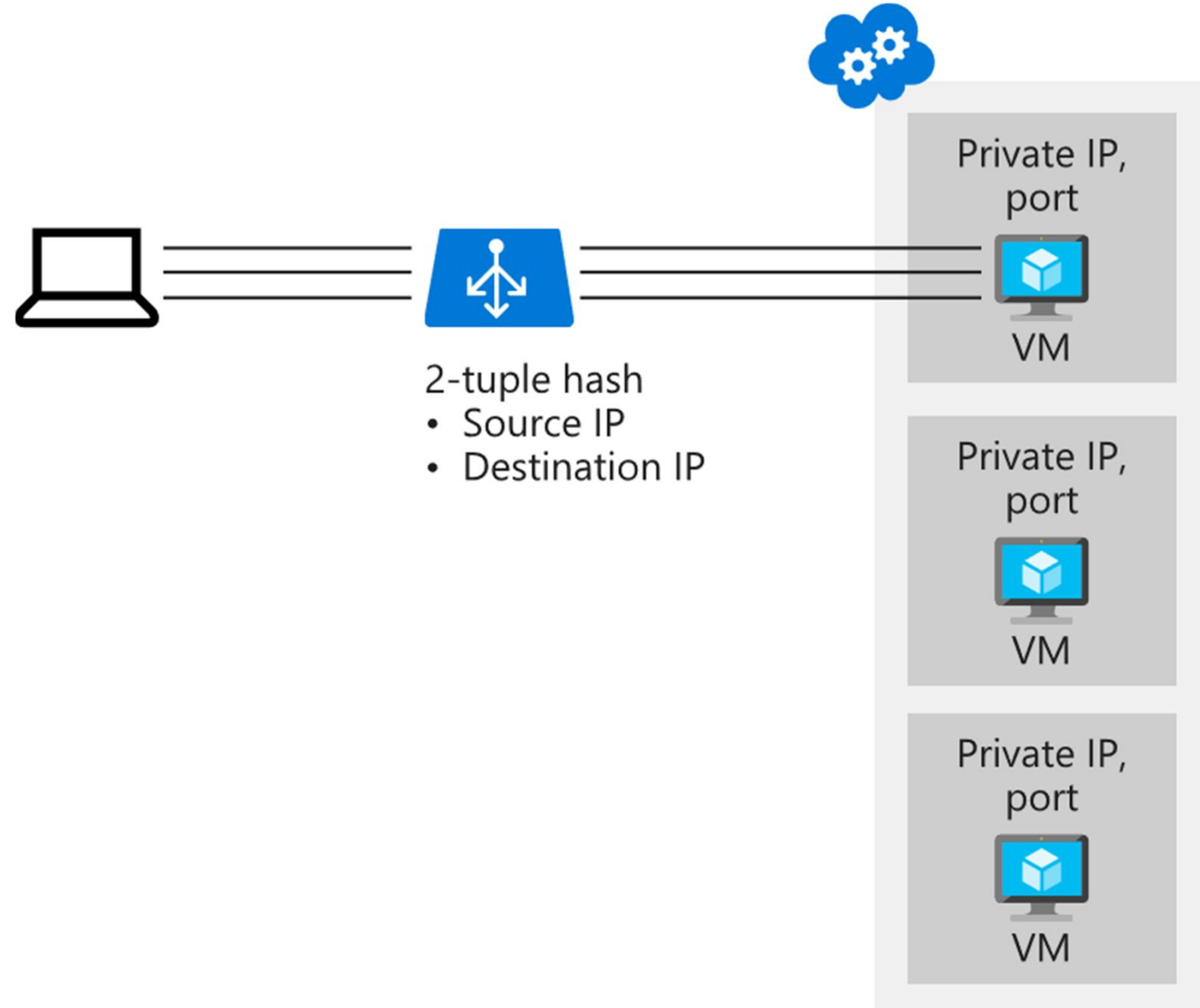
- Five-tuple hash



Configure a Public Load Balancer (2 of 3)

Distribution mode

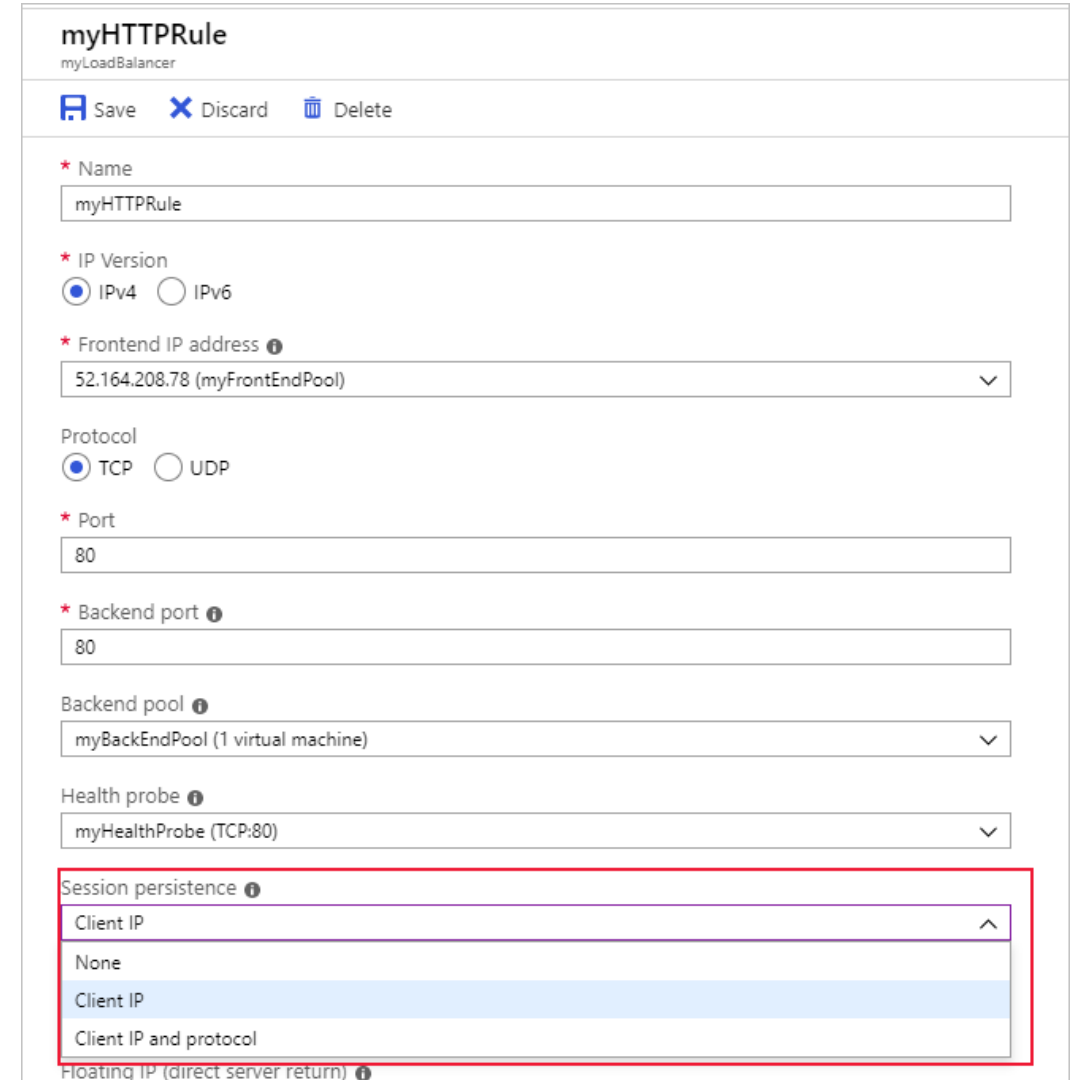
- Source IP affinity



Configure a Public Load Balancer (3 of 3)

Choose a distribution mode

- None
- Client IP (use for Remote Desktop Gateway)
- Client IP and protocol



myHTTPRule
myLoadBalancer

Save Discard Delete

* Name
myHTTPRule

* IP Version
☒ IPv4 ☐ IPv6

* Frontend IP address ⓘ
52.164.208.78 (myFrontEndPool) ▼

Protocol
☒ TCP ☐ UDP

* Port
80

* Backend port ⓘ
80

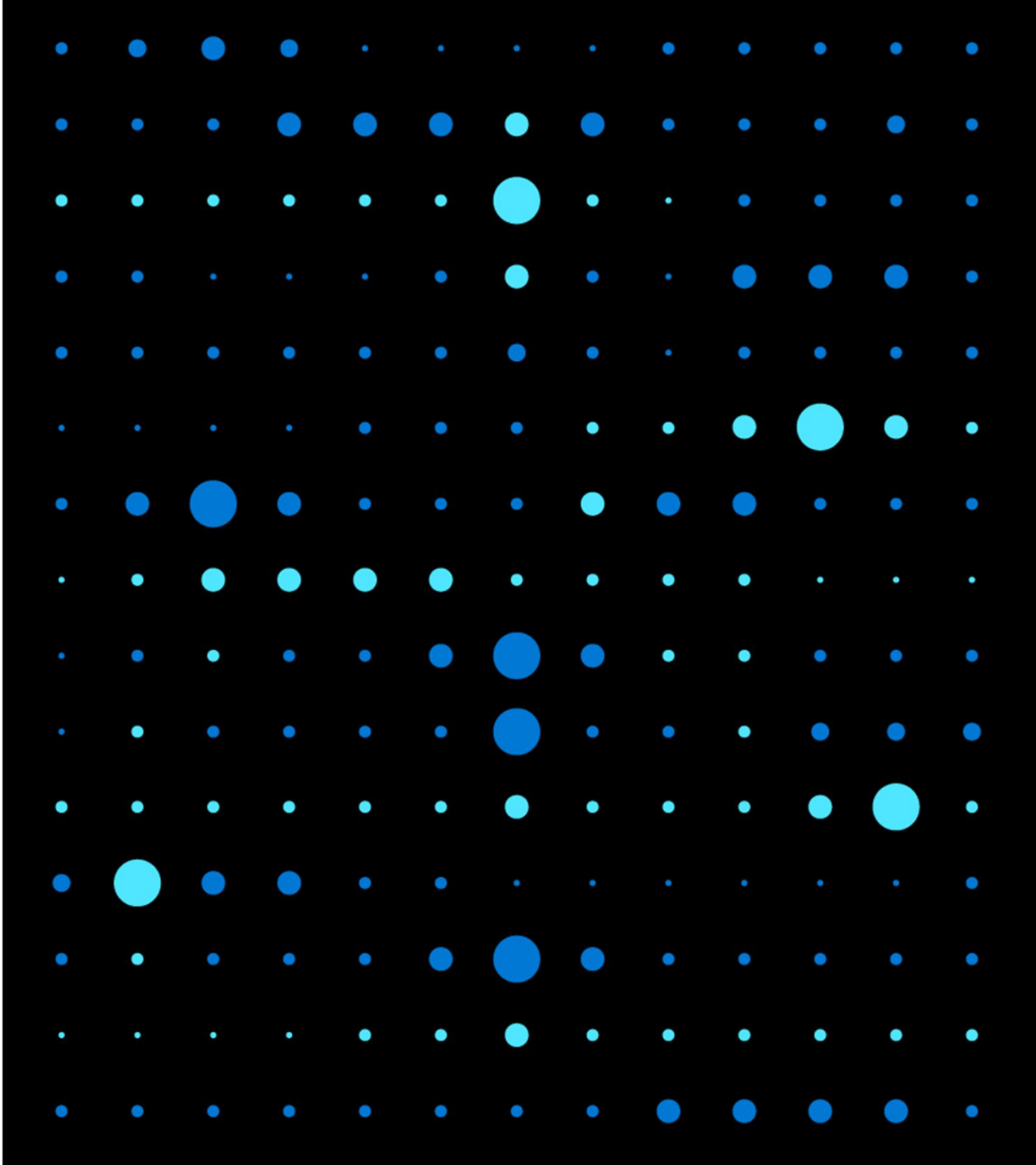
Backend pool ⓘ
myBackEndPool (1 virtual machine) ▼

Health probe ⓘ
myHealthProbe (TCP:80) ▼

Session persistence ⓘ
Client IP ^
None
Client IP
Client IP and protocol
Floating IP (direct server return) ⓘ

Demonstration: Create a Load Balancer to Load Balance VMs

- Create a load balancer
- Create load balancer resources
- Create virtual machines
- Create NSG rule
- Install IIS
- Test the load balancer

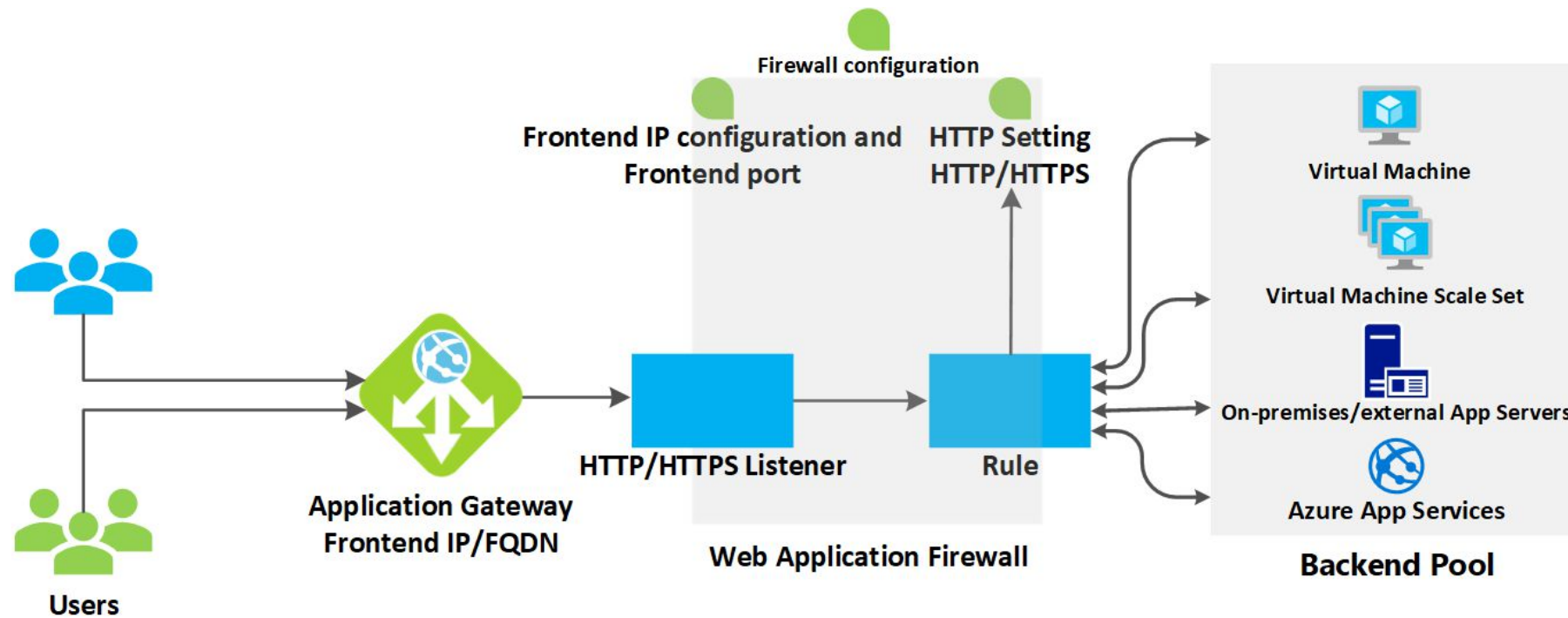


Implement an Application Gateway



Application Gateway (1 of 2)

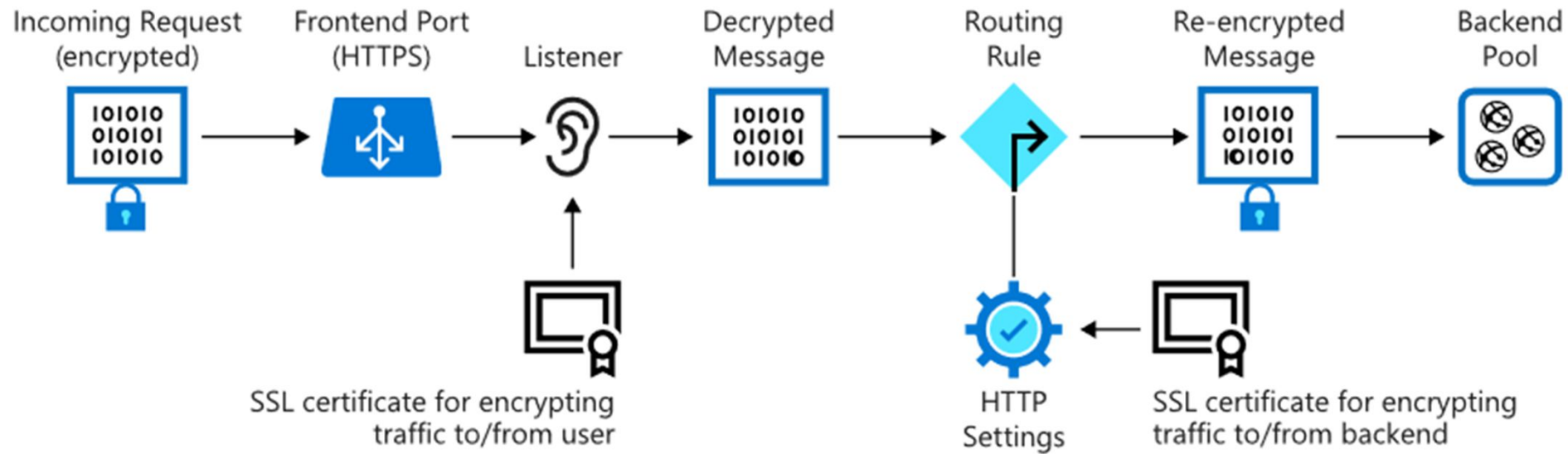
How an application gateway accepts a request



Application Gateway (2 of 2)

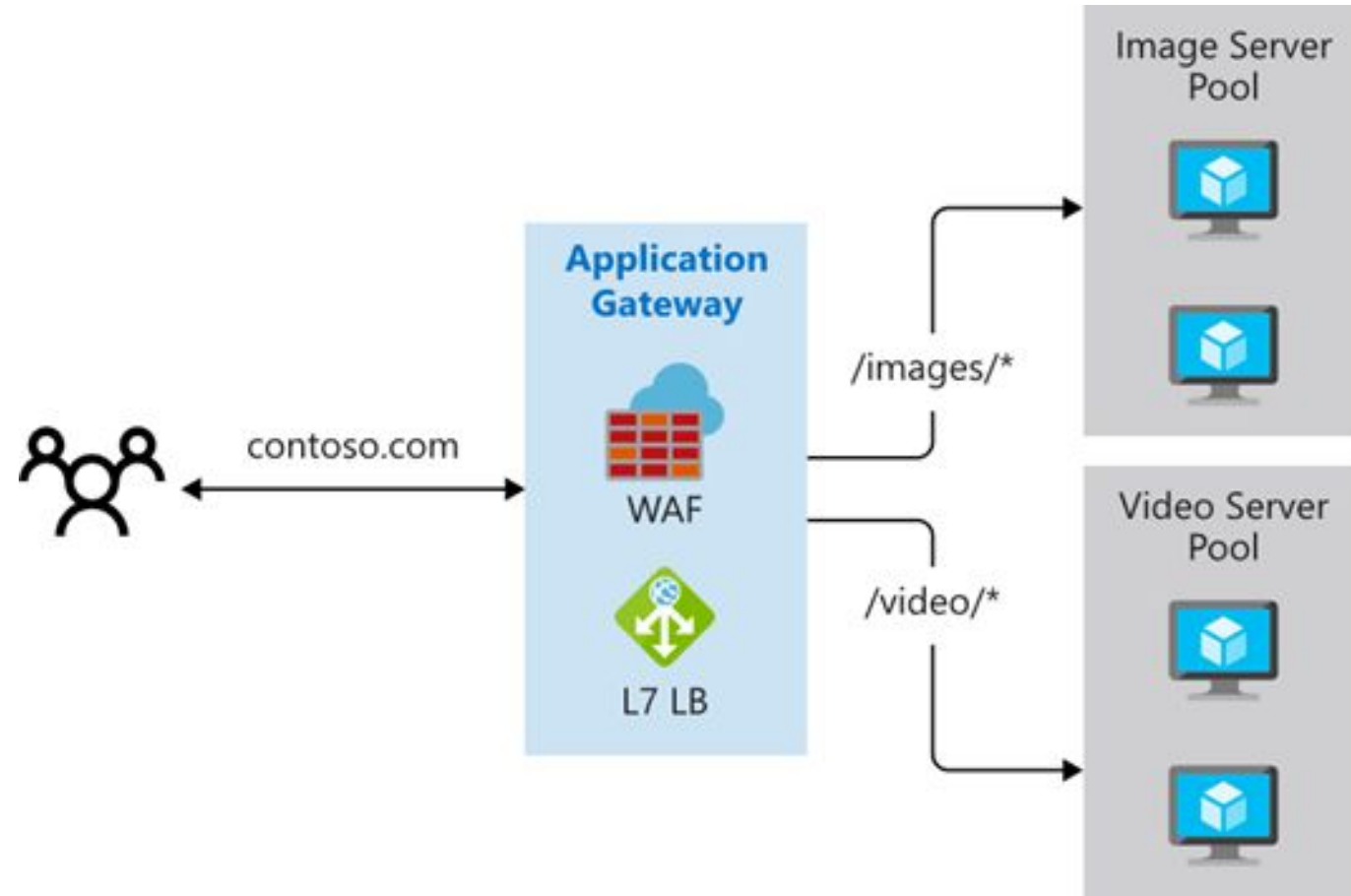
Application gateway components:

- Frontend port and listener
- Backend pool



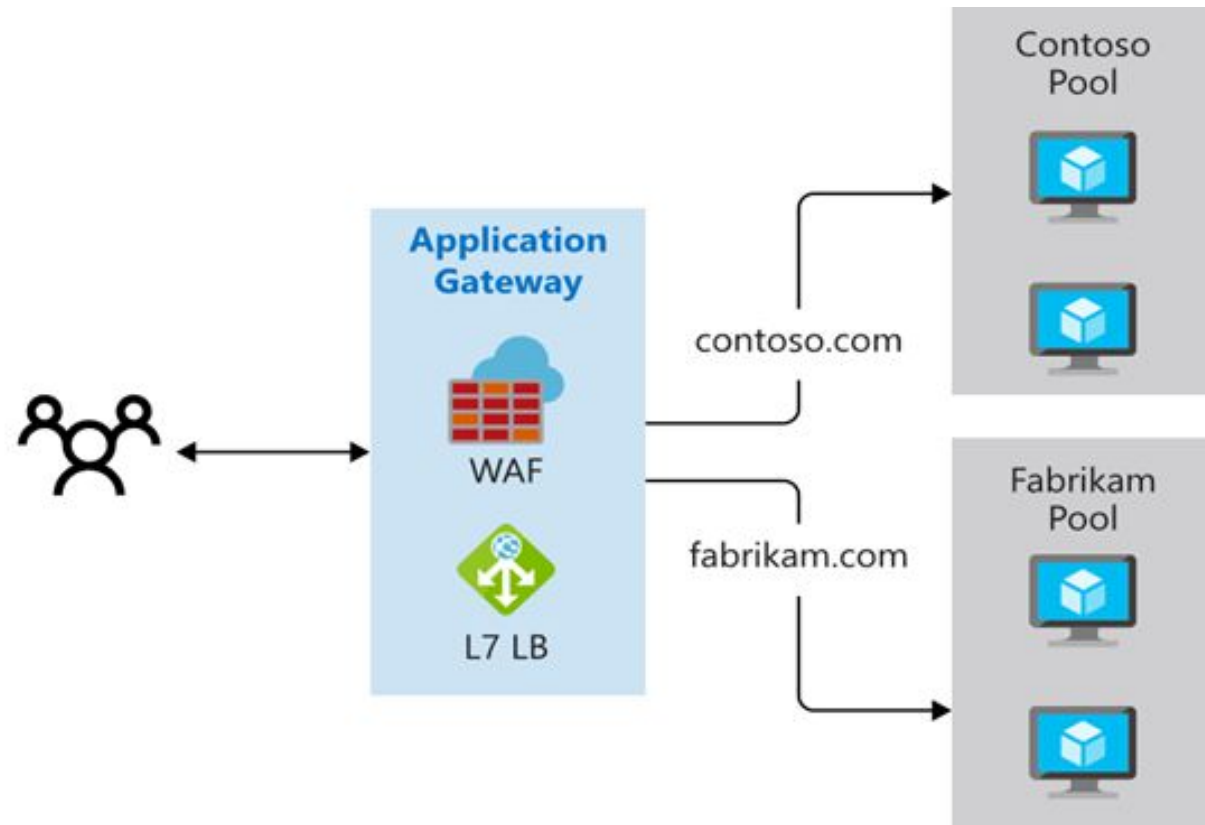
Application Gateway Routing (1 of 3)

Path-based routing



Application Gateway Routing (2 of 3)

Multiple site routing



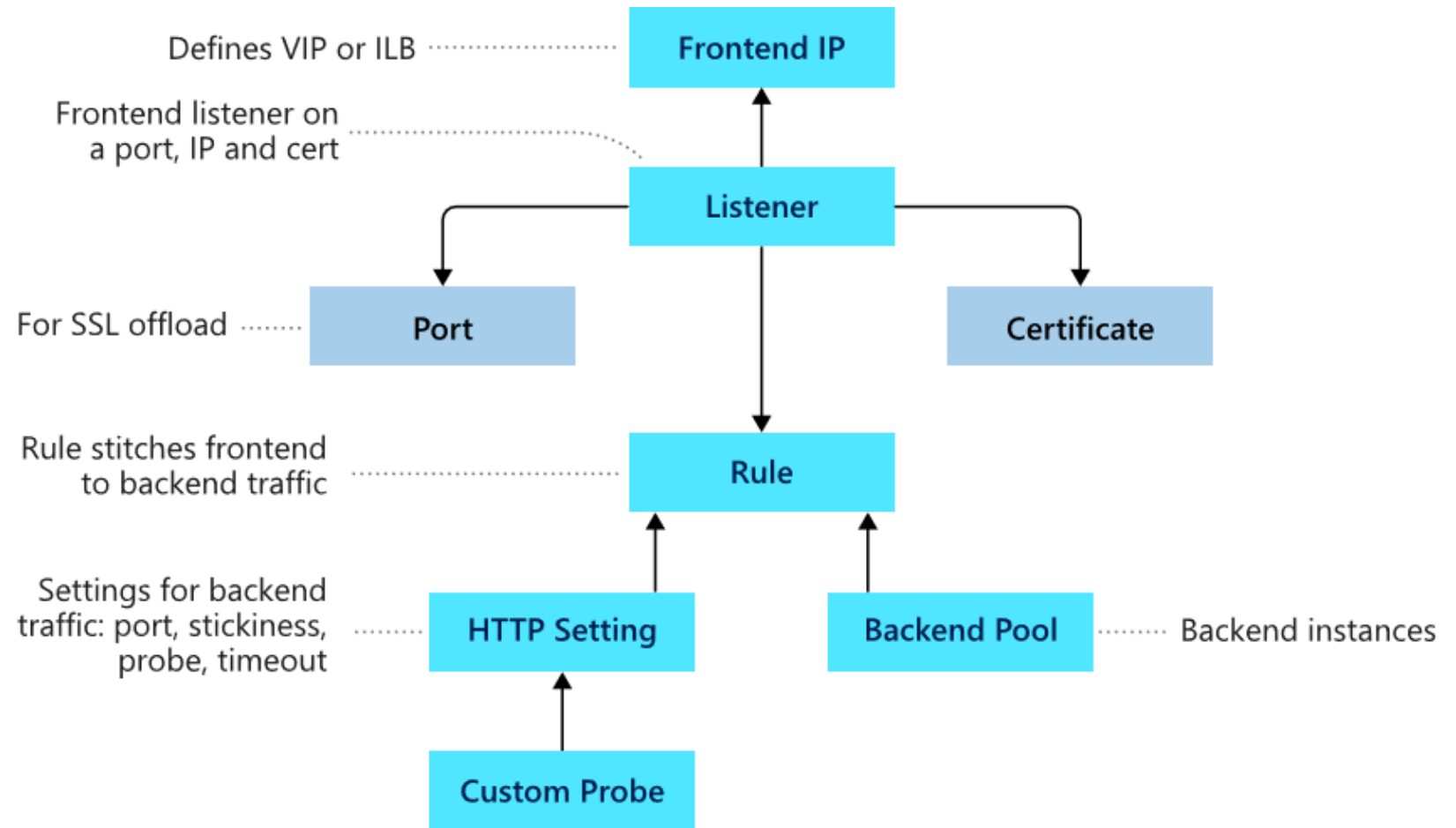
Application Gateway Routing (3 of 3)

Additional features:

- Redirection
- Rewrite HTTP headers
- Custom error pages

Application Gateway Configuration

- Front-end IP address
- Listeners
- Routing rules
- Back-end pools
- Web application firewall
- Health probes

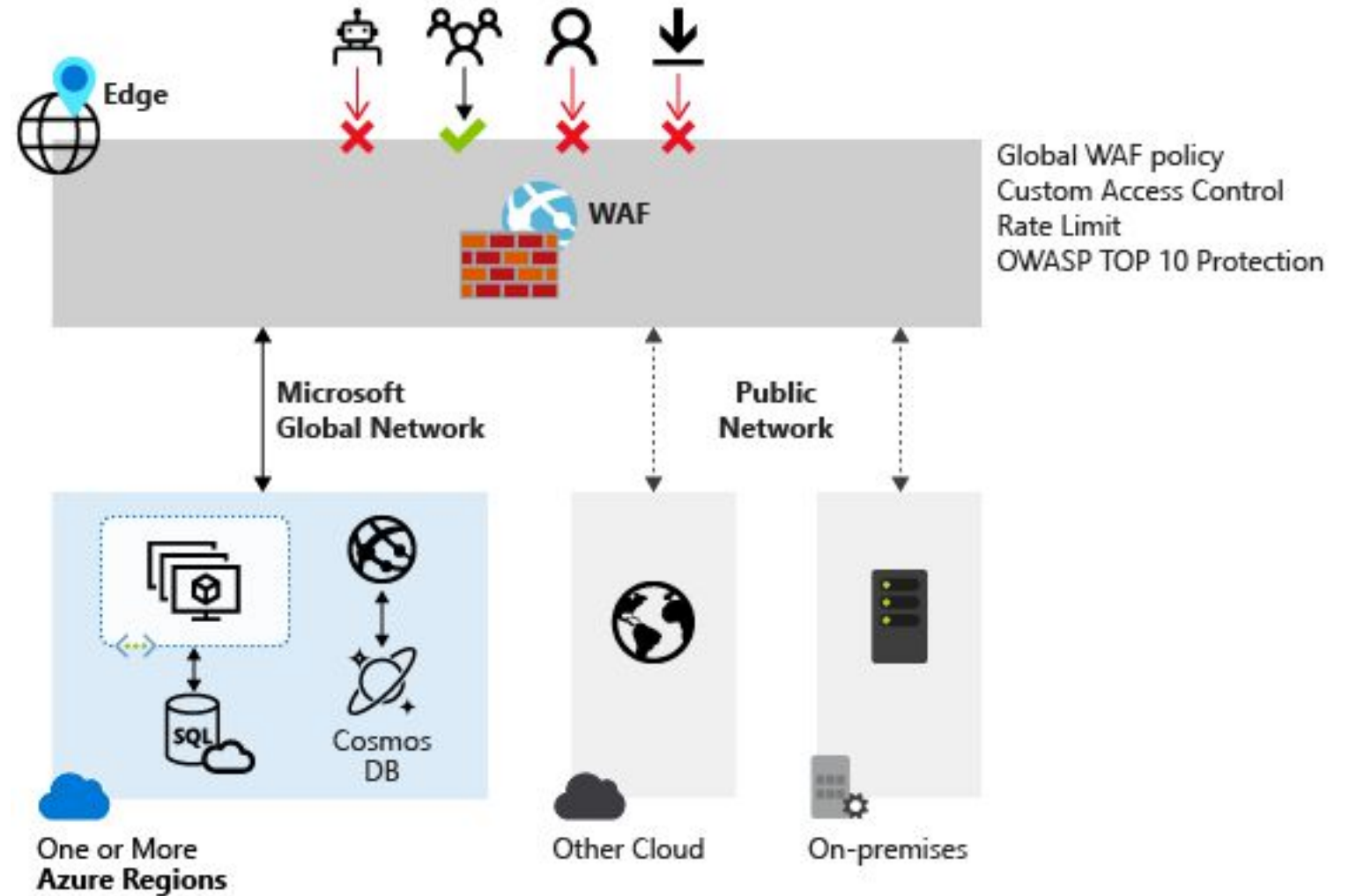


Web Application Firewall



Web Application Firewall Overview (1 of 2)

Web Application Firewall (WAF)



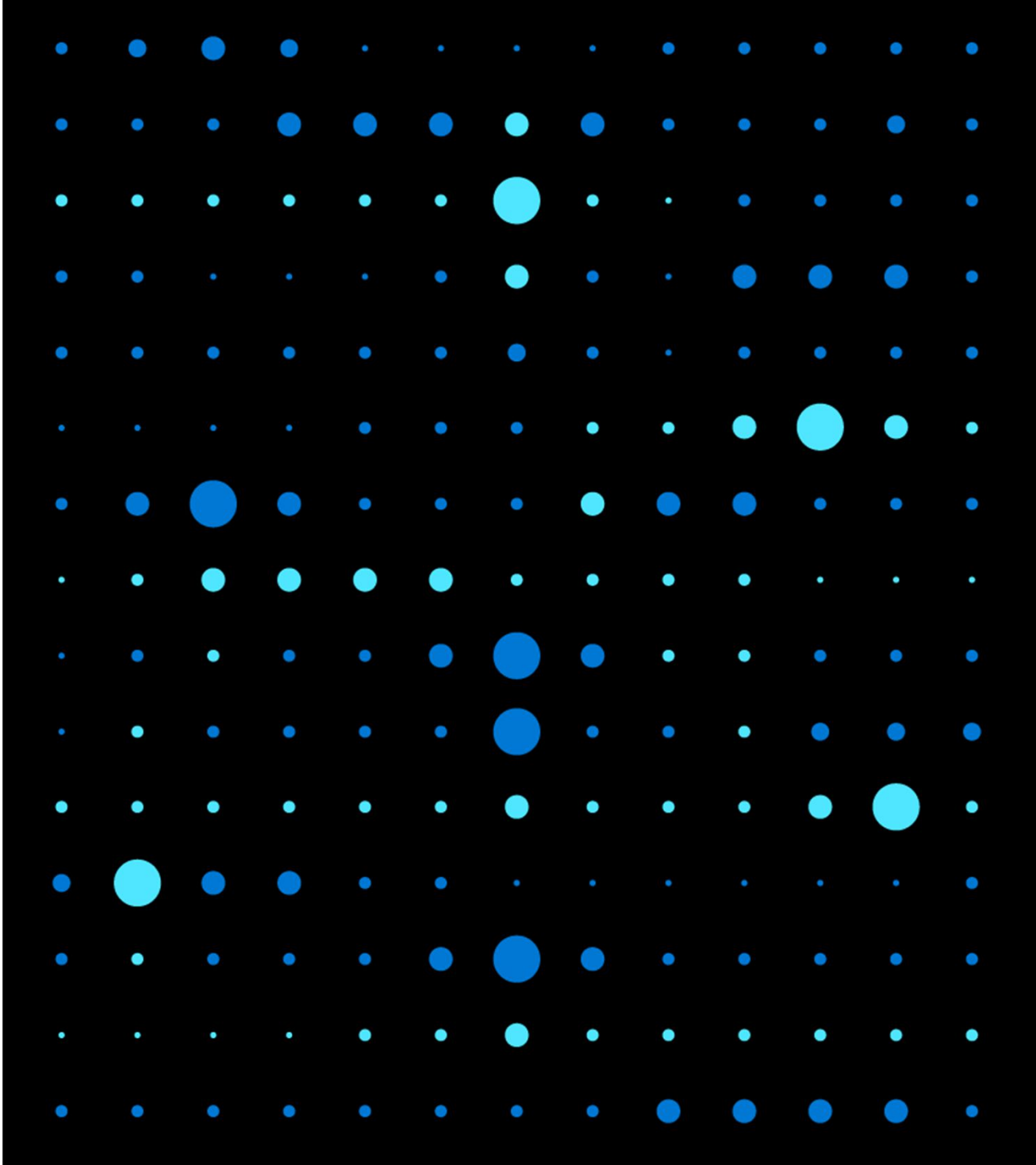
Web Application Firewall Overview (2 of 2)

Supported services:

- Azure Application Gateway
- Azure Front Door
- Azure Content Delivery Network (preview)

Demonstration: Create an application gateway with a web application firewall

- Create an application gateway

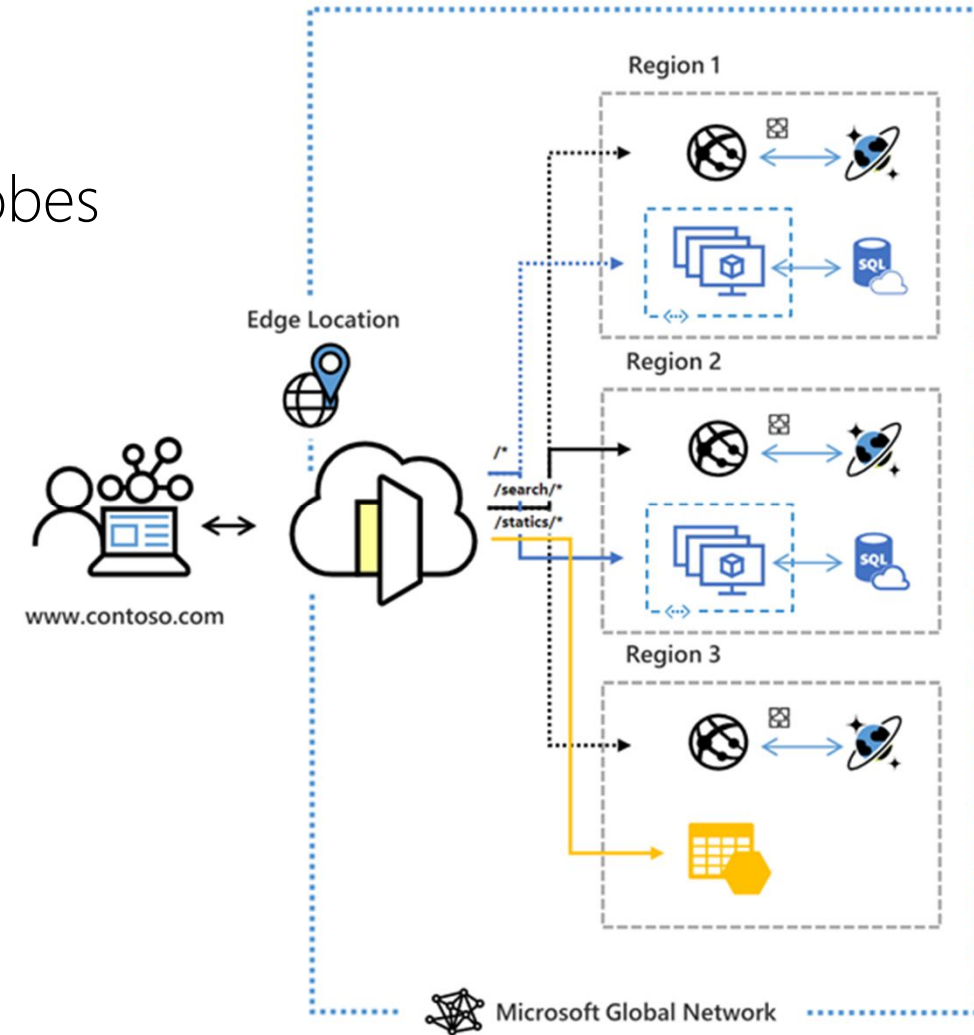


Implement Azure Front Door



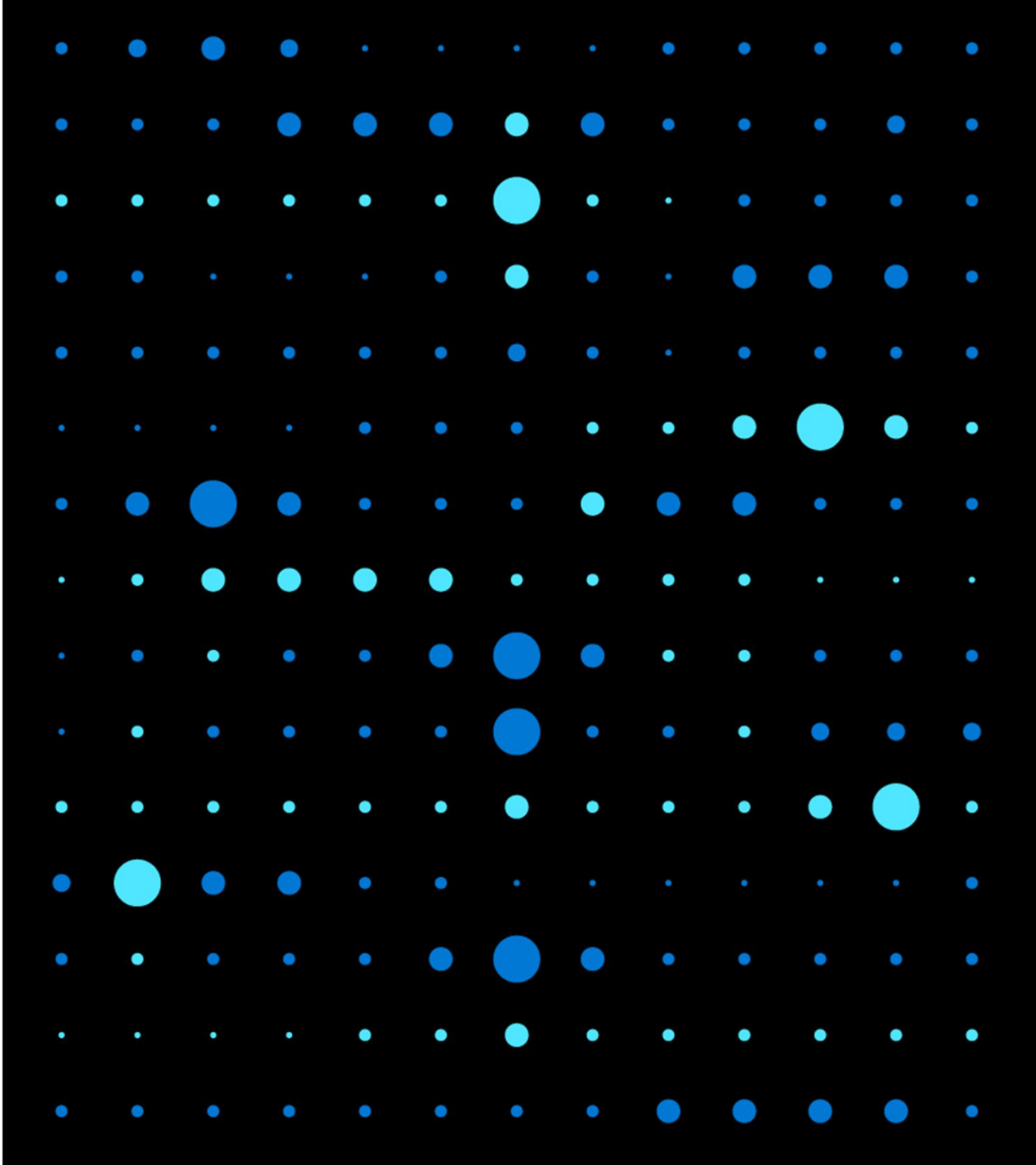
Azure Front Door

- Accelerate application performance
- Increase application availability with smart health probes
- URL-based routing
- Multiple-site hosting
- Session affinity
- TLS termination
- Custom domains and certificate management
- URL redirection
- URL rewrite
- Protocol support – IPv6 and HTTP/2 traffic



Demonstration: Create an Azure Front Door

- Create an Azure Front Door
- View Front Door in action

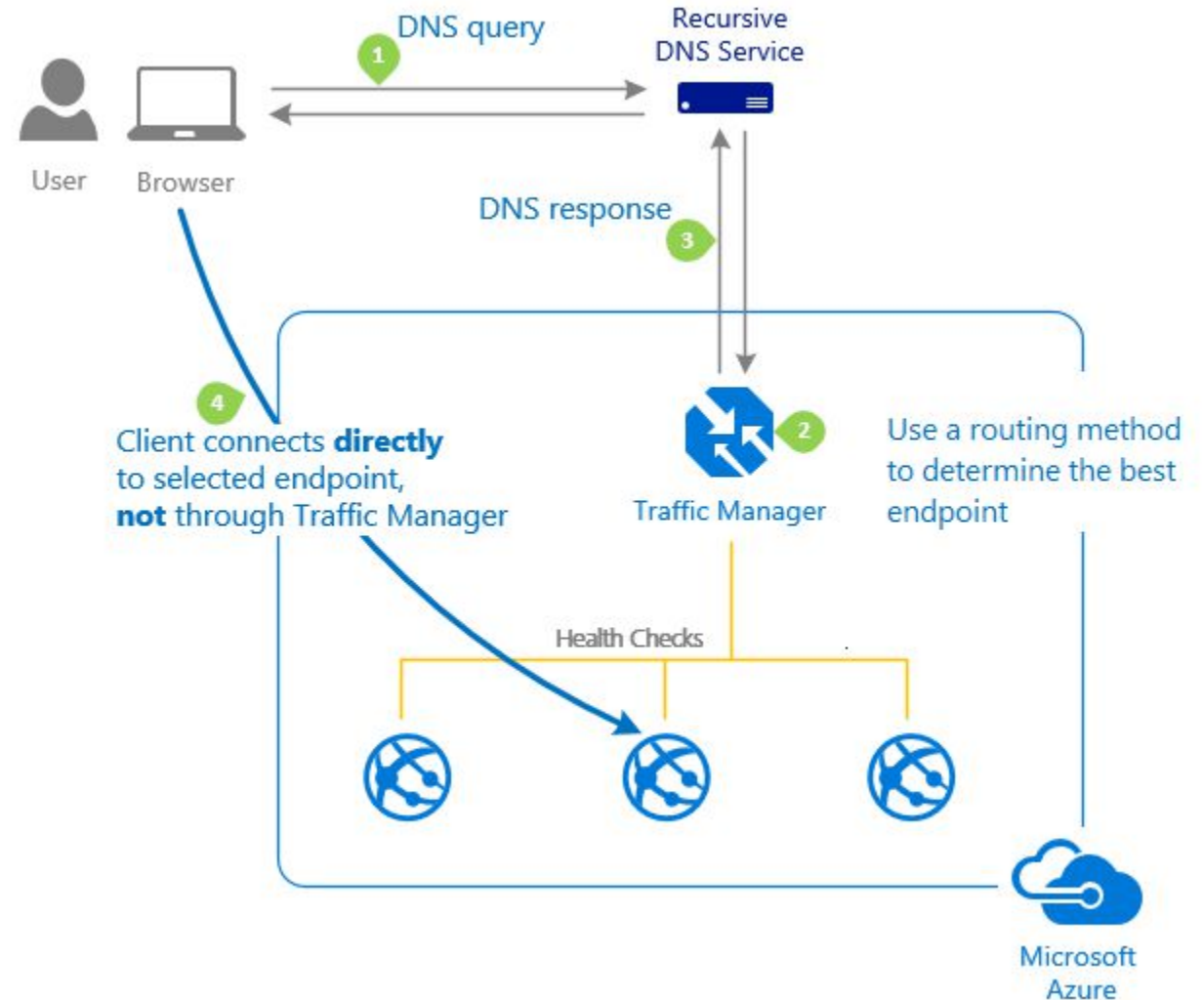


Implementing Azure Traffic Manager



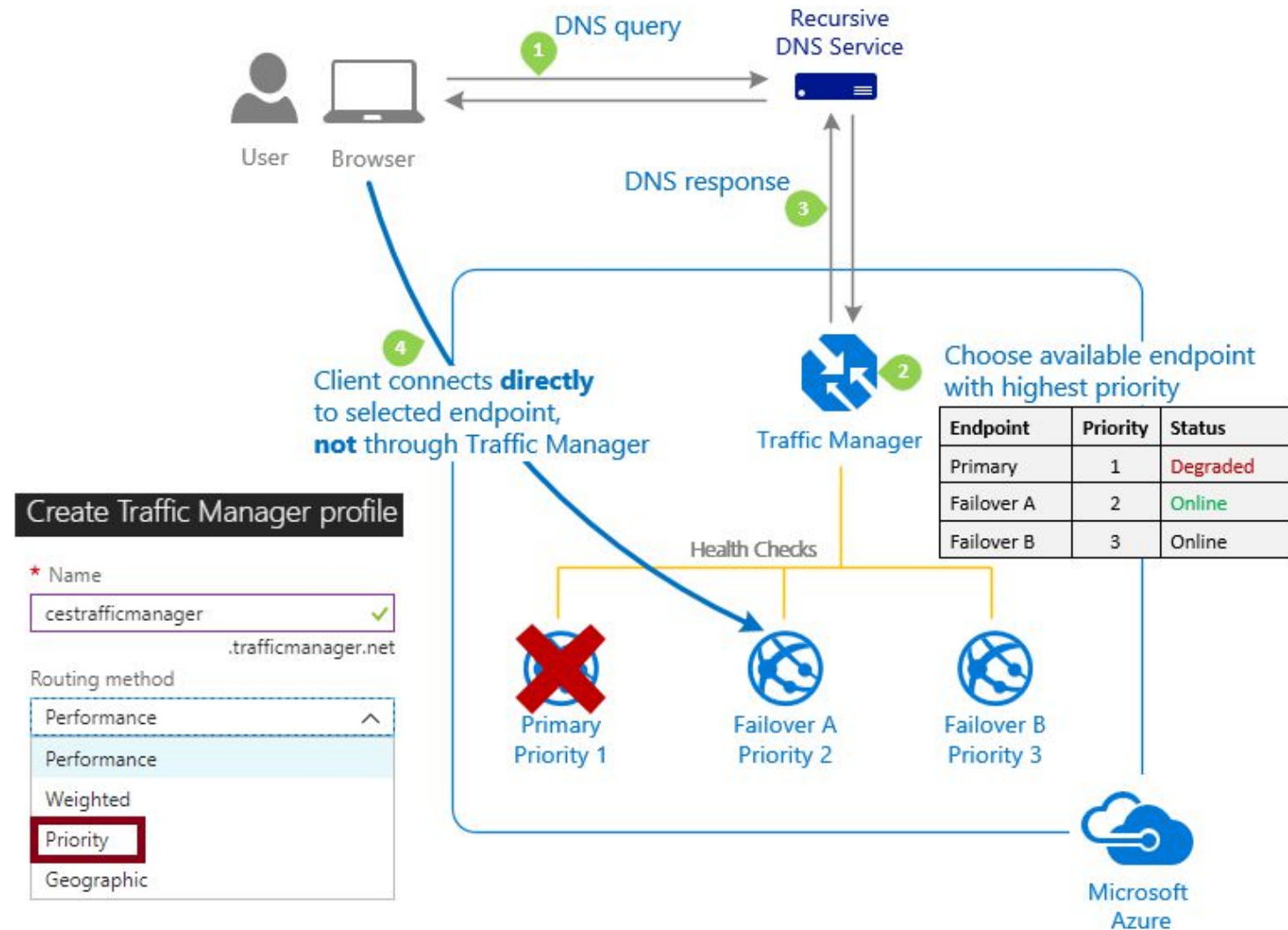
Azure Traffic Manager

- Works by using DNS to direct requests to the most appropriate endpoint
- Selects endpoints based on configured traffic routing method
- Provides endpoint health checks and automatic failover



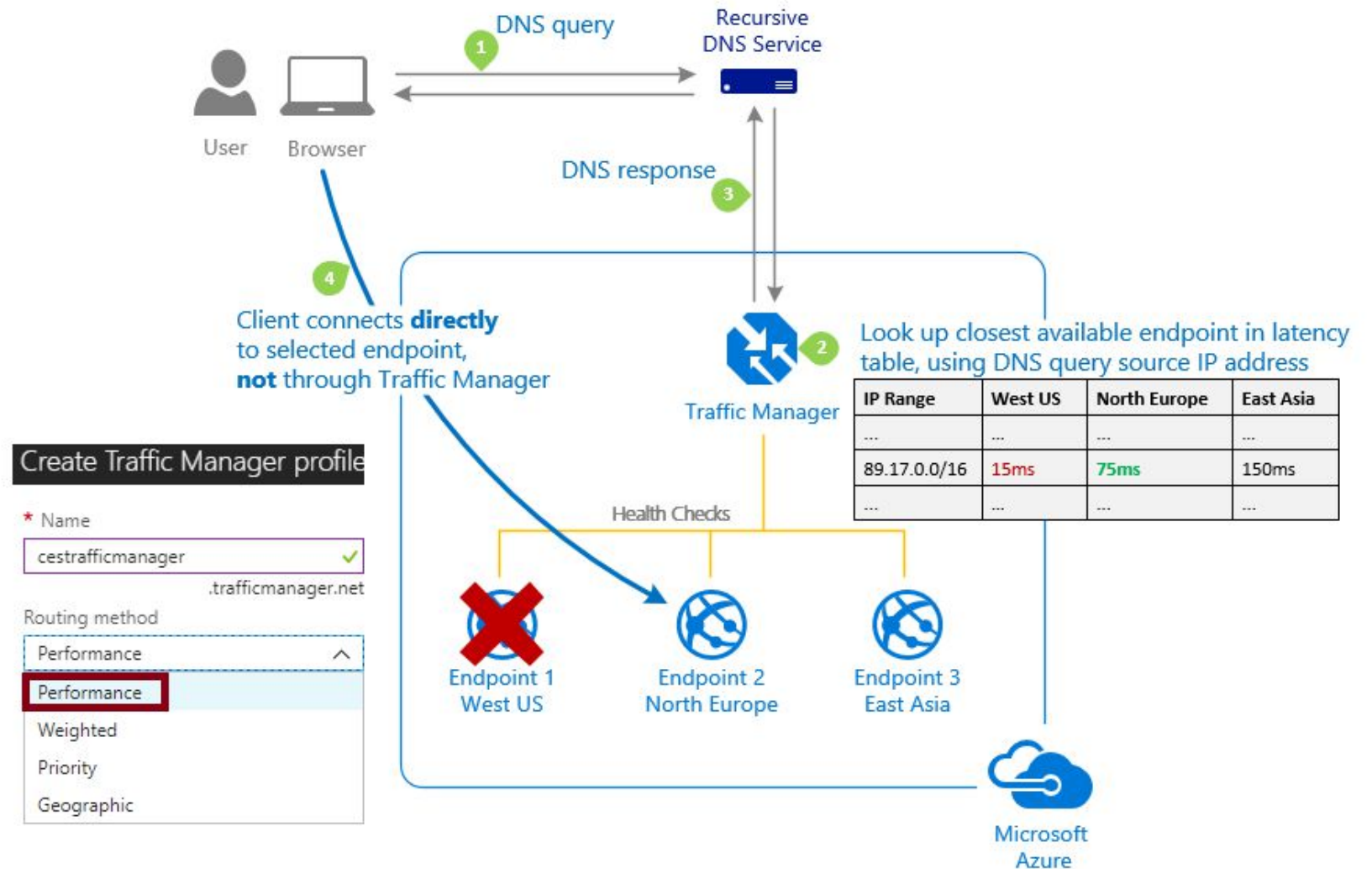
Traffic Manager Routing Methods (1 of 4)

Priority routing



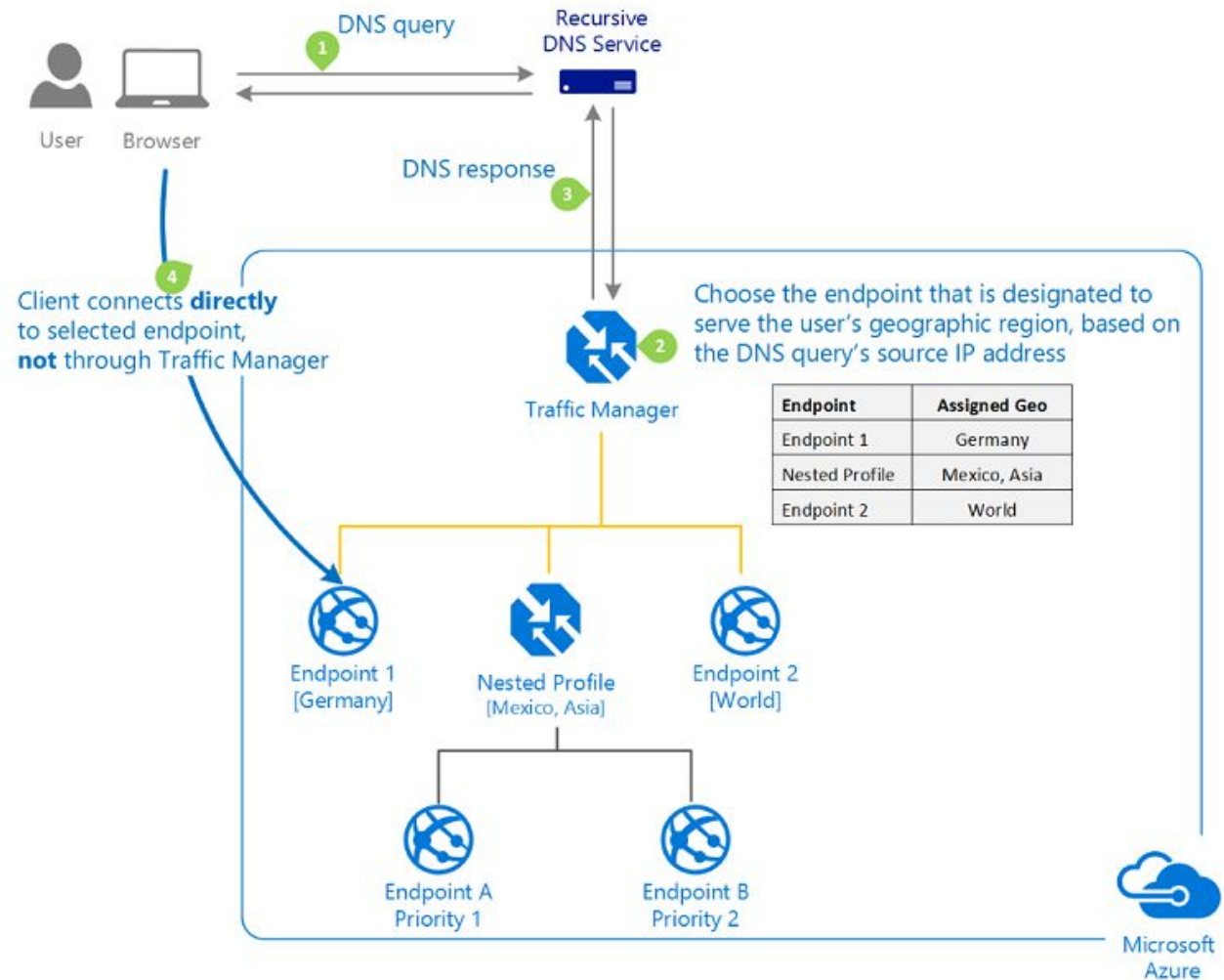
Traffic Manager Routing Methods (2 of 4)

Performance routing



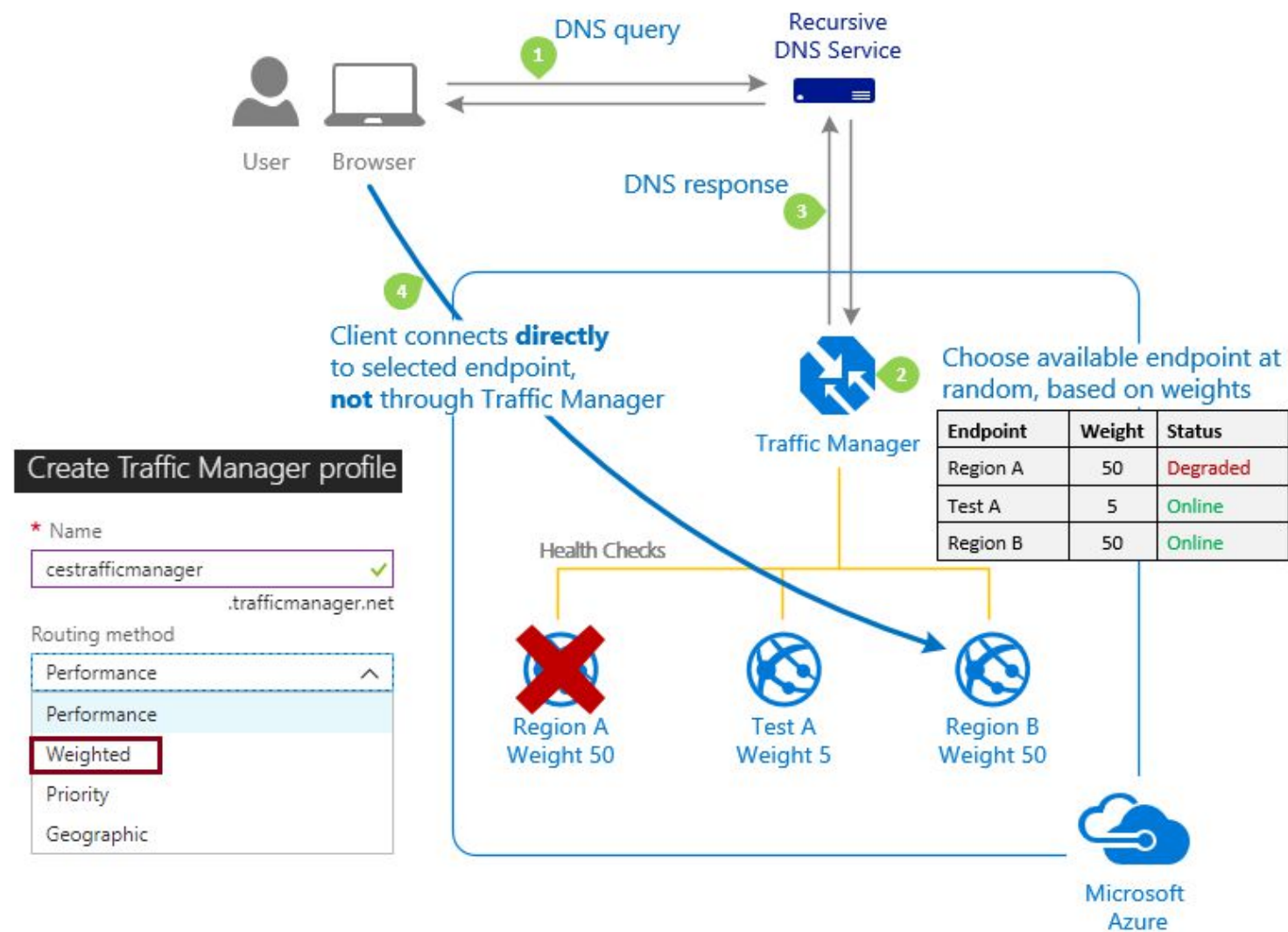
Traffic Manager Routing Methods (3 of 4)

Geographic routing



Traffic Manager Routing Methods (4 of 4)

Weighted routing



Distributing Network Traffic

Compare the Azure Load Balancer with Traffic Manager

Service	Azure Load Balancer	Application Gateway	Traffic Manager	Azure Front Door
Technology	Transport Layer (level 4)	Transport Layer (level 7)	DNS Resolver	Layer 7 or HTTP/HTTPS
Protocols	Any TCP or UDP Protocol	HTTP, HTTPS, HTTP/2, & WebSockets	DNS Resolution	Split TCP-based anycast protocol
Backends and Endpoints	Azure VMs, and Azure VM Scale Sets	Azure VMs, Azure VM Scale Sets, Azure App Services, IP Addresses, and Hostnames	Azure Cloud Services, Azure App Services, Azure App Service Slots, and Public IP Addresses	Internet-facing services hosted inside or outside of Azure
Network connectivity	External and Internal	External and Internal	External	External and Internal

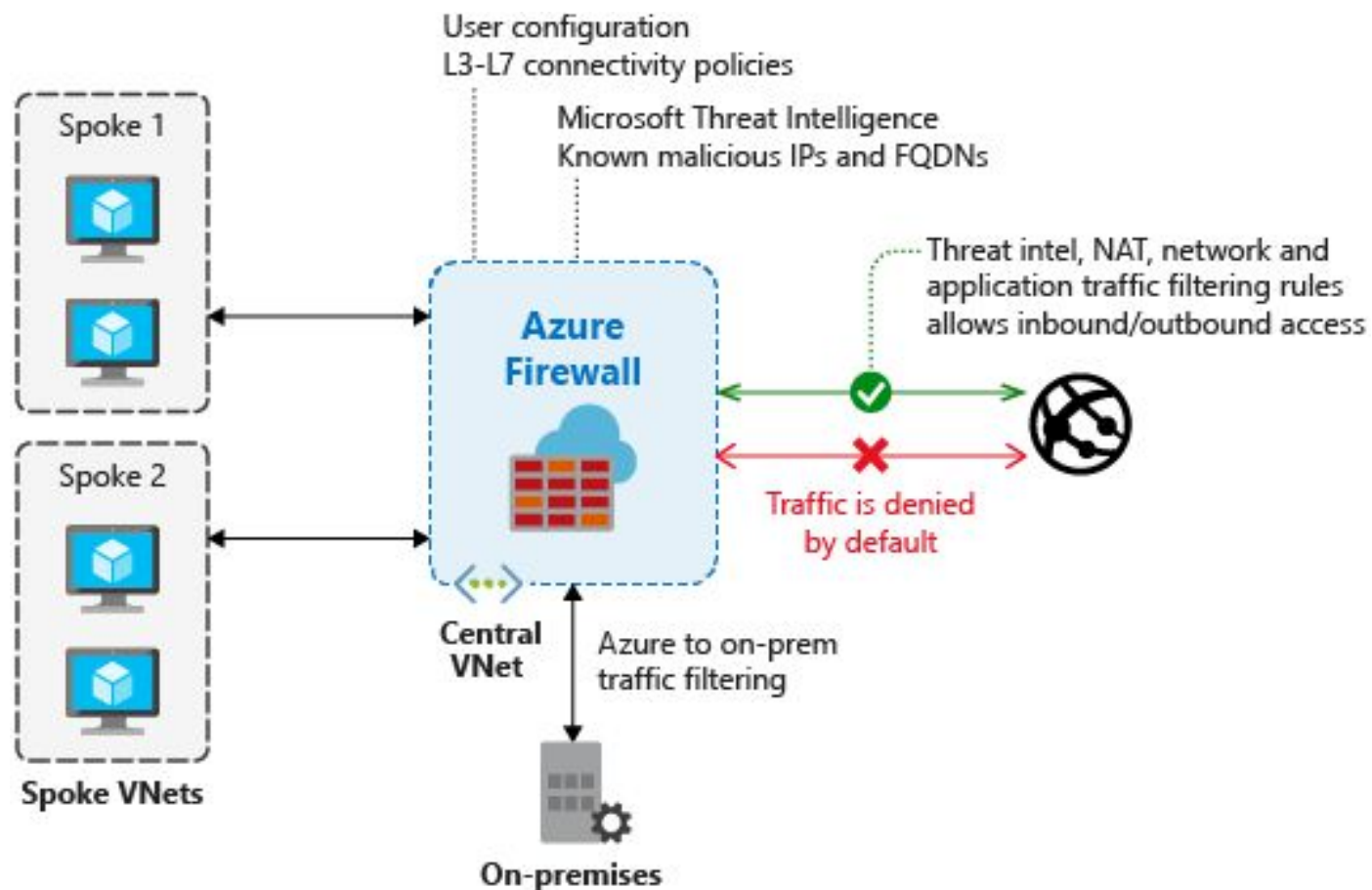
Implement Azure Firewall



Azure Firewall

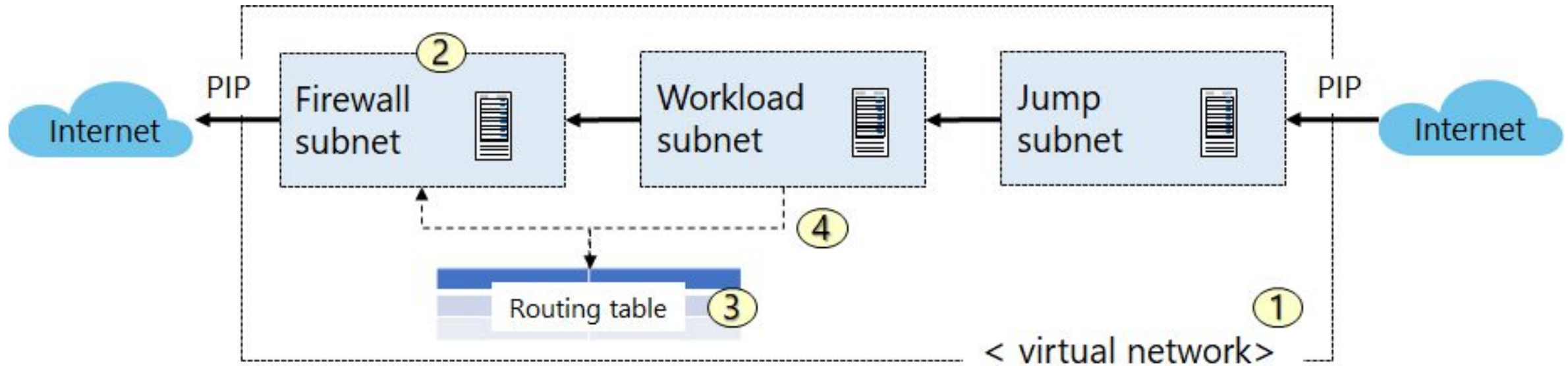
Azure Firewall features:

- Built-in high availability
- Availability zones
- Unrestricted cloud scalability
- Application FQDN filtering rules
- Network traffic filtering rules
- Threat intelligence
- Multiple public IP addresses



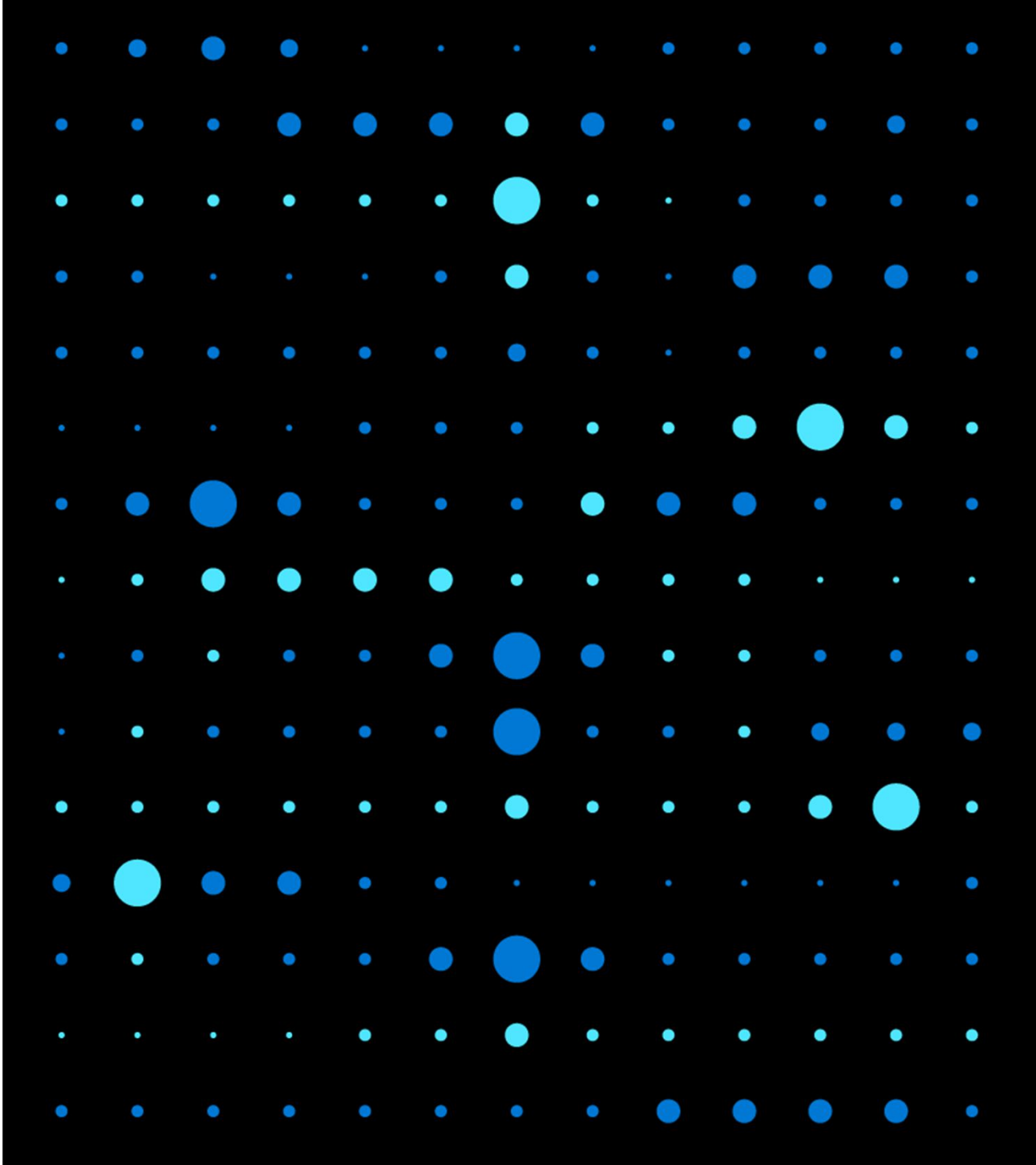
Implementing Azure Firewall

1. Create the network infrastructure
2. Deploy the firewall
3. Create a default route
4. Configure an application rule



Demonstration: Deploy Azure Firewall

- Set up a network
- Create virtual machines
- Deploy the firewall

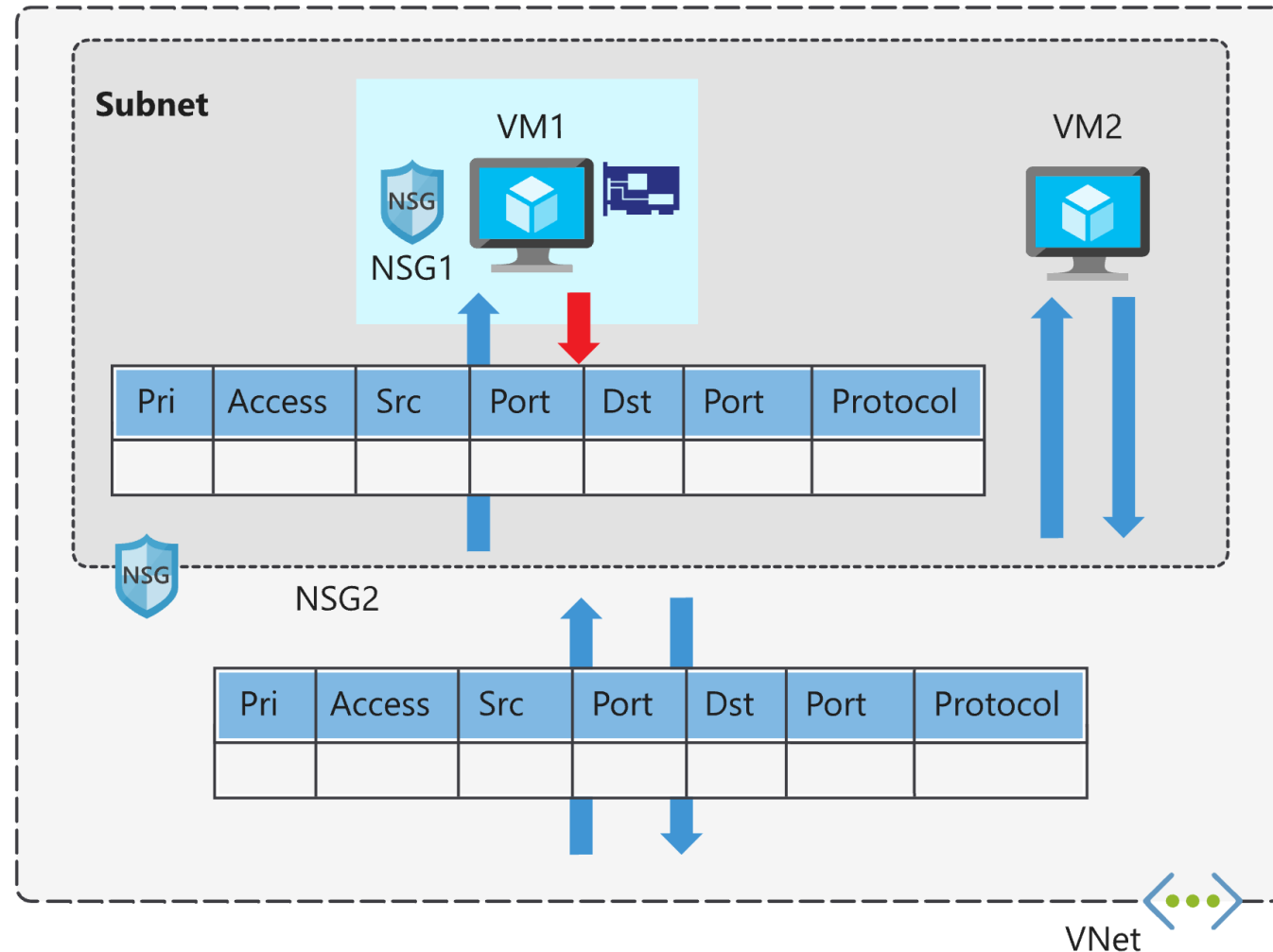


Implement Network Security Groups and Application Security Groups



Network Security Groups (NSGs)

Network security group assignment and evaluation



Security Rules (1 of 2)

Rules properties:

- Name
- Priority
- Source or destination
- Protocol
- Direction
- Port range
- Action

Augmented security rules allow you to add the following options to a rule:

- multiple IP addresses
- multiple ports
- service tags
- application security groups

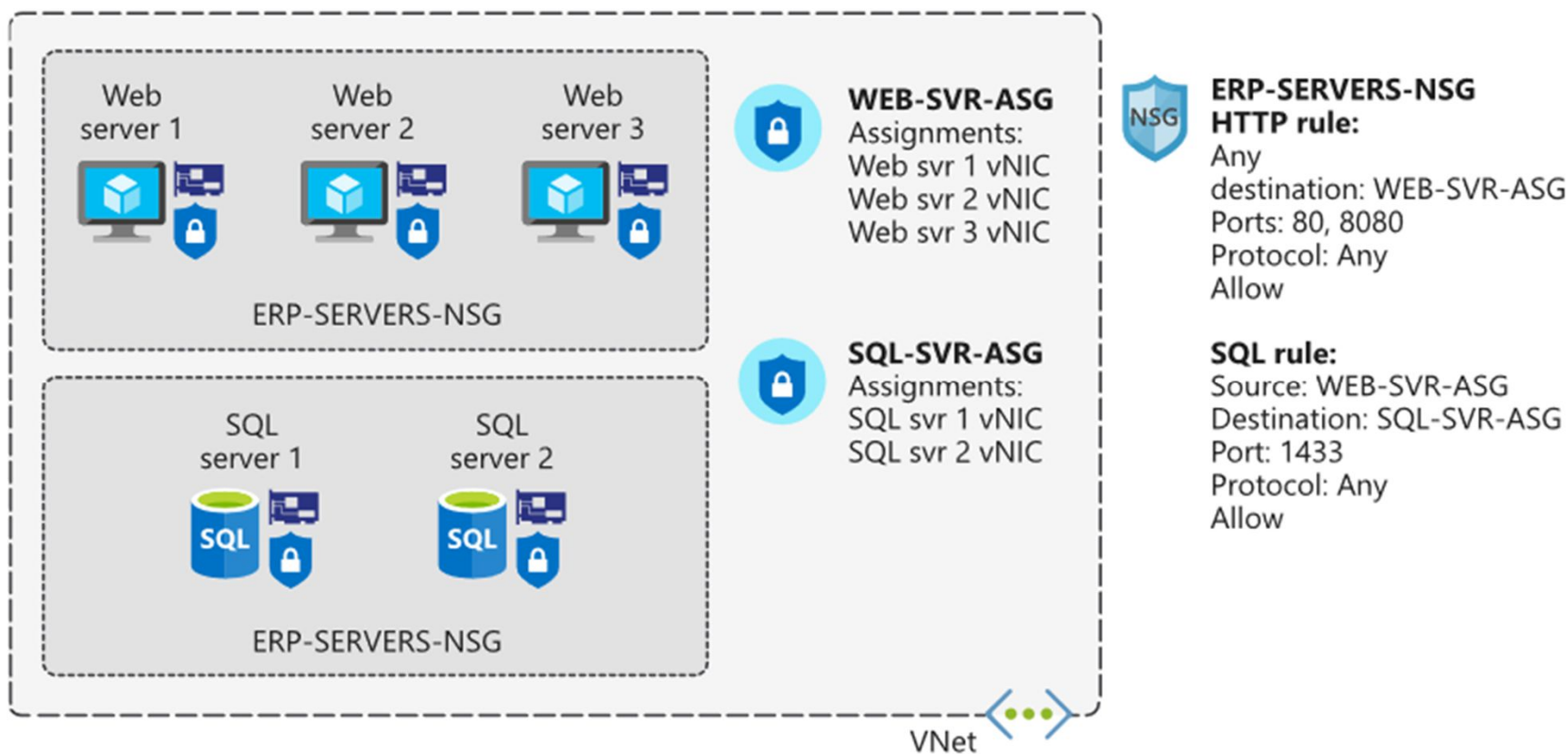
Security Rules (2 of 2)

Service tags simplify defining rules by designating services such as:

- VirtualNetwork
- AzureLoadBalancer
- Internet
- AzureTrafficManager
- Storage
- SQL
- AppService

Application Security Groups

An application security group scopes a rule to a group of custom-defined resources

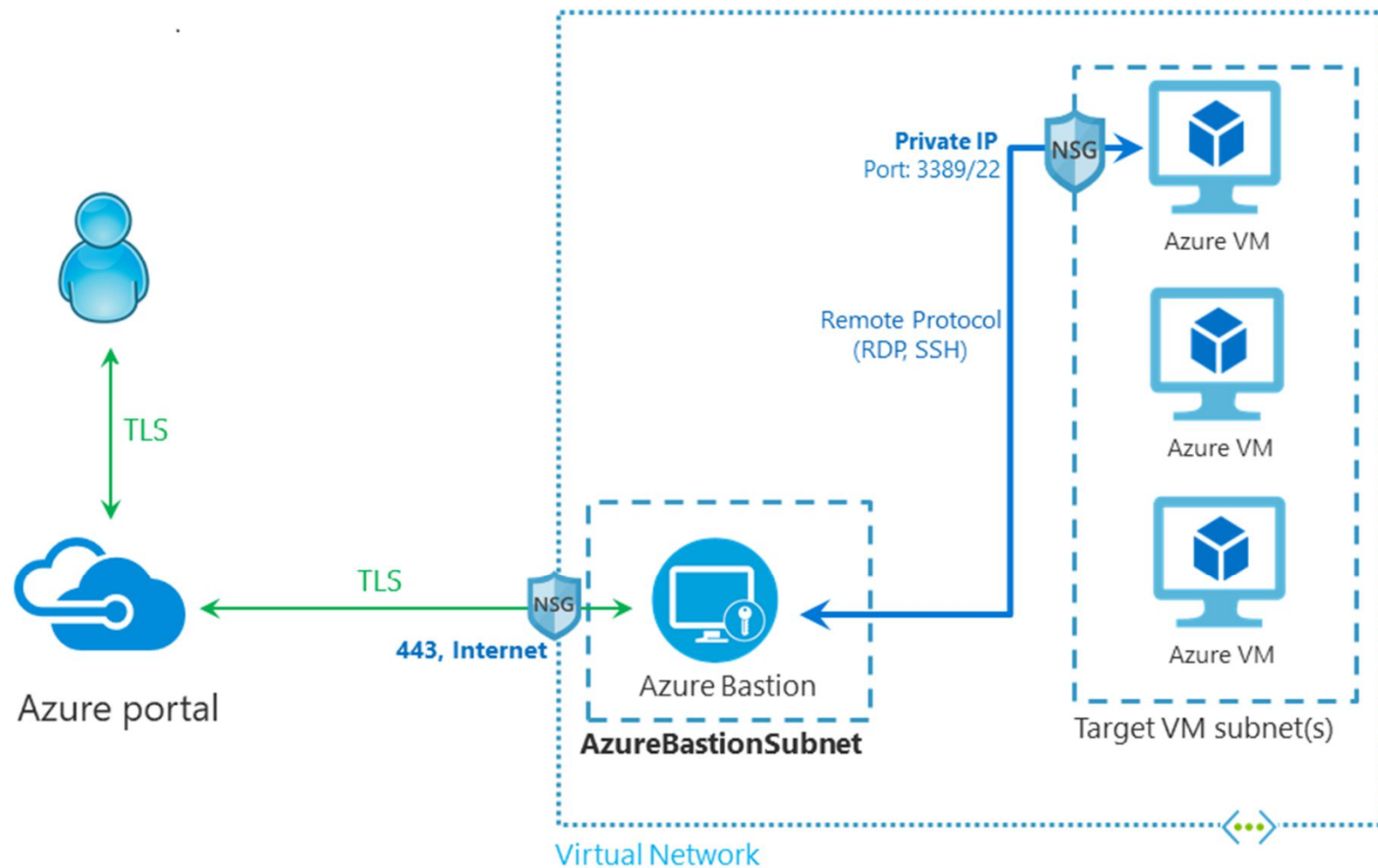


Implement Azure Bastion



Azure Bastion (1 of 2)

Architecture



Azure Bastion (2 of 2)

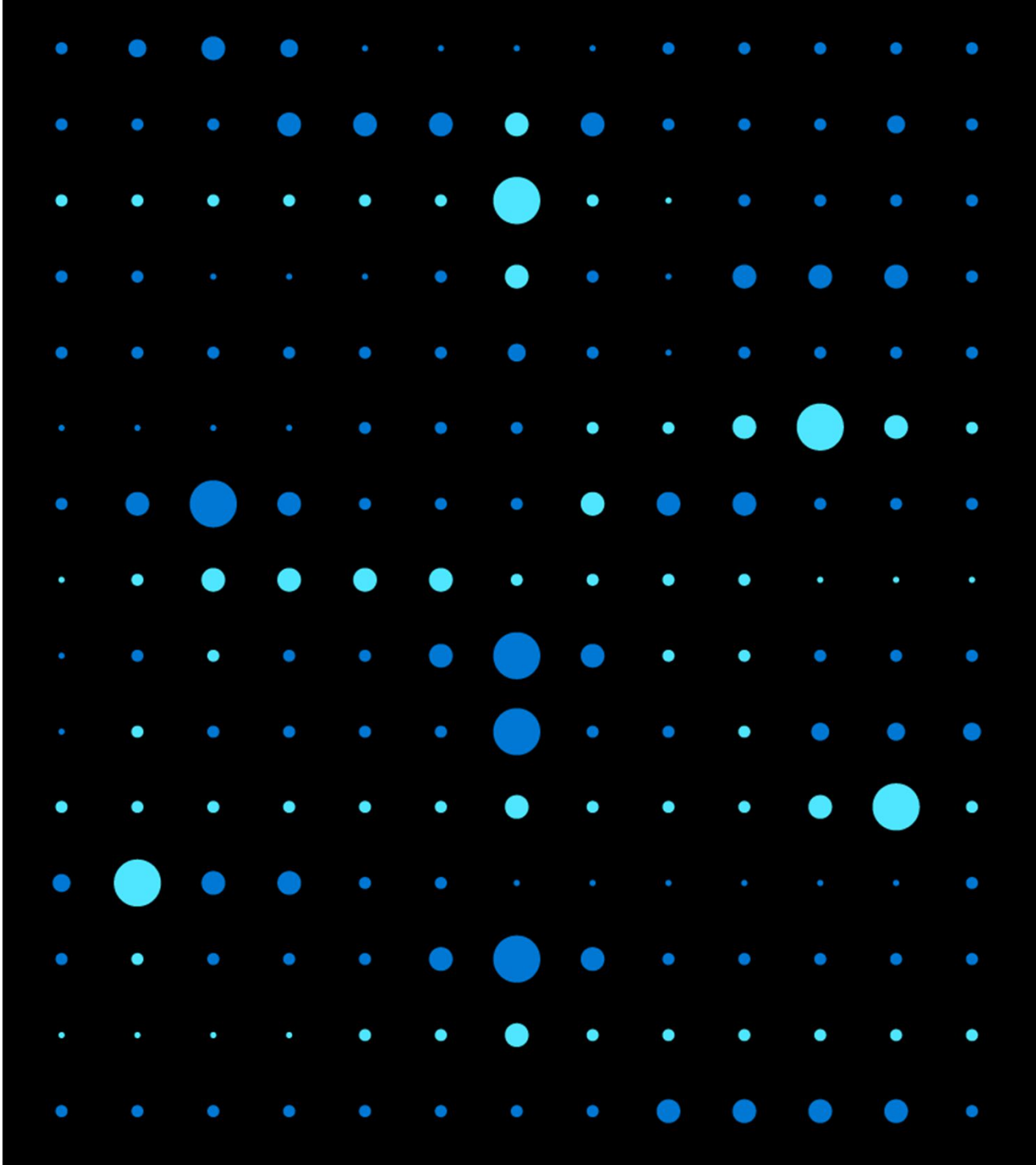
Key features:

- RDP and SSH directly in Azure portal
- Remote session over TLS and firewall traversal for RDP/SSH
- No Public IP required on the Azure VM
- No hassle of managing NSGs
- Protection against port scanning
- Protection against zero-day exploits

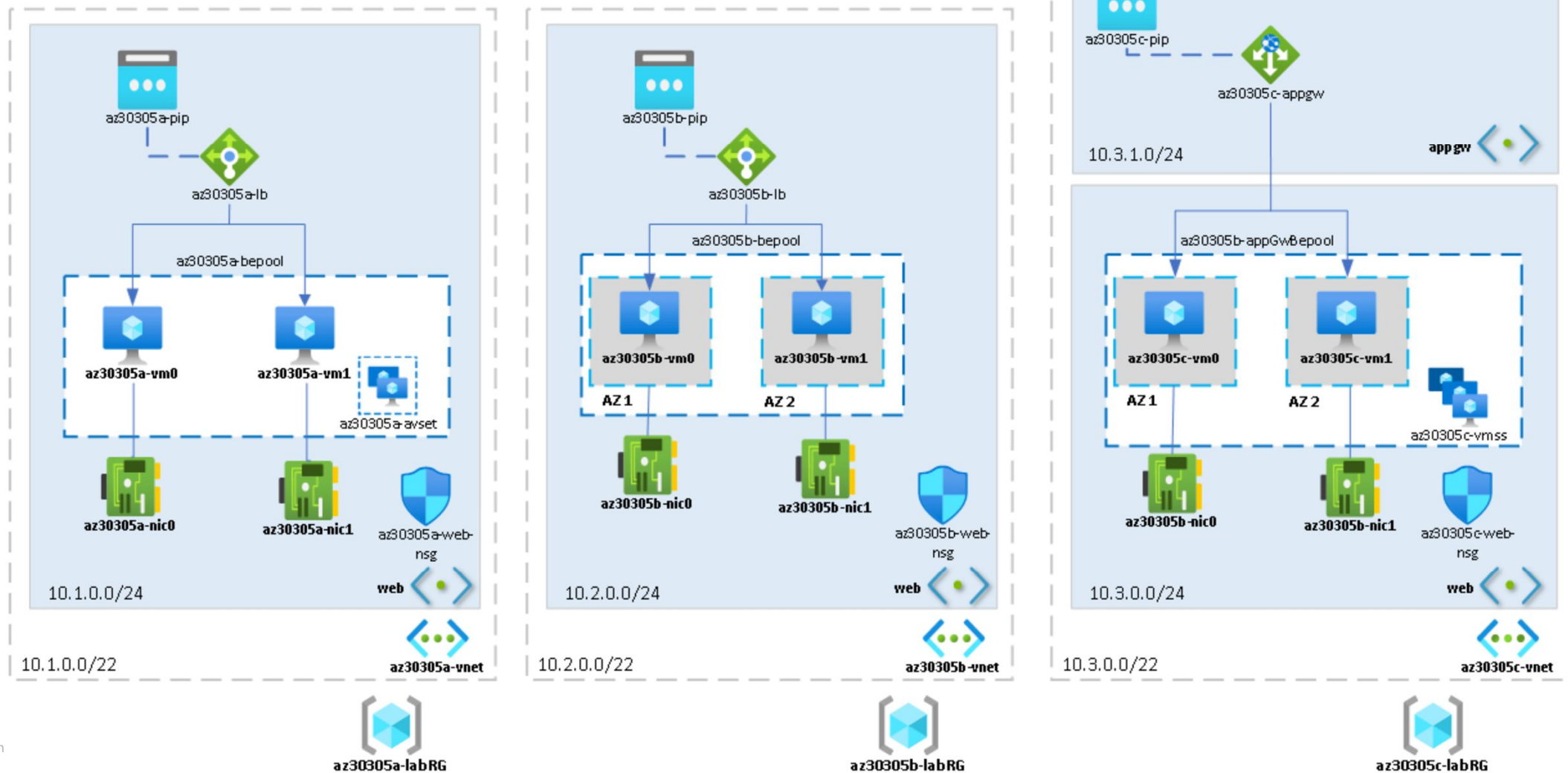


Demonstration: Create an Azure Bastion host

- Create a new Azure Bastion resource from the Azure portal



Lab: Implementing Highly Available Azure IaaS Compute Architecture



Module Review Questions



Online Role-based training resources:

Microsoft Learn

<https://docs.microsoft.com/en-us/learn/>

Thank you.