Microsoft

Mastering Azure networking concepts – ExpressRoute and Azure Firewall

Jon Ormond, Principal PM
Azure Networking

Session learning objectives

Business Problems:

- Contoso has a branch office where Ops Personnel need to connect to their Azure deployments.
- Contoso wants to host a web site in Azure but is concerned about security both in the cloud and on-premises.

At the end of this session, you should be better able to…

- discuss Azure Networking options in general
- describe how virtual networks can be used, including VNet Peering
- describe connectivity options from on-premises to Azure
- know how to implement and configure Azure Firewall
- understand and describe the three rule types associated with Azure Firewall
- understand how to monitor and track events on the Azure Firewall

Azure PowerShell SDK Update

New Azure PowerShell SDK - Az

- New Azure PowerShell SDK Module - Az
  - Not compatible with AzureRM (ie can't be installed side by side)
  - There is an alias set so AzureRM commands will still work
  - It's not required now, but new features are going into Az only

- New Azure Login Method
  - Connect-AzAccount
  - Do this in an admin PowerShell console session to give permanent access for a machine

- AzureRM commands should work with `Enable-AzureRmAlias`

https://azure.microsoft.com/blog/how-to-migrate-from-azurerm-to-az-in-azure-powershell/

Idempotent PowerShell Operations

```
# 3.3 Create Public IPs
Write-Host (Get-Date)' - ' -NoNewline
Write-Host “Creating Public IP address“ -ForegroundColor Cyan
Try {$pip = Get-AzPublicIpAddress -ResourceGroupName $ResourceGroup `
                                  -Name $VMNameASH'-pip' -ErrorAction Stop
     Write-Host "resource exists, skipping“
     }
Catch {$pip = New-AzPublicIpAddress -ResourceGroupName $ResourceGroup `
                                    -Location $EastRegion `
                                    -AllocationMethod Dynamic `
                                    -Name $VMNameASH'-pip’
       }
```

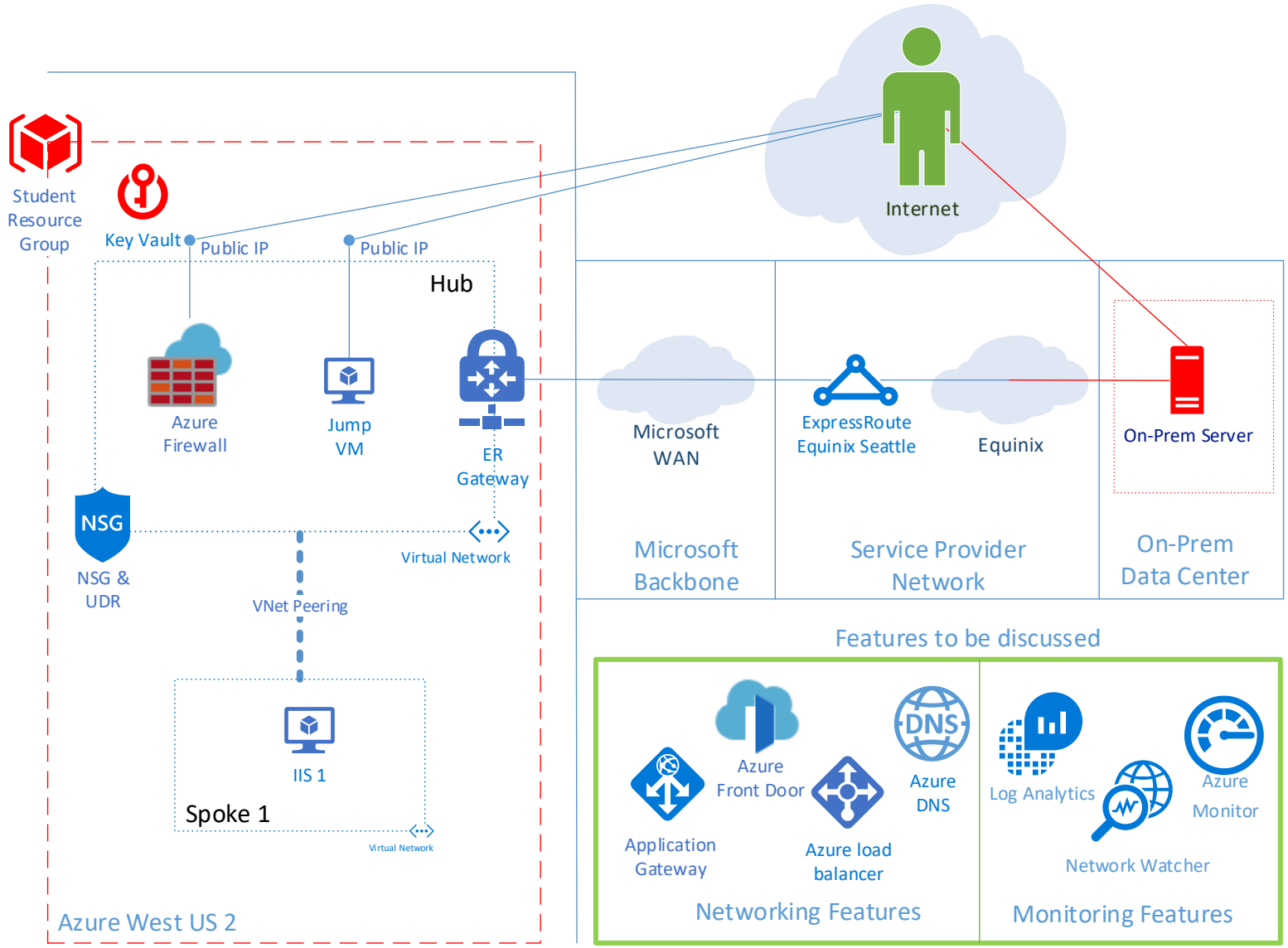
Building the Environment

Final Environment

Red resources have been pre-built for you

Blue resources will be built by you today in the workshop

The green box stuff won't be built but will be discussed



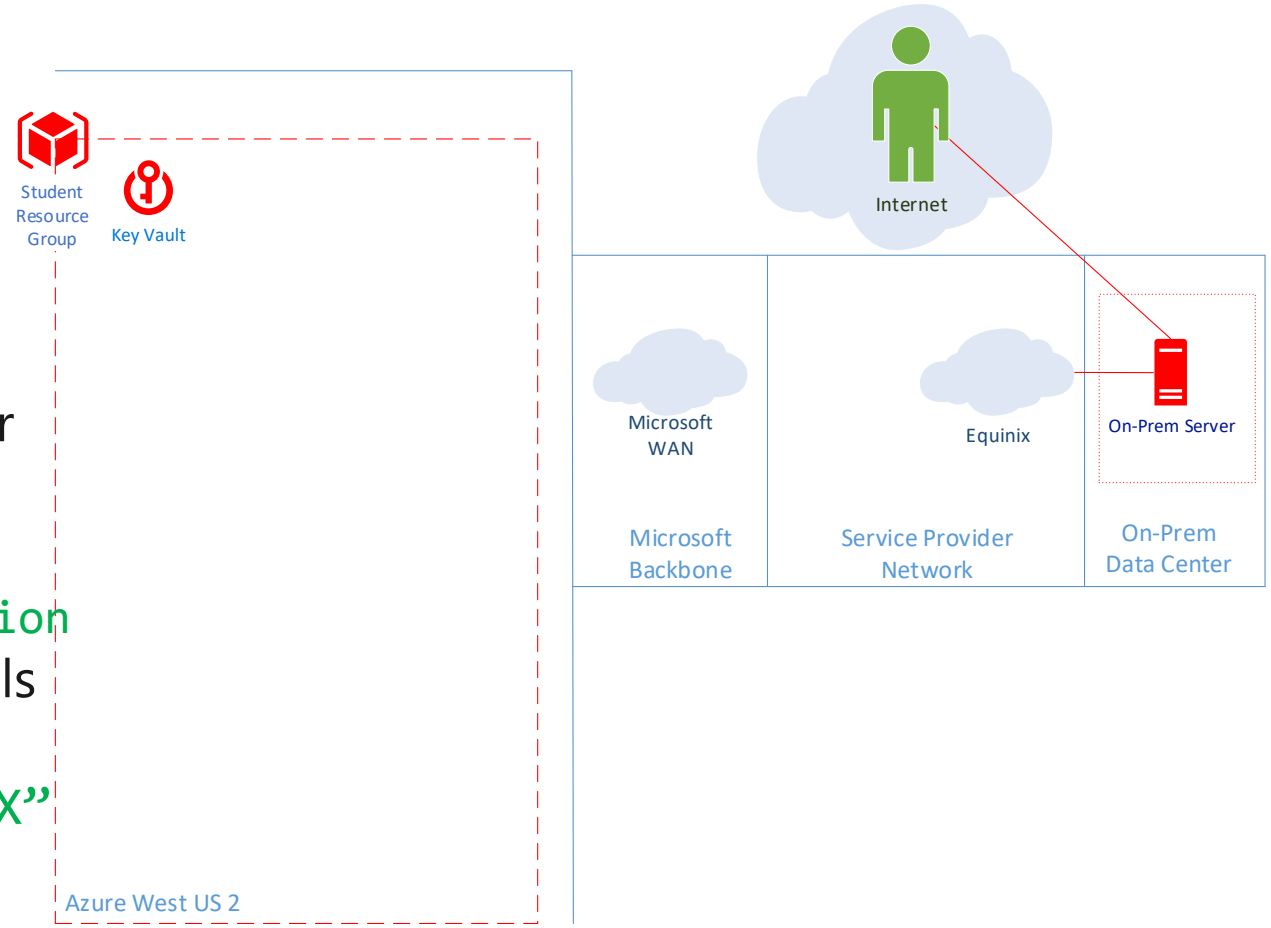
Step 0

Execution:

1. Connect to WiFi
2. Use your company card credentials to login to https://portal.azure.com
3. Get user name and password in KeyVault
4. Using those creds, RDP to the on-prem server *sea.pathlab.xyz:200xx (xx=Company Number)*
5. On server, open PowerShell run
   `Connect-AzAccount -UseDeviceAuthentication`
   and login using your company card credentials
6. Run
   `Get-AzResourceGroup –Name “CompanyXX”`
   to validate PowerShell and your access

(You may need to Set-AzContext to "Virtual Data Center Workshop“)

NOTE: The on-prem server should be where all PowerShell and any validation should be performed.



Virtual Networks

Your virtual private network in the cloud

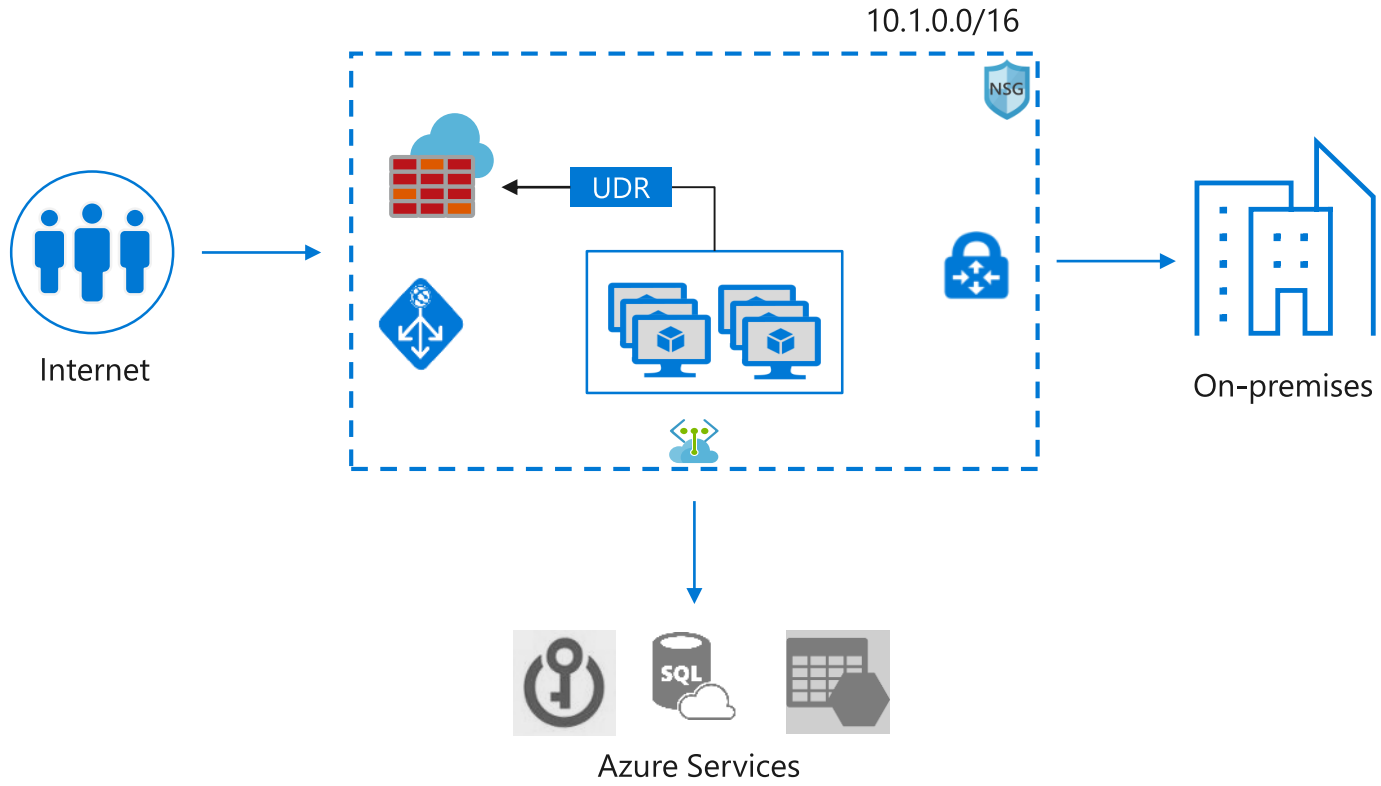
Private isolated logical network

Supports Network ACLs and IP Management

User defined routing for network virtual appliances

Extends on-premises network to the cloud

Provides secure connectivity to Azure services



"User Defined Routing (UDR) allows customers to easily secure their lift-n-shift and cloud-native applications in Azure using next-generation firewalls like VM-Series.
This includes micro-segmentation in an Azure VNET and securing Azure applications at scale with VM-Series instances behind the Azure Standard Load Balancer."

Jigar Shah
Product Line Manager, Palo Alto Networks

Extending VNets to Containers

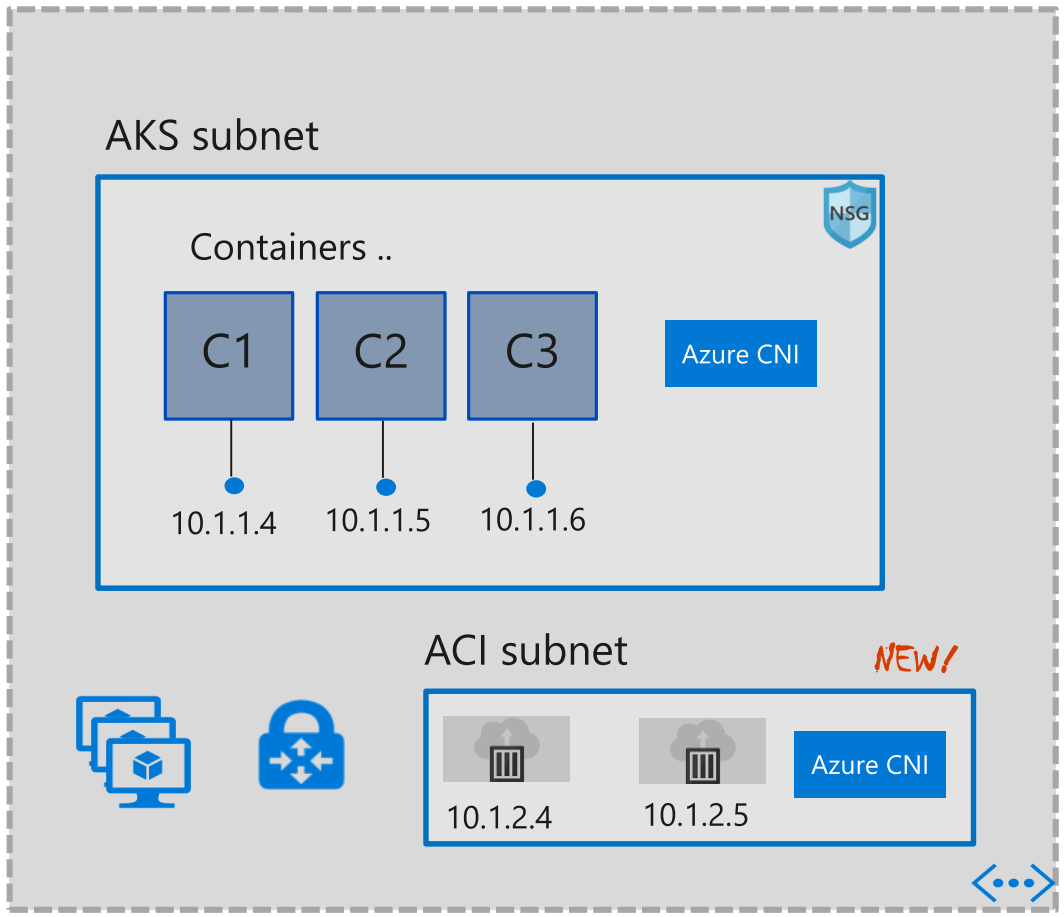
Containers are first class citizens

Deploy containers into your VNet using Azure CNI plugin

All VNet and security policies apply to containers (like VMs)

Azure Kubernetes Service (AKS)

Azure Container Instances (ACI) can now be deployed into your VNet (Preview)



AccuWeather

*"AccuWeather's decision to utilize **Azure CNI** was around the **ease of connecting our AKS Clusters in various regions** using **VNet peering**. This also provided the option to use **ExpressRoute** to facilitate **local network connection**"*

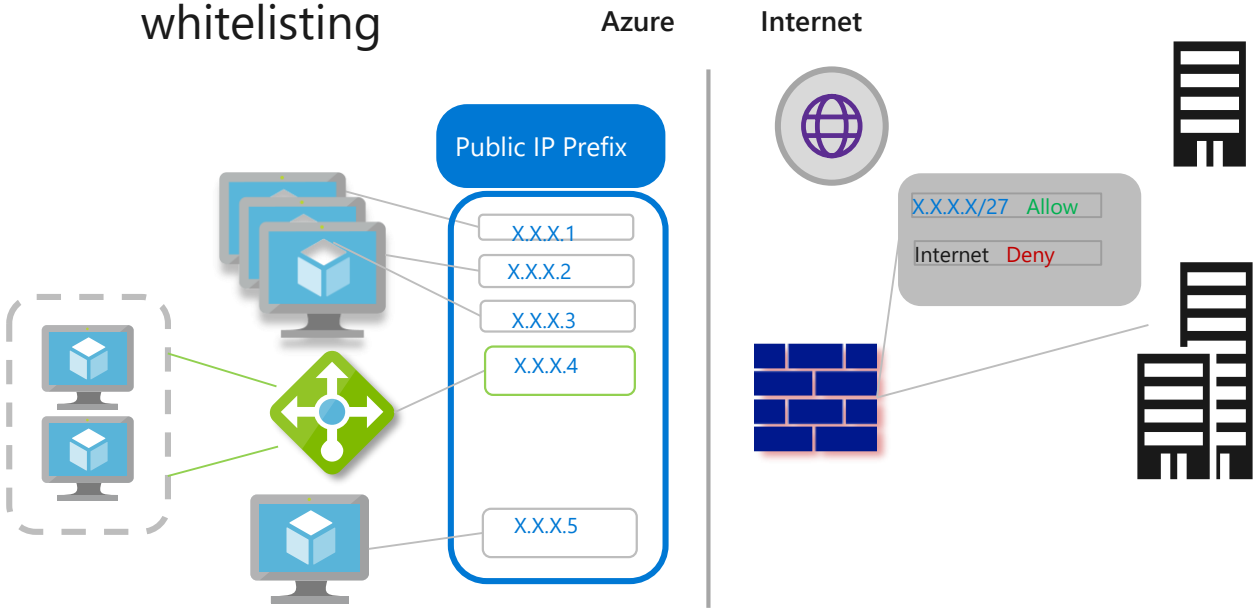
Doug Honikel
Vice President, Software Development

Virtual Network
What's new

Public IP Prefix

A reserved IP range for your public endpoints in Azure

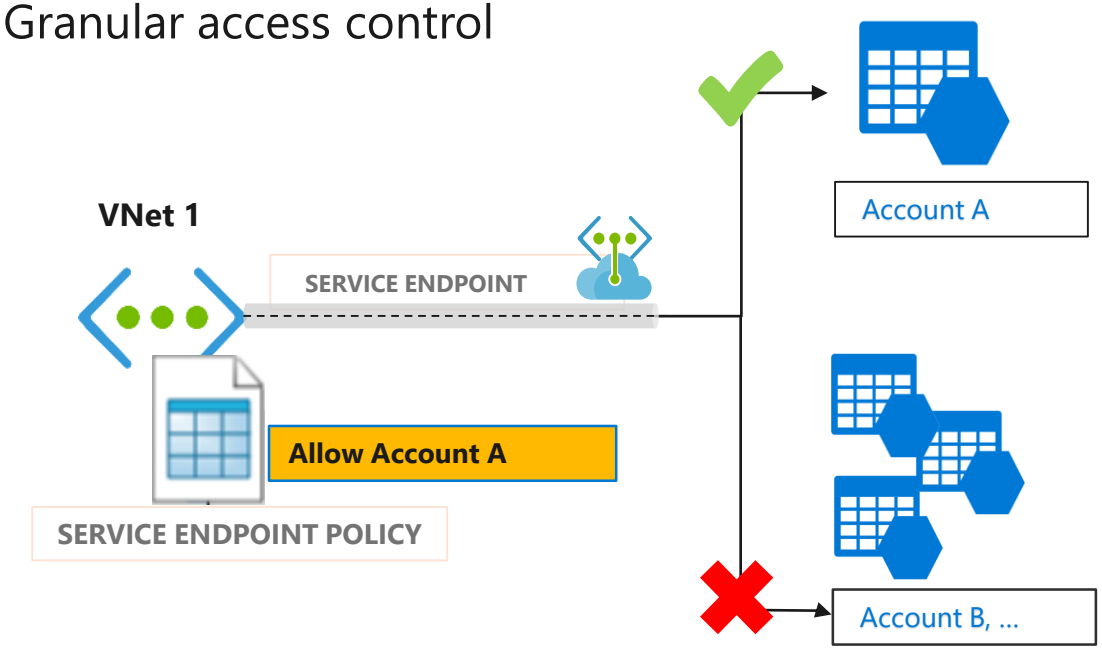
- Simplify IP address management
- Predictable, contiguous public IP addresses
- One CIDR block to give your customers for whitelisting



Service Endpoint Policies

Enhanced VNet security for Azure services

- Prevent access of unauthorized Storage accounts from VNet
- Restrict Vnet access to specific Storage Accounts
- Granular access control



Azure DDoS Protection

Cloud scale DDoS protection tuned to applications

GA

Simple to provision for all your virtual network resources

Always on monitoring with near real time telemetry and alerting

Automatic network layer attack mitigation

Protection policies tuned to your application's traffic profile

What's new

DDoS Attack Analytics

Near real time network attack mitigation flow logs

Attack data snapshots and full post attack summary

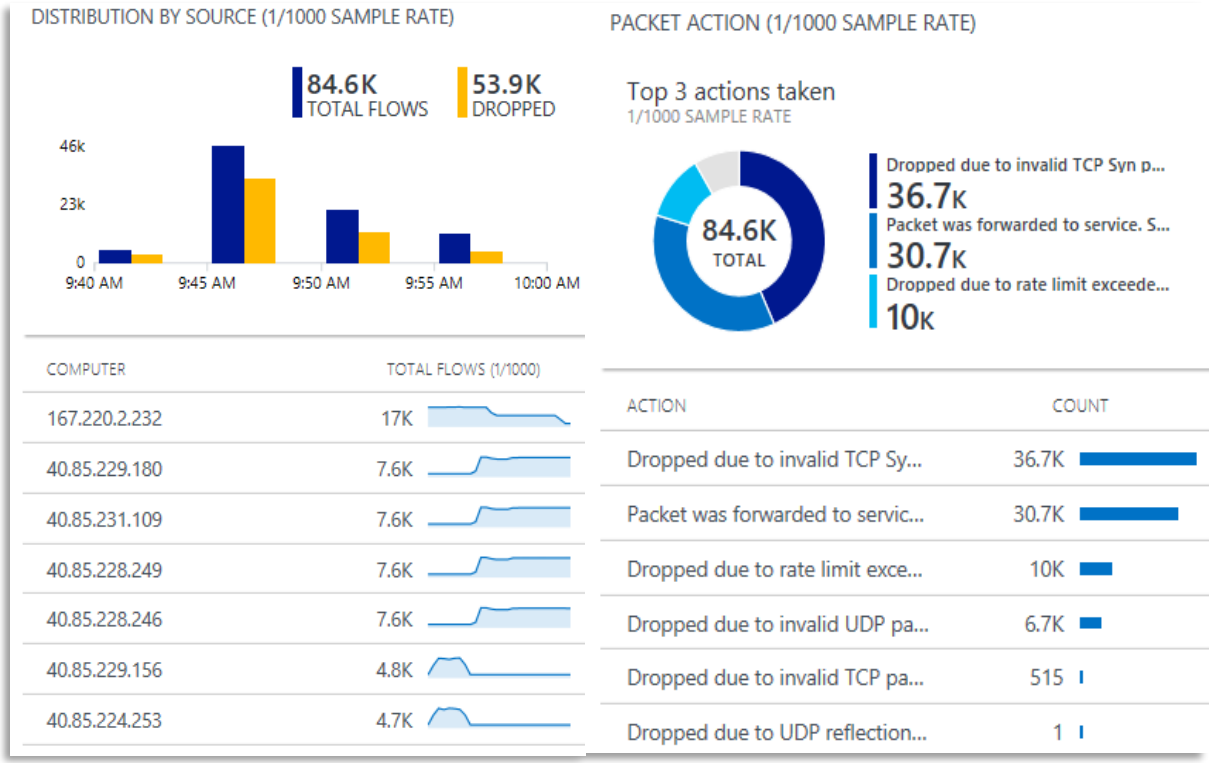
DDoS Rapid Response

Specialized Rapid Response team support during active attacks

Custom mitigation policy configuration

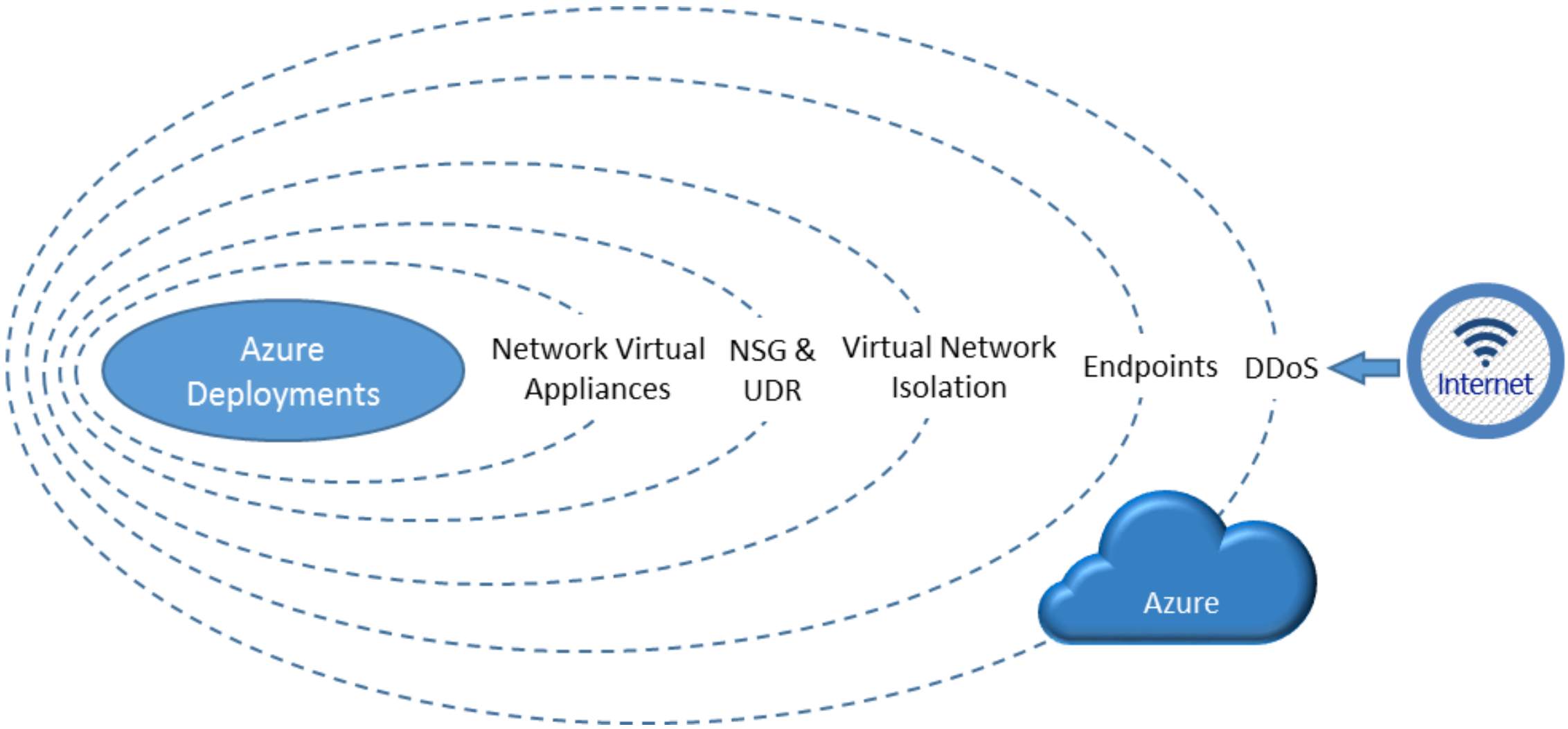
Azure Security Center integration

Intelligent DDoS Protection virtual network recommendation



Attack flow logs Azure Log Analytics view

Visualizing layers of security



Step 1

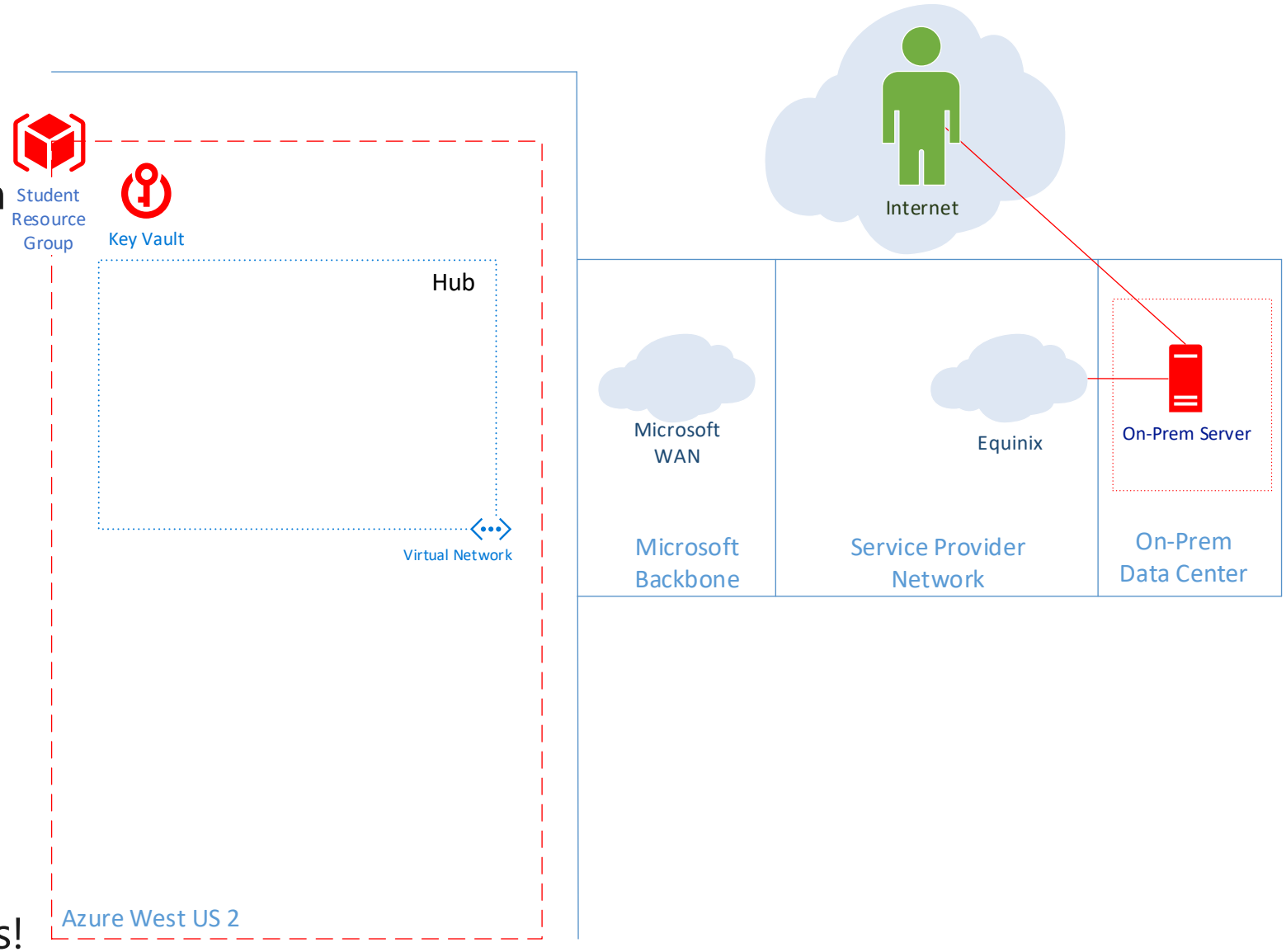
Execution:

1. Open a new PowerShell ISE session
2. Open WorkshopStep1.ps1
   (at `C:\vdcWorkshop\Scripts`)
3. Run `WorkshopStep1.ps1`

Validation:

1. Browse to your VNet in the Portal
2. Review the subnets
3. You should see three subnets

Take Away:
You now have a network in Azure
to which you can now deploy resources!



Step 2

Execution:

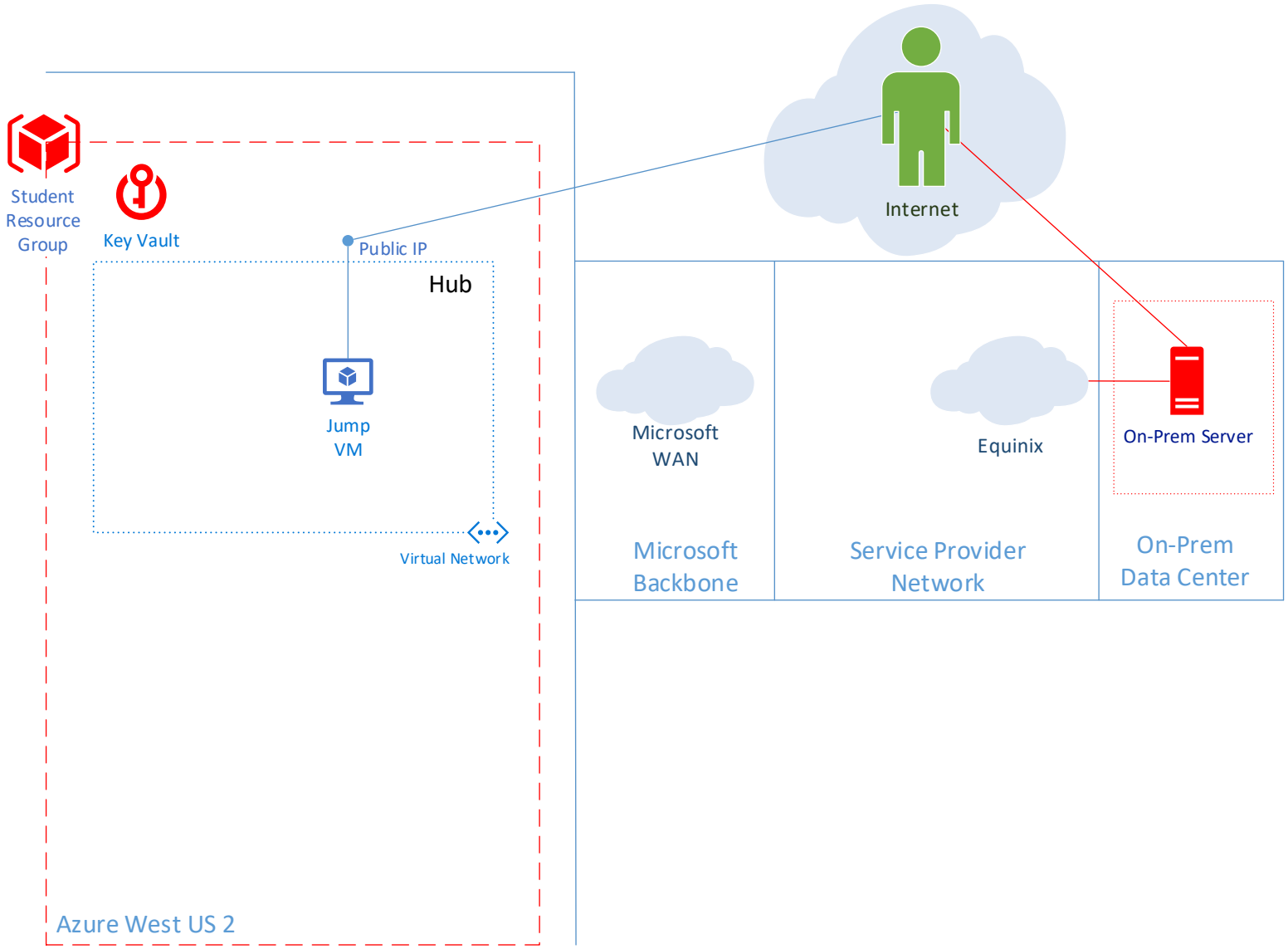
1. In a PowerShell ISE session
2. Open WorkshopStep2.ps1 (at `C:\vdcWorkshop\Scripts`)
3. Run `WorkshopStep2.ps1`

Validation:

1. Review the VM components
2. RDP to the public IP using User01 credentials from the Key Vault

Take Away:

You now know how to deploy a simple publicly accessible VM into a VNet in Azure.



Step 3

Execution:

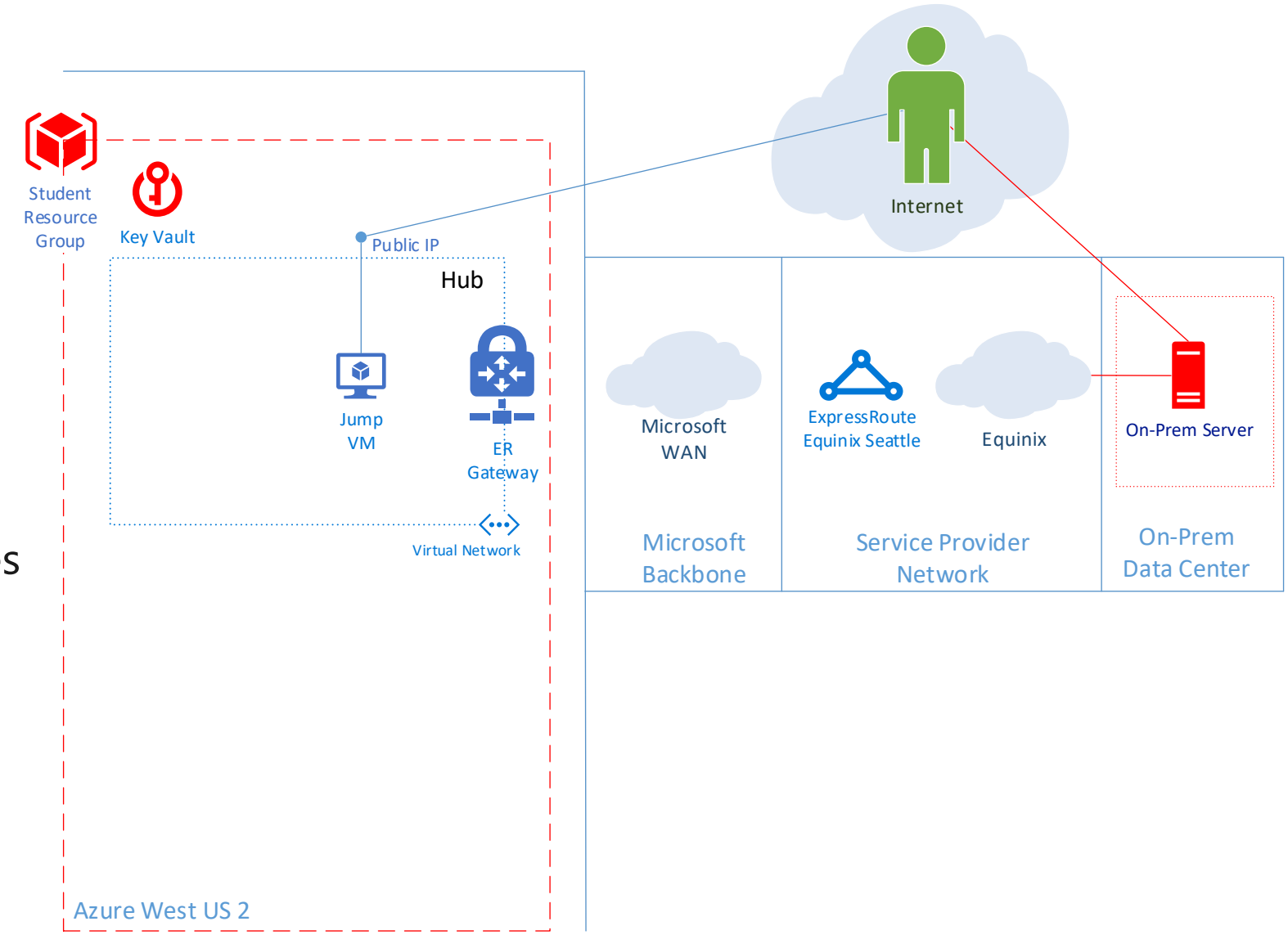
1. In a PowerShell ISE session
2. Open WorkshopStep3.ps1 (at **`C:\vdcWorkshop\Scripts`**)
3. Run `WorkshopStep3.ps1`

Validation:

1. In the portal explore the properties of both the new gateway and ExpressRoute circuit

Take Away:

You now know how to create an ExpressRoute circuit.



Also Announced:

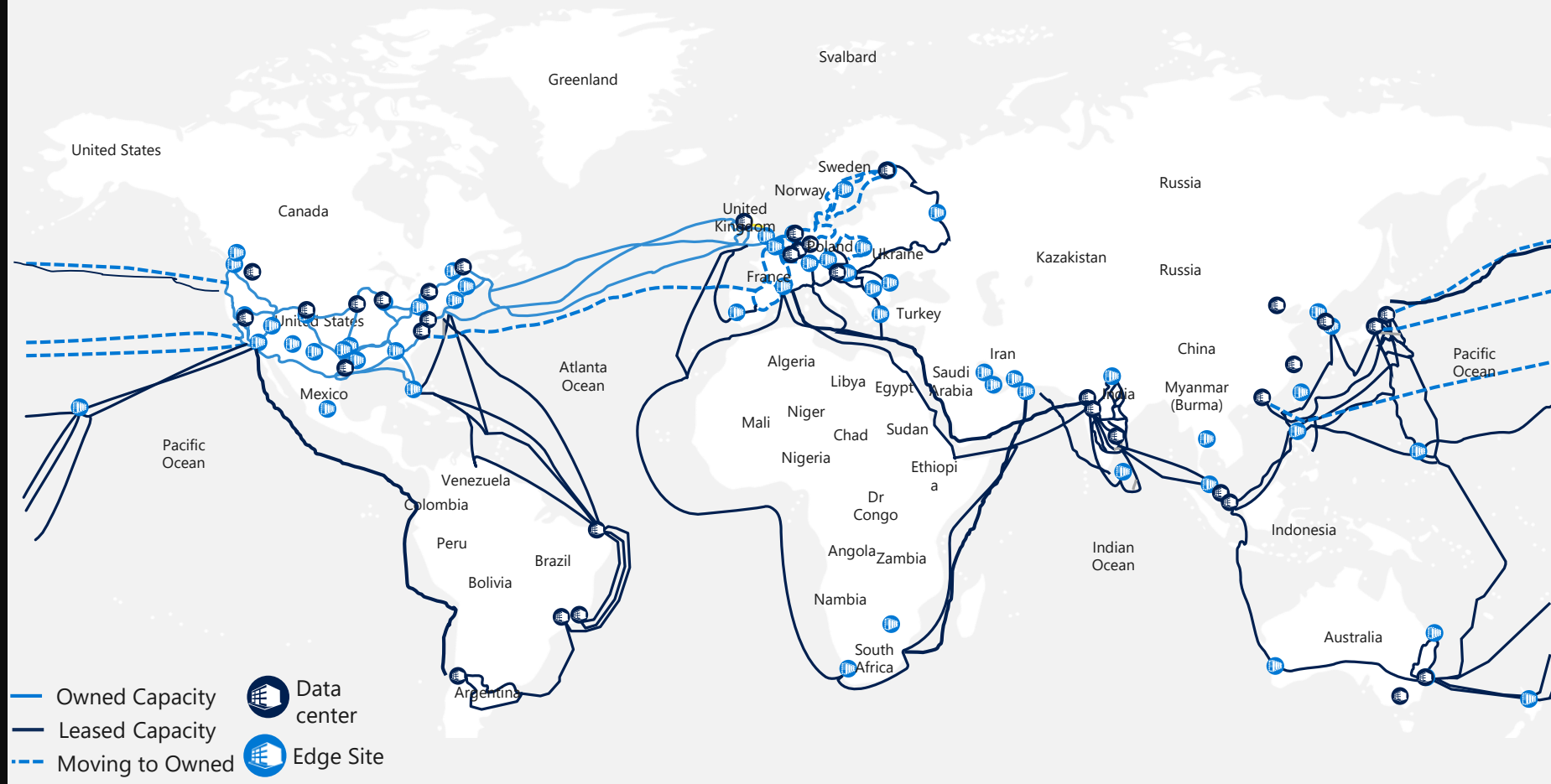
- Germany North
- Germany West Central
- Switzerland North
- Switzerland West
- Norway East
- Norway West
- UAE Central
- UAE North

Microsoft Global Network

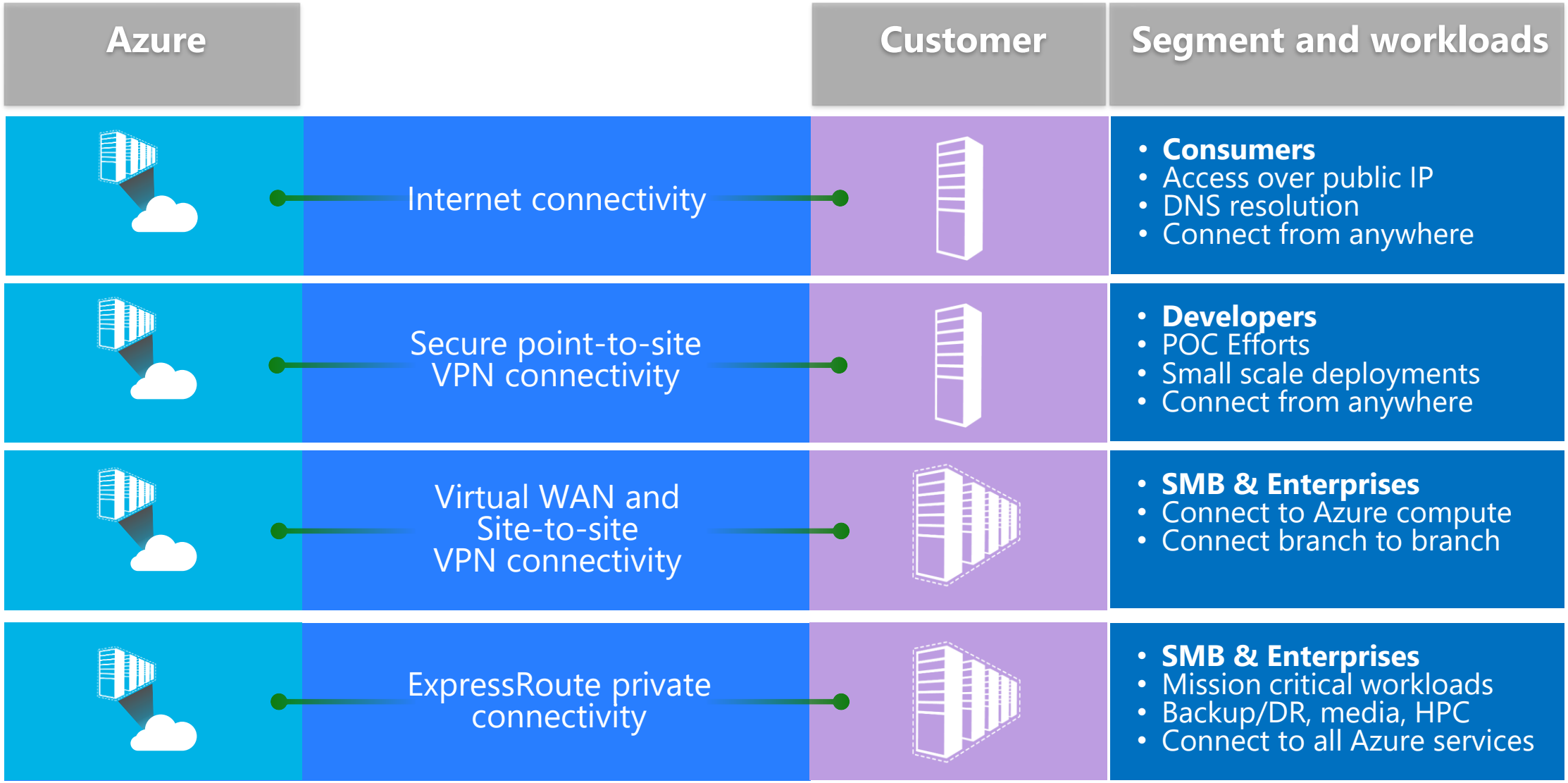
One of the largest private networks in the world

- 100K+ miles of lit fiber
- 130+ edge sites
- 8,000+ ISP sessions
- 44 ExpressRoute locations
- 200+ ExpressRoute Partners
- SDN Managed (SWAN, OLS)

DCs and Network sites not exhaustive

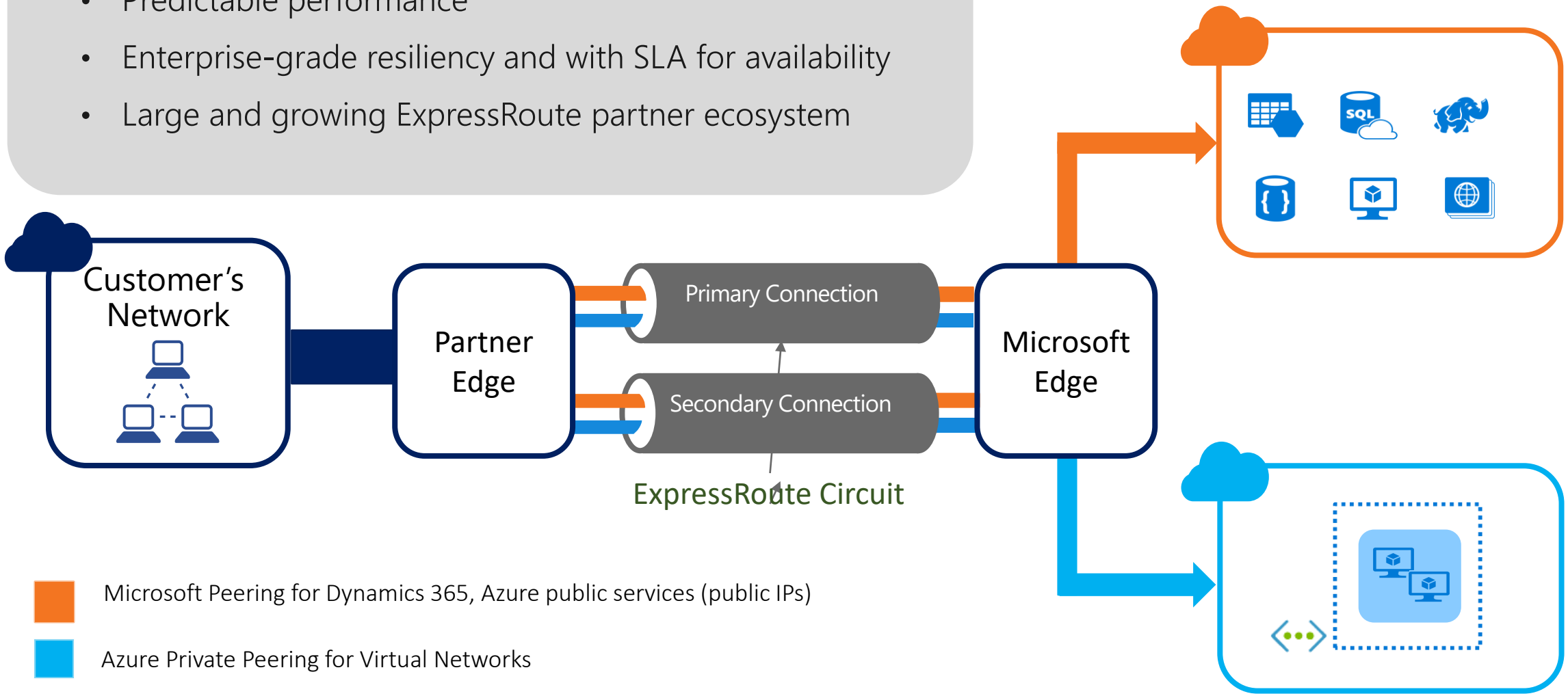


Connectivity options and hybrid offerings



Azure ExpressRoute

- Private connectivity to Microsoft
- Predictable performance
- Enterprise-grade resiliency and with SLA for availability
- Large and growing ExpressRoute partner ecosystem



200+ ExpressRoute Partners

Announcing
Azure ExpressRoute Direct

10X

Breaking the speed barrier

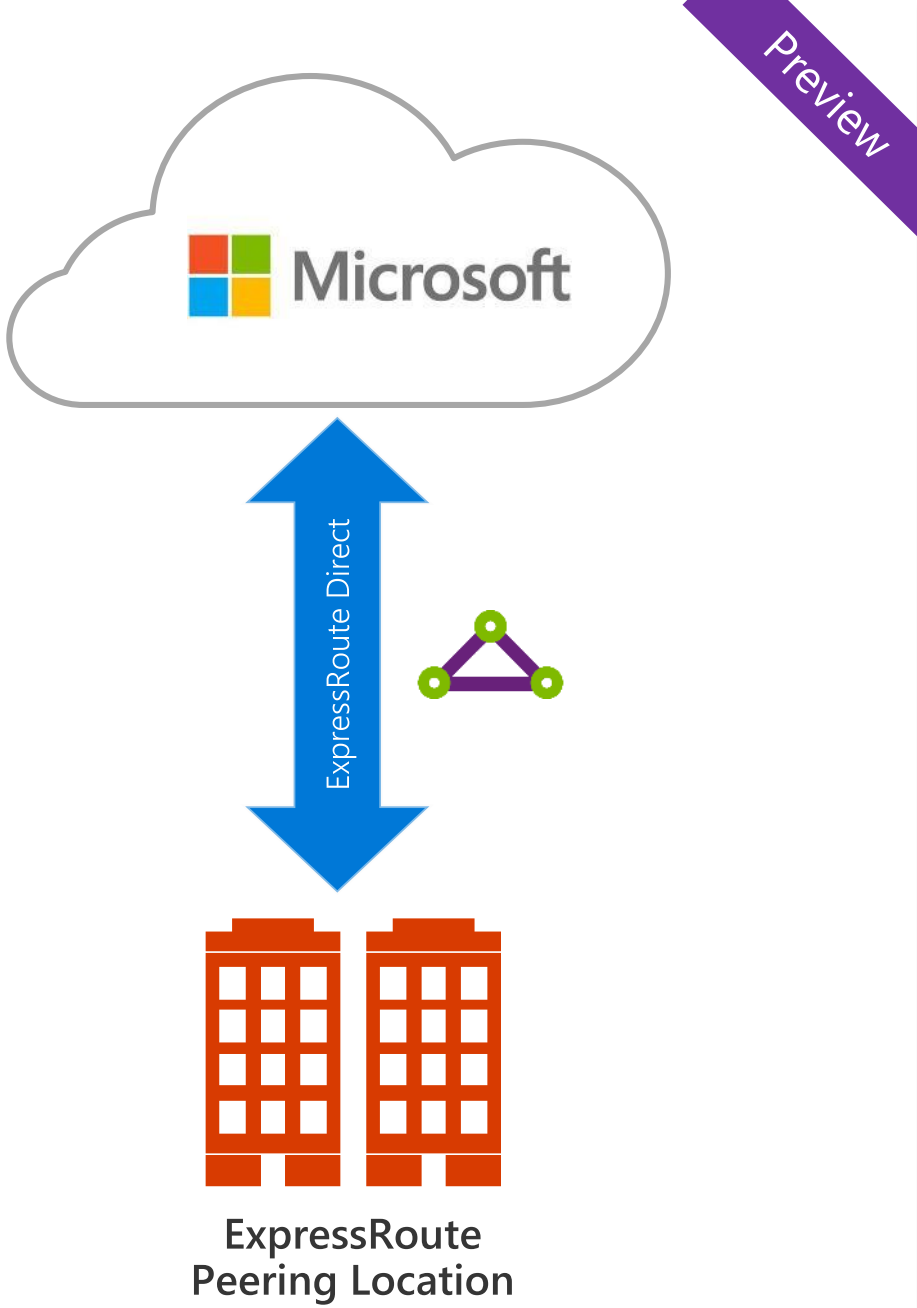
Fastest of all cloud providers!

100 Gbps direct to Azure

Built for customers with extreme bandwidth needs for massive data ingestion

Flexibility in bandwidth allocation

In-geo and global connectivity



ExpressRoute Global Reach

Deploy global site-to-site connectivity using the Microsoft global network

- On-demand connectivity between your sites using existing ExpressRoute circuits
- Complements your service provider's WAN solution
- Traffic stays on Microsoft's global network

Available in Public Cloud

- U.S., U.K., Hong Kong, Ireland, Netherlands, Japan
- *Australia, Singapore and Korea coming soon*

Available in US Government Cloud

Step 4

Execution:

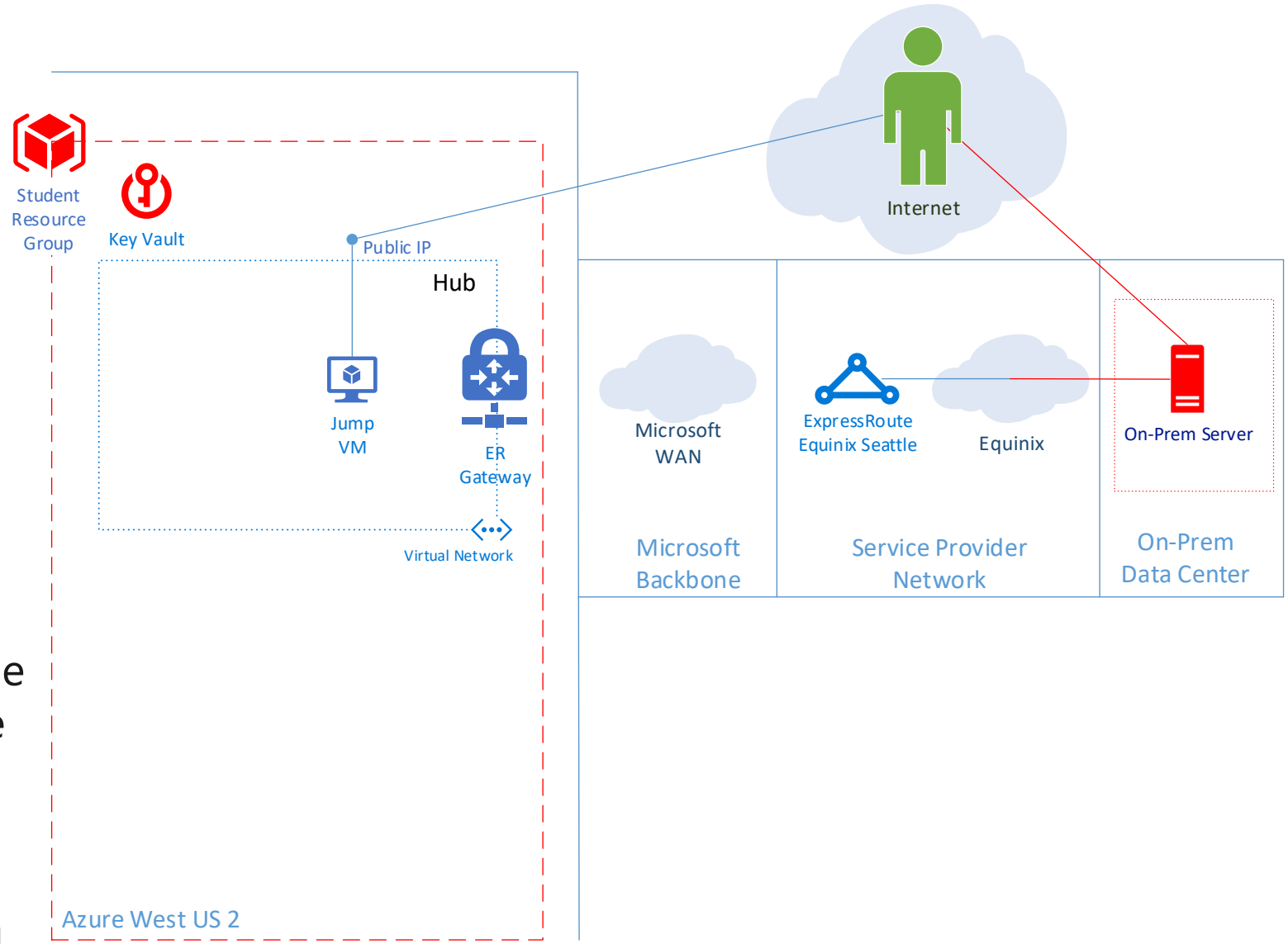
1. In a PowerShell ISE session
2. Open WorkshopStep4.ps1 (at `C:\vdcWorkshop\Scripts`)
3. Run `WorkshopStep4.ps1`

Validation:

1. In the portal, pull up the ExpressRoute circuit
2. Notice the provider status
3. In the Private Peering, check out the route table (you should see a route from on-premises).

Take Away:

You should have a basic understanding of connecting on-premise to Microsoft's network edge.



Step 5

Execution:

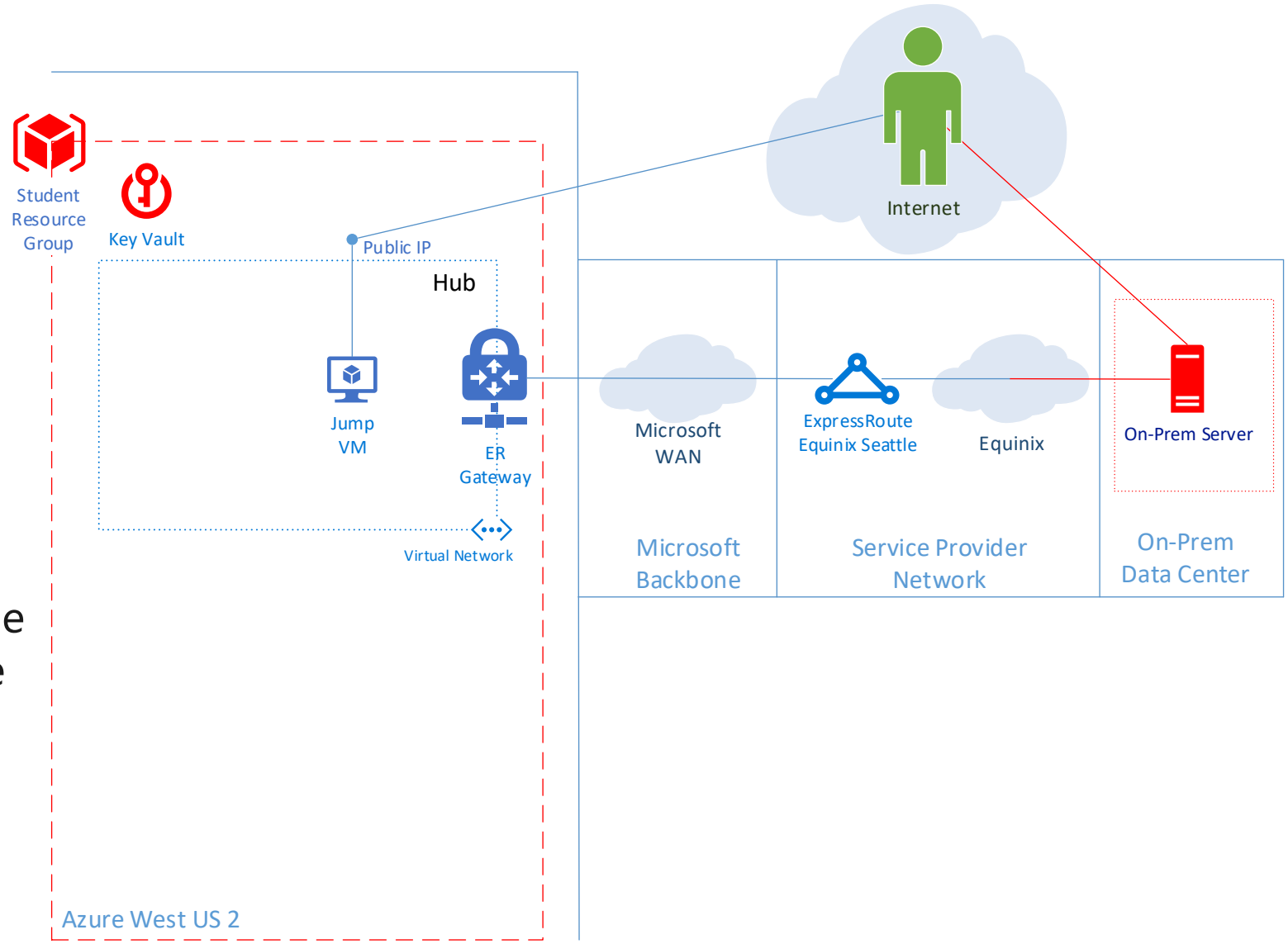
1. In a PowerShell ISE session
2. Open WorkshopStep5.ps1 (at `C:\vdcWorkshop\Scripts`)
3. Run `WorkshopStep5.ps1`

Validation:

1. In the portal, pull up the ExpressRoute circuit
2. In the Private Peering, check out the route table (you should see a route from on-premises and multiple routes from your VNet).
3. RDP to the private IP of the Azure VM

Take Away:

You have now connected both networks!



Azure Firewall

Cloud native stateful Firewall as a service

A first among public cloud providers

Central governance of all traffic flows

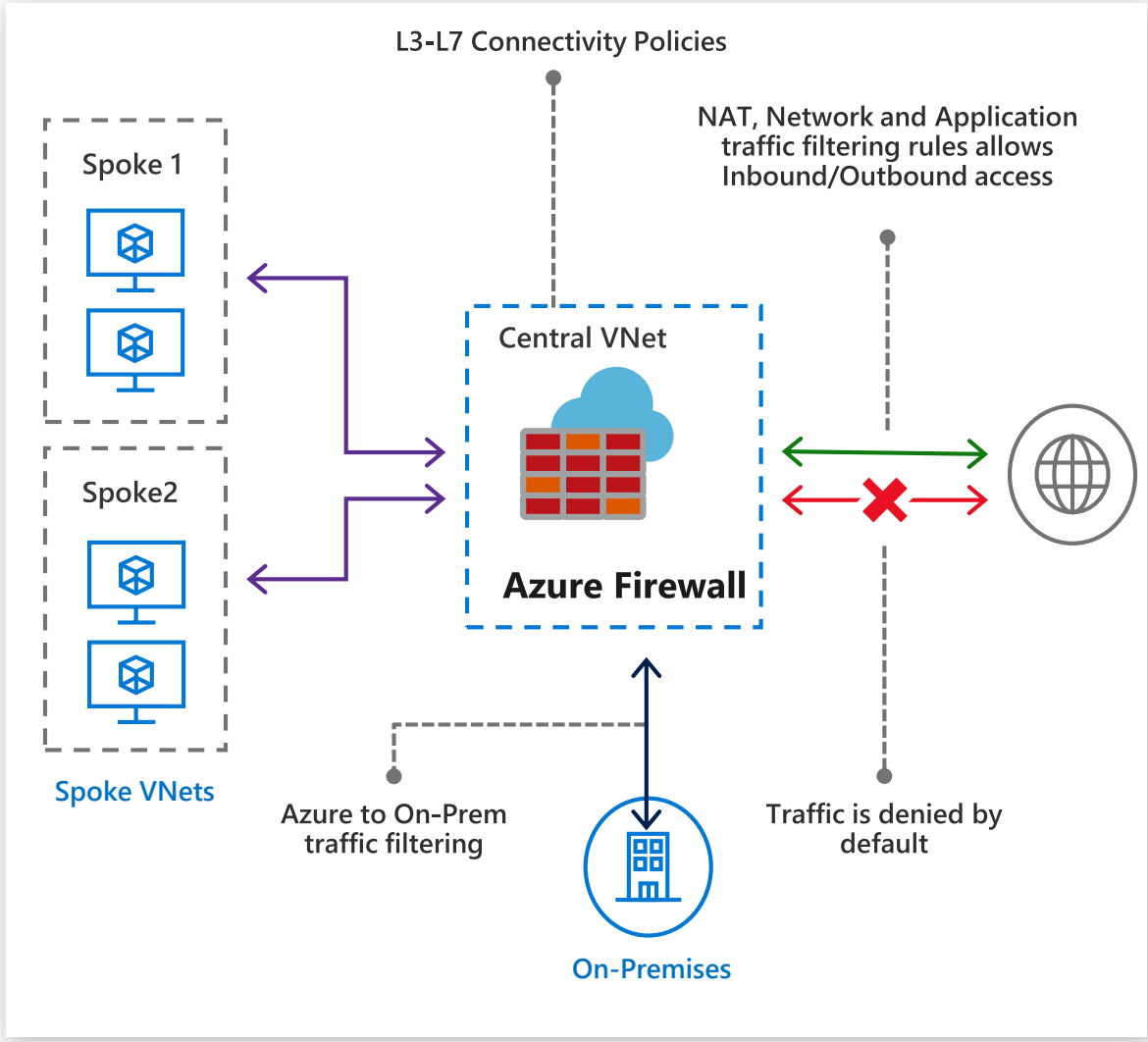
- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions

Complete VNET protection

- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)

Centralized logging

- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice



Step 6

Execution:

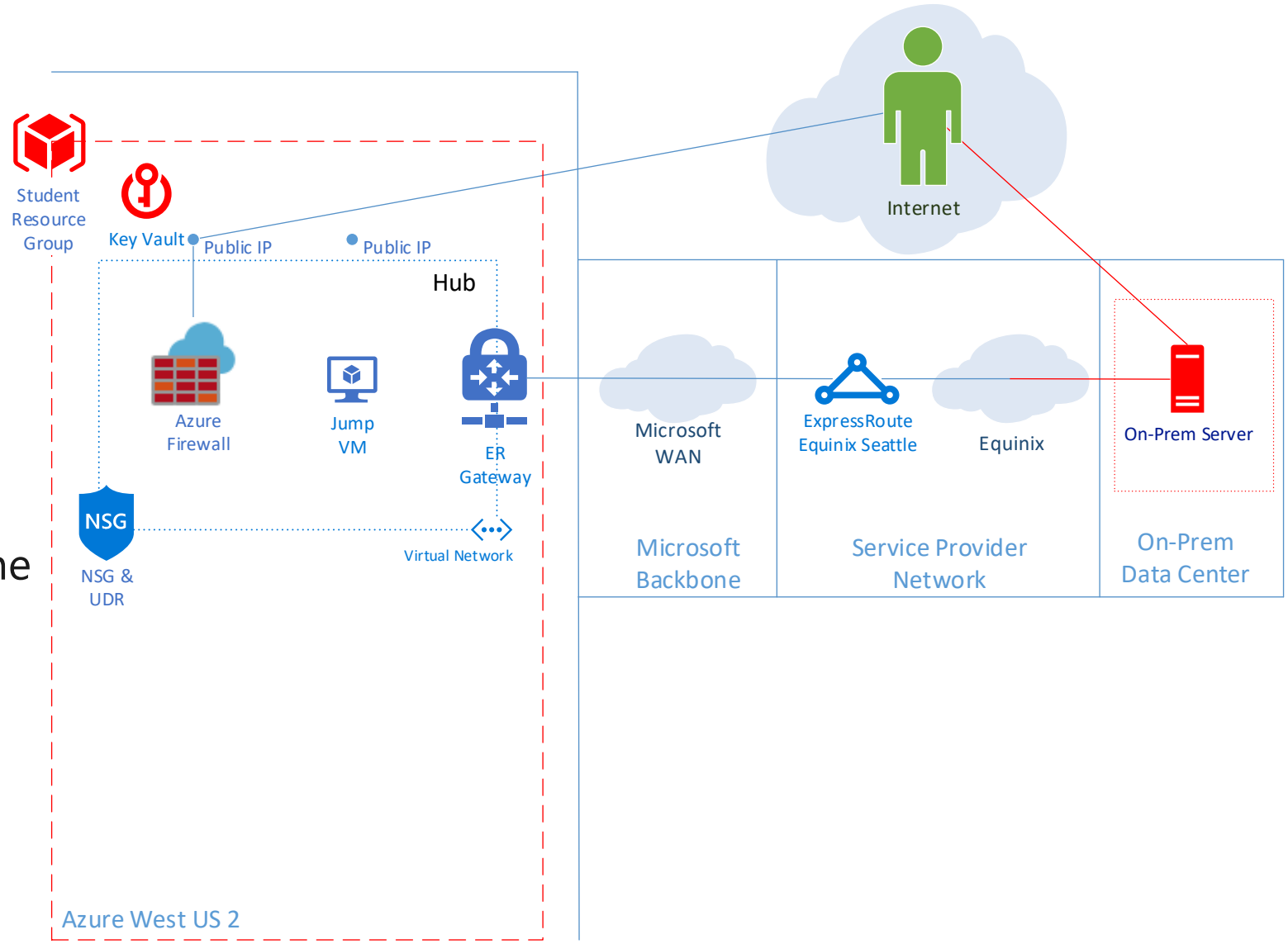
1. In a PowerShell ISE session
2. Open WorkshopStep6.ps1 (at **`C:\vdcWorkshop\Scripts`**)
3. Run `WorkshopStep6.ps1`

Validation:

1. In the portal, pull up the Firewall
2. Review the properties, especially the Rules section.
3. Try RDPing to your Azure VMs public IP, because we don't have a rule for that, it will fail.

Take Away:

You just protected your resources from the Internet.



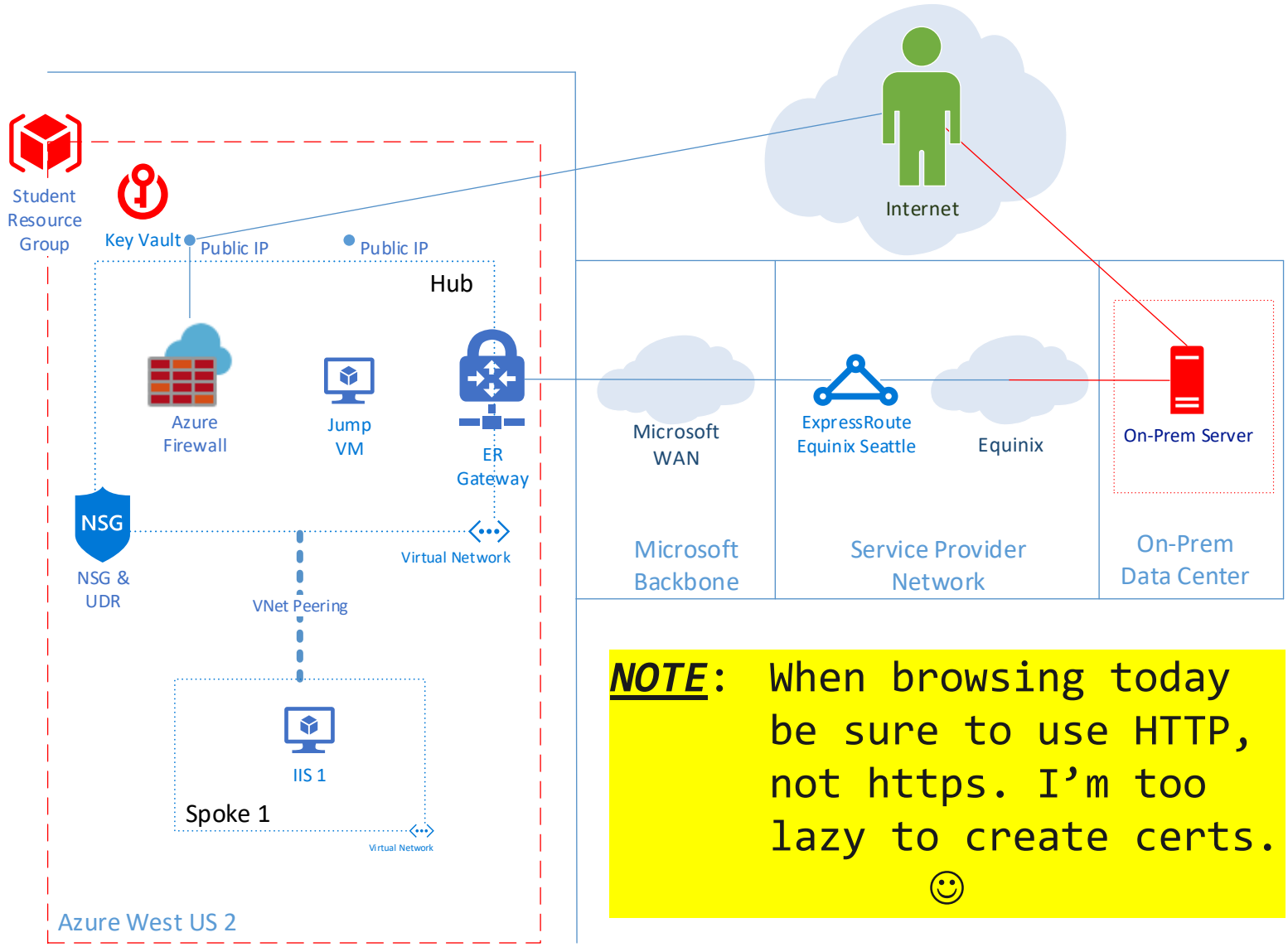
Step 7

Execution:

1. In a PowerShell ISE session
2. Open WorkshopStep7.ps1 (at **C:\vdcWorkshop\Scripts**)
3. Run WorkshopStep7.ps1

Validation:

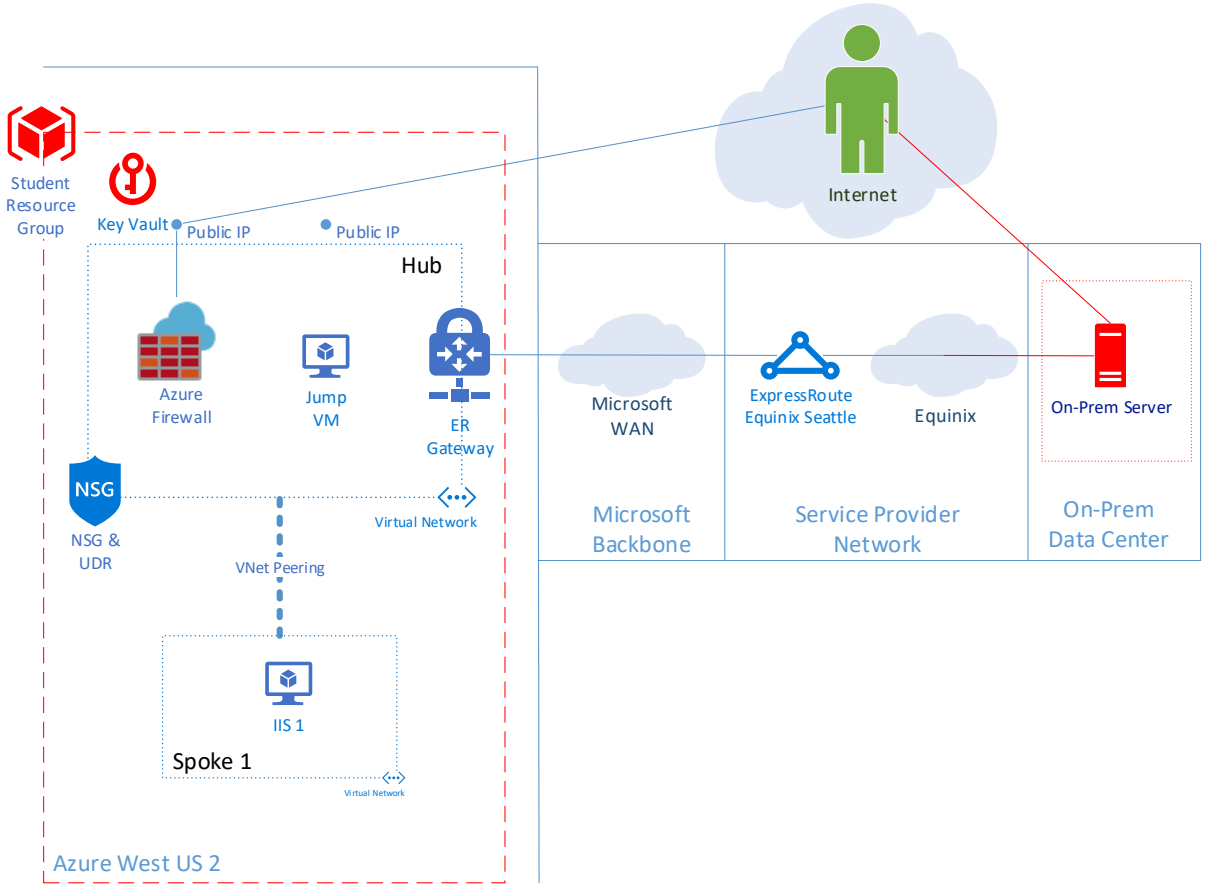
1. In the portal, pull up the Firewall
2. Review the Rules section.
3. From a browser hit the public IP of the firewall (it will NAT to the IIS server and provide a web page)
4. Hit the private IP of the IIS server (the firewall network rules should allow the page to be visible)



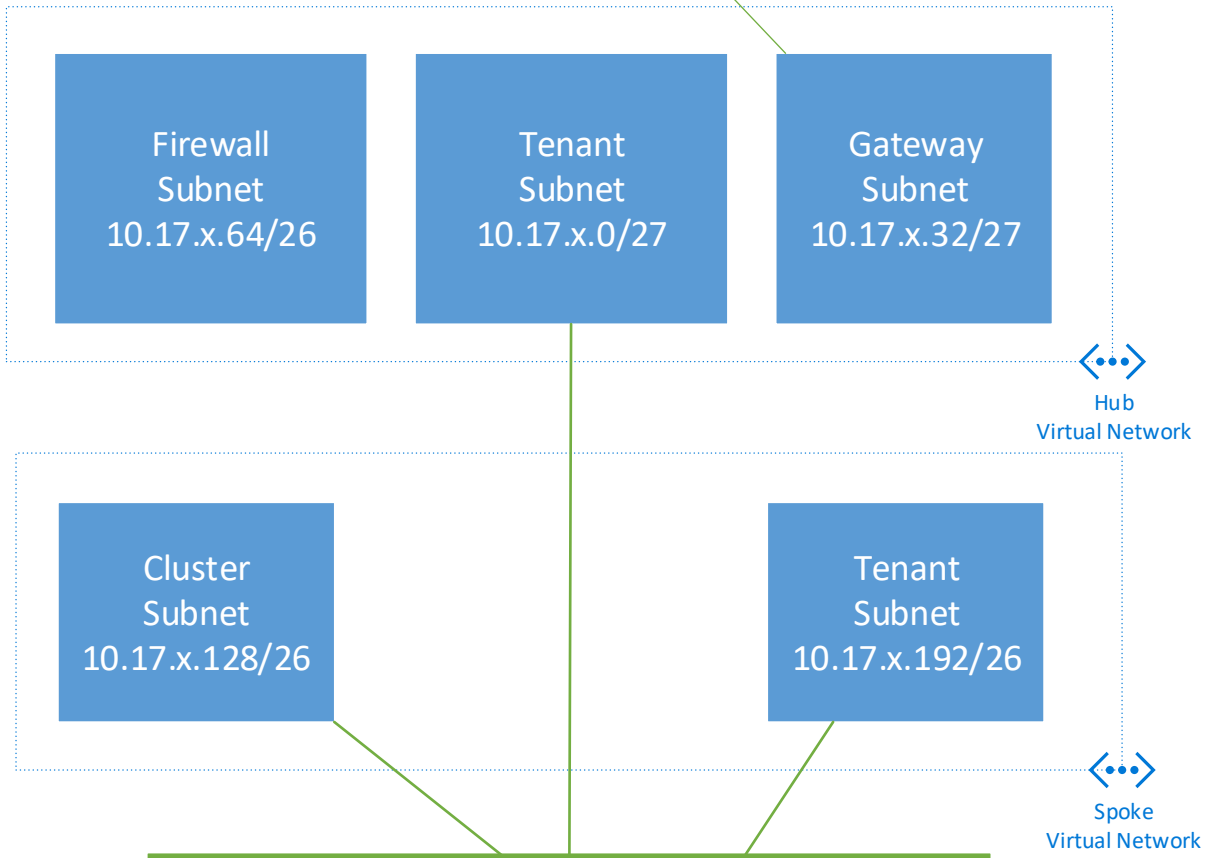
NOTE: When browsing today be sure to use HTTP, not https. I'm too lazy to create certs. ☺

Take Away:
You just deployed your company's first web site!

UDR



Prefix	Description	Next Hop
10.17.x.0/27	Hub Tenant	Firewall
10.17.x.128/25	Spoke VNet	Firewall



Prefix	Description	Next Hop
0.0.0.0/0	All Addresses	Firewall
(BGP propagation turned off on this table)		

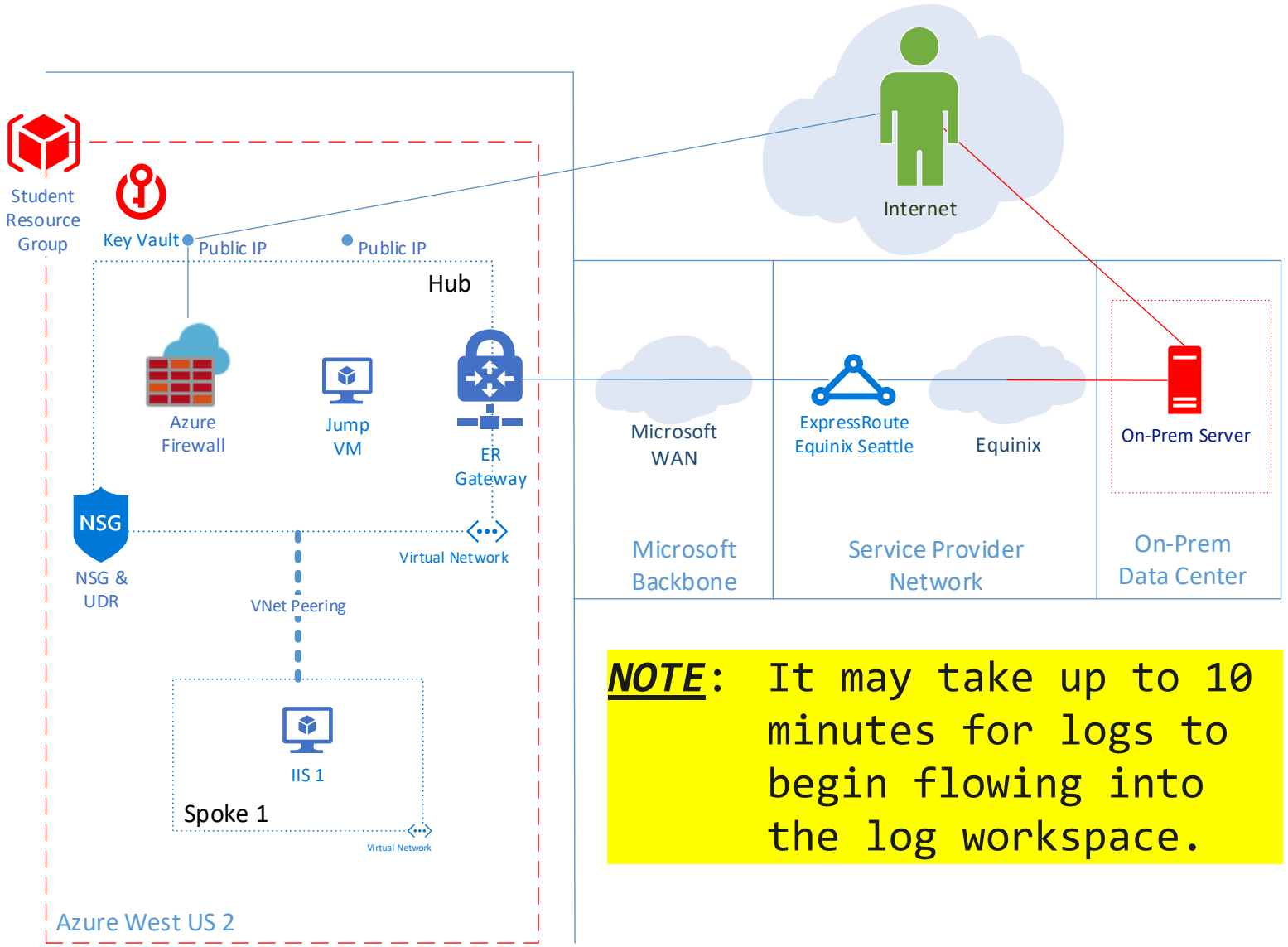
Step 7 (cont)

Execution:
Let's turn on and review monitoring

1. In the portal open the firewall
2. Click the "Diagnostic settings" tab
3. Click the "Turn on diagnostic" link
4. Name your setting "Firewall-Logs"
5. Check "Send to Log Analytics"
6. Select your Company's workspace
7. Check both log types and save

Validation:

1. In your Resource Group open your "Log Analytics workspace"
2. Open the "Logs" tab
3. In the Query Window paste one of the queries from: http://aka.ms/vdcFWQuery



NOTE: It may take up to 10 minutes for logs to begin flowing into the log workspace.

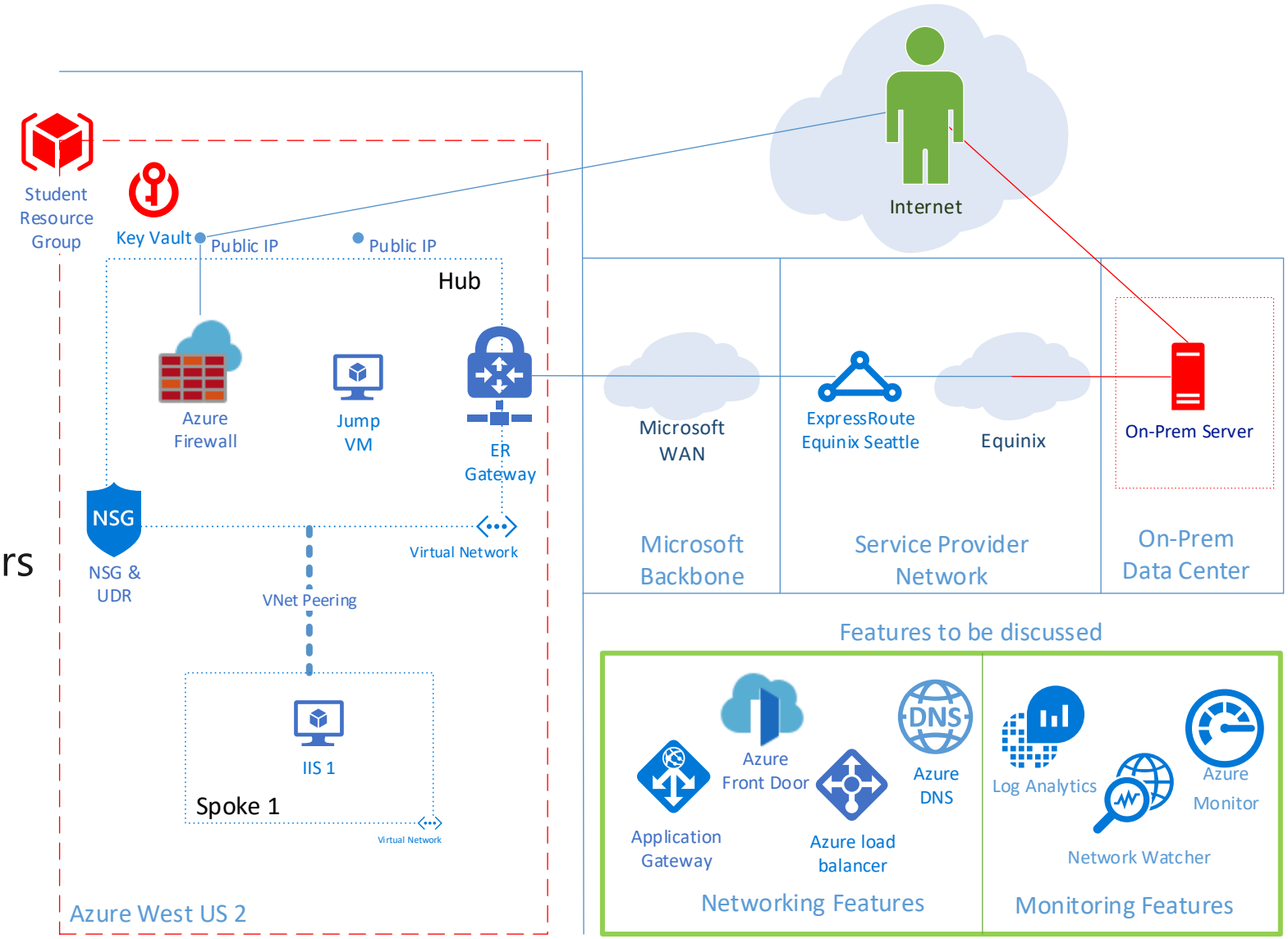
Final

Discussion:

- Virtual WAN

- Load Balancing Overview
- Global: Azure Front Door
- Global: Traffic Manager
- Regional: Application Gateway
- Regional/Local: Azure Load Balancers

- Azure DNS



Azure Virtual WAN

GA

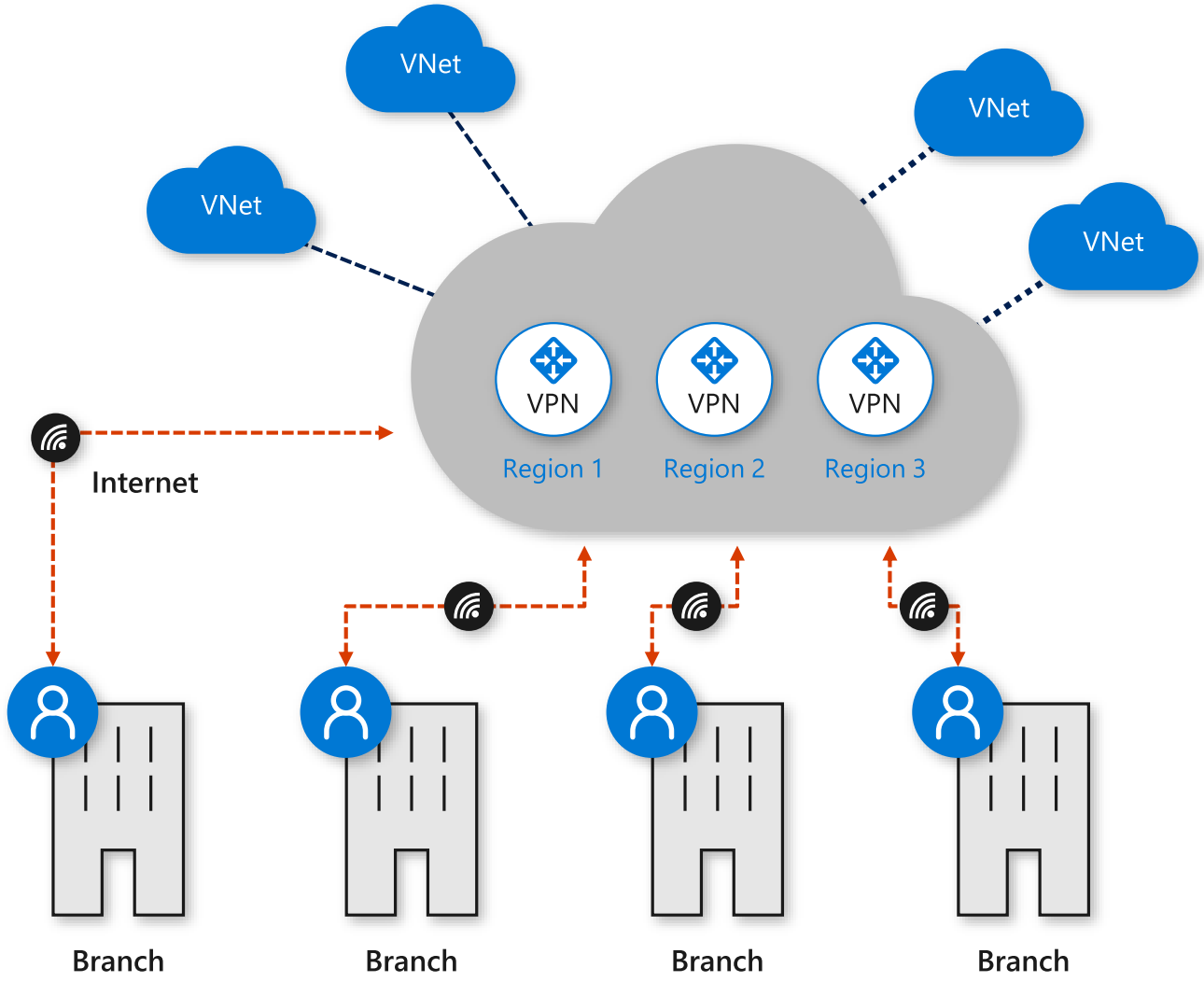
Easy deployment of large-scale branch connectivity

Branch to Azure, Branch to Branch

Automated provisioning and configuration

Scalability and high throughput

Large and growing integrated partner ecosystem



Azure Virtual WAN – Unified Cloud Connectivity

GA

Features

Hubs in Azure

Enable/disable branch to branch

IPsec IKEv1 and IKEv2

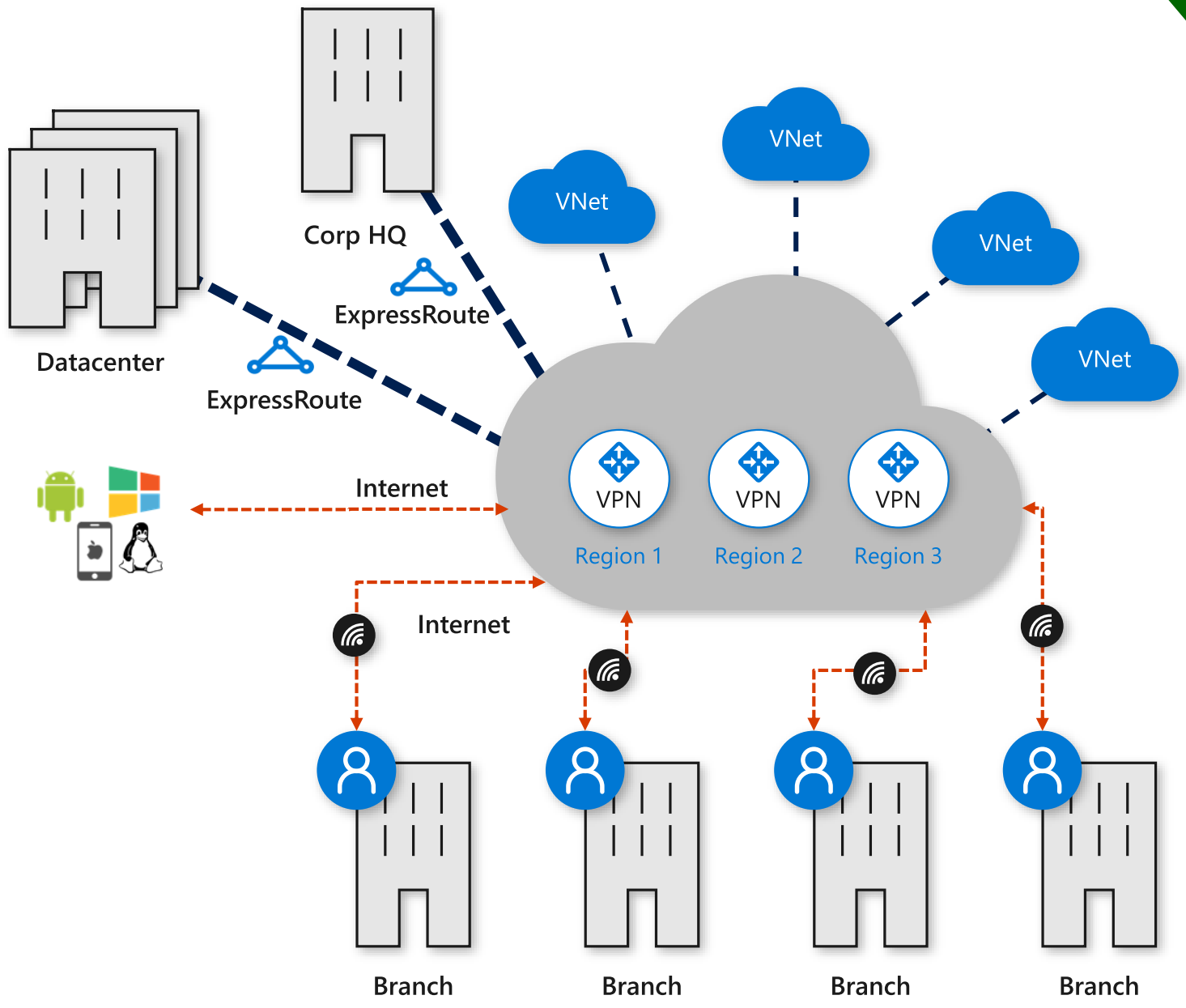
Scale unit-based billing

E2E Monitoring and Resource Health

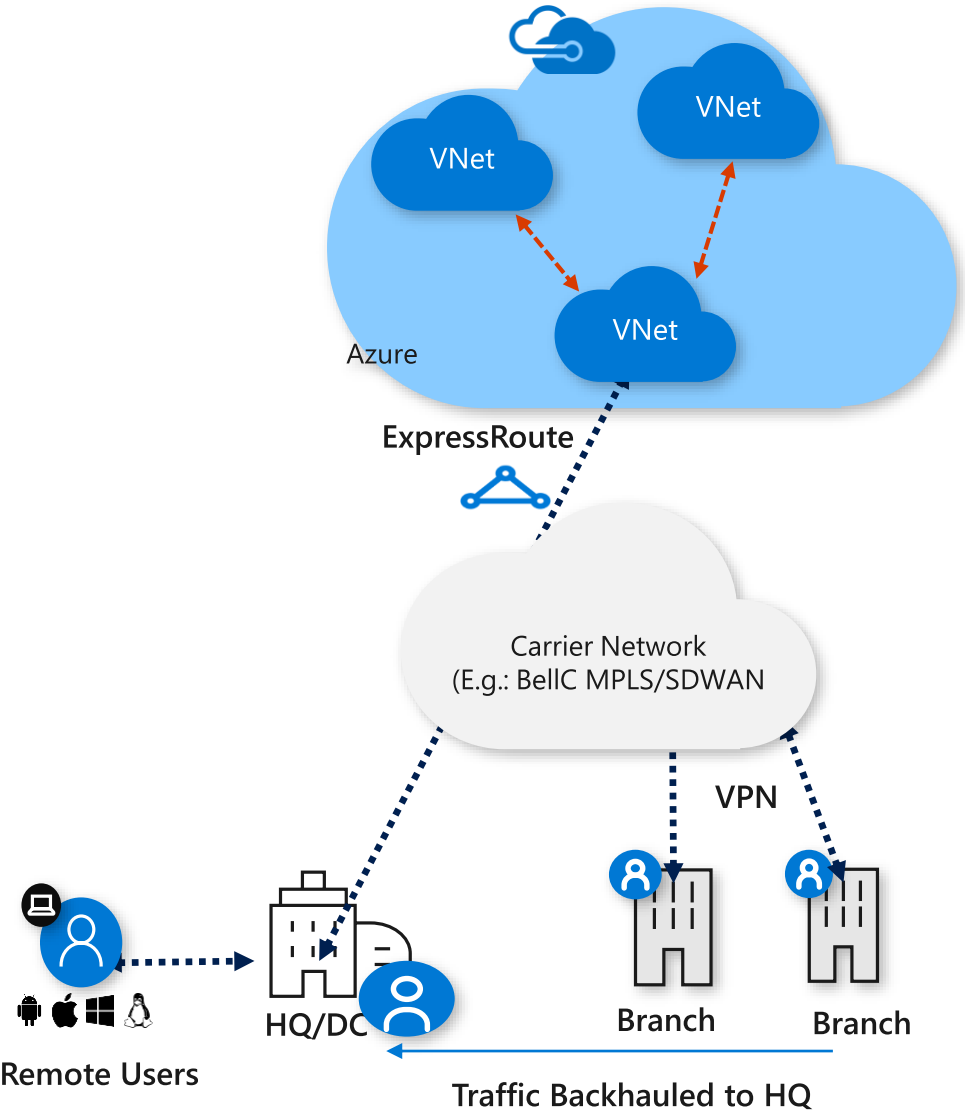
ExpressRoute (Preview)

P2S with IKEv2 and OpenVPN (Preview)

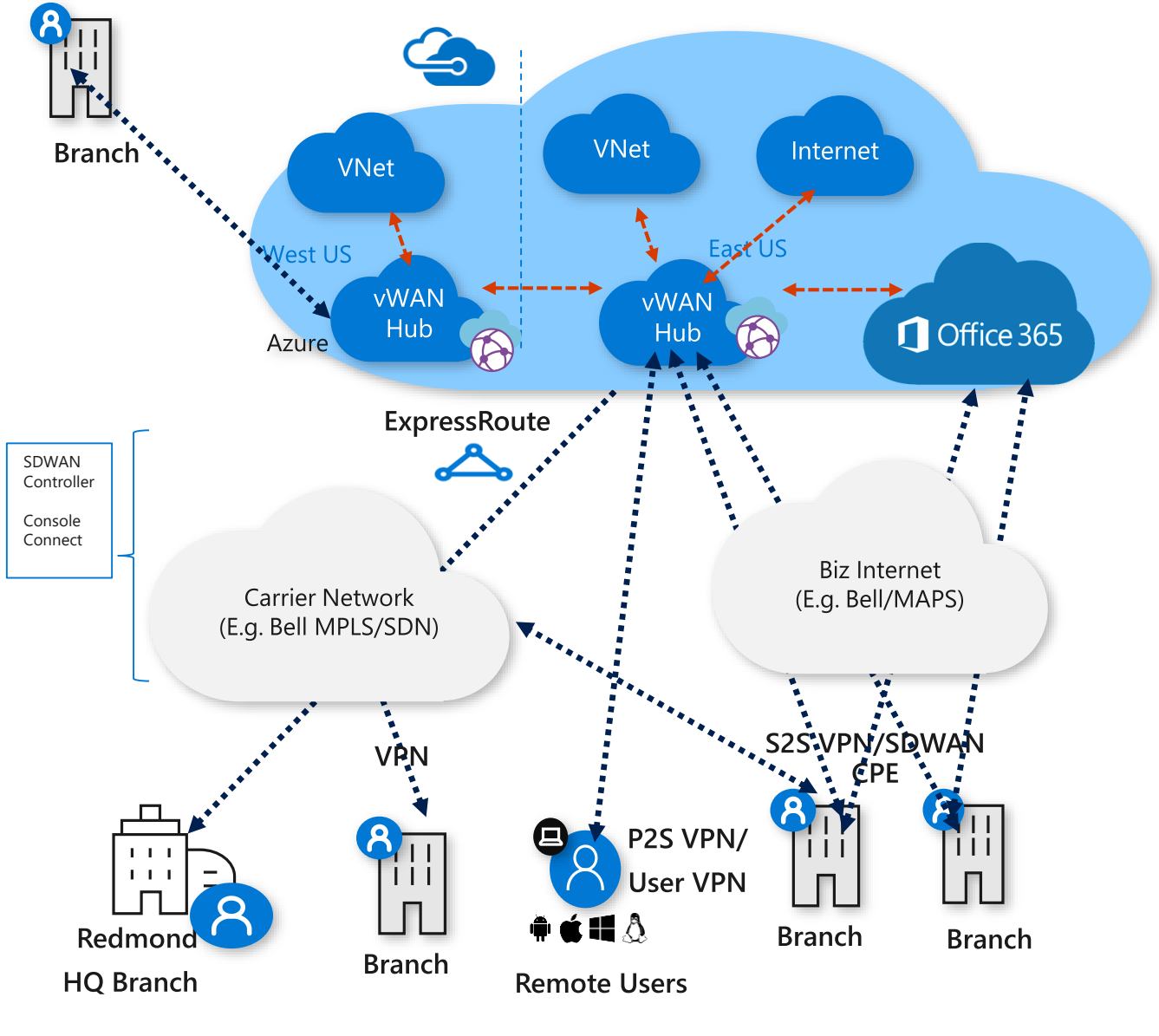
O365 Policy (Preview)



Traditional WAN



Azure vWAN



Azure Virtual WAN Partners

Coming soon

nuagenetworks
From Nokia

velocloud™
Now part of VMware

Azure Front Door Service

Preview

Your global entry-point to the cloud

Application acceleration

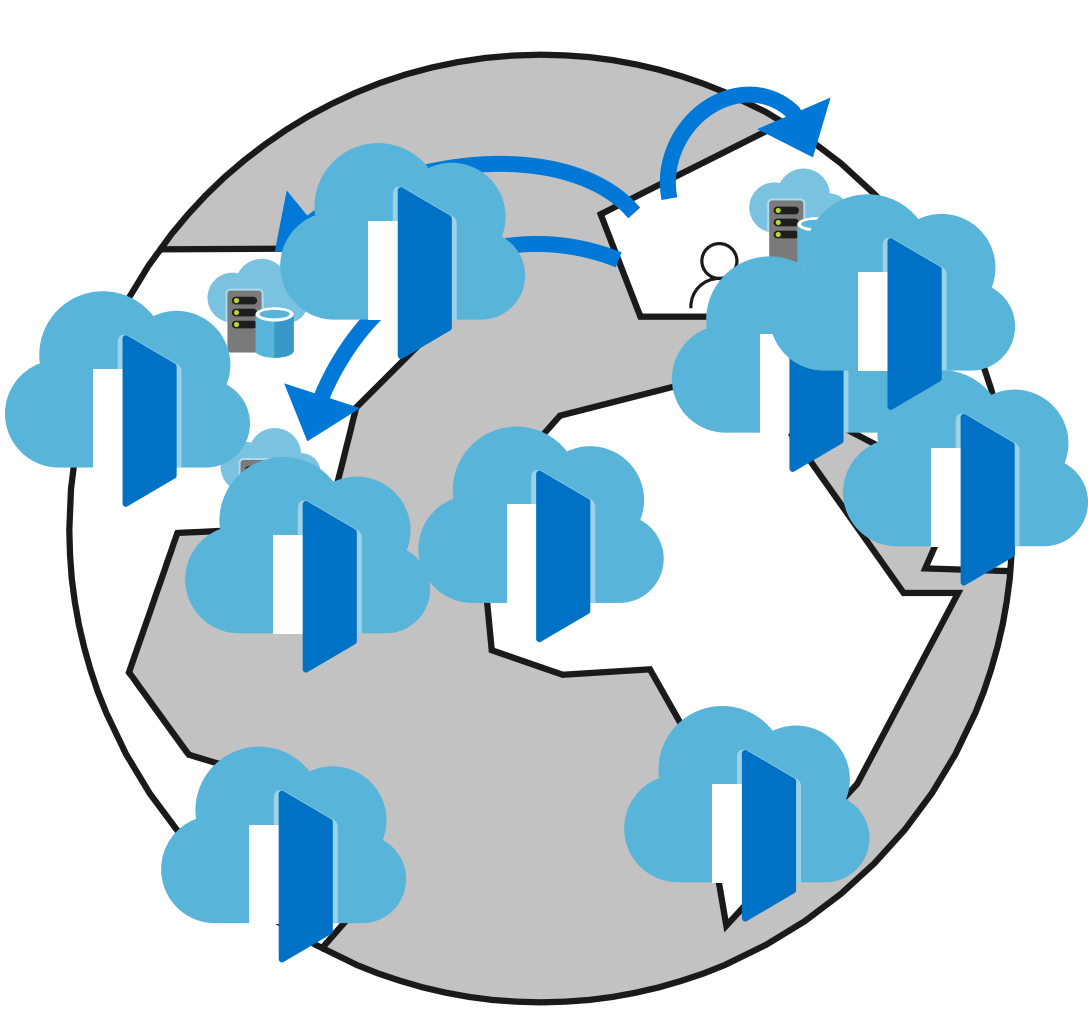
- HTTP proxy at the edge of Microsoft's global network
- Reduce latency and improve throughput for your app
- Scale out with massive SSL offload
- Supports IPv6

Global HTTP/S load balancing

- Active probing with global instant failover
- Path based routing for microservices
- Request rate limiting
- Sticky, weighted and priority routing

Global insights

- Central traffic dashboard
- Regional backend health



Azure Traffic Manager

Smart Traffic Engineering for Azure and external endpoints

Intelligent Routing

Geo, Subnet, Failover, Latency & Weighted

Traffic View

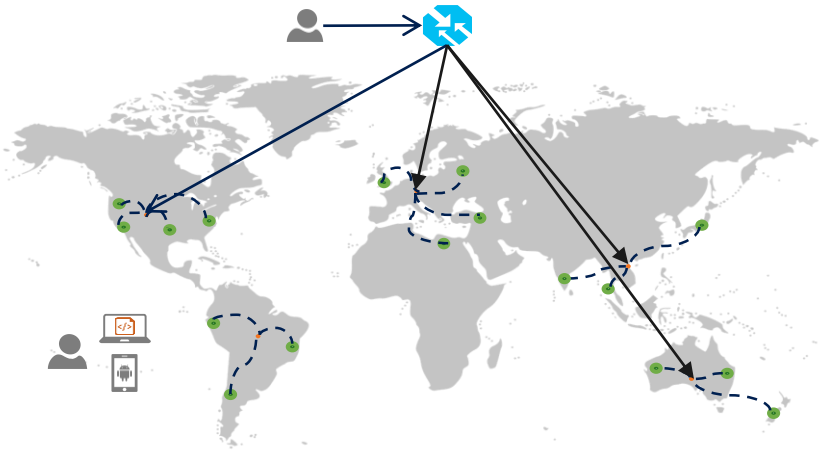
Actionable Insights on real time data

Analytics and Logs

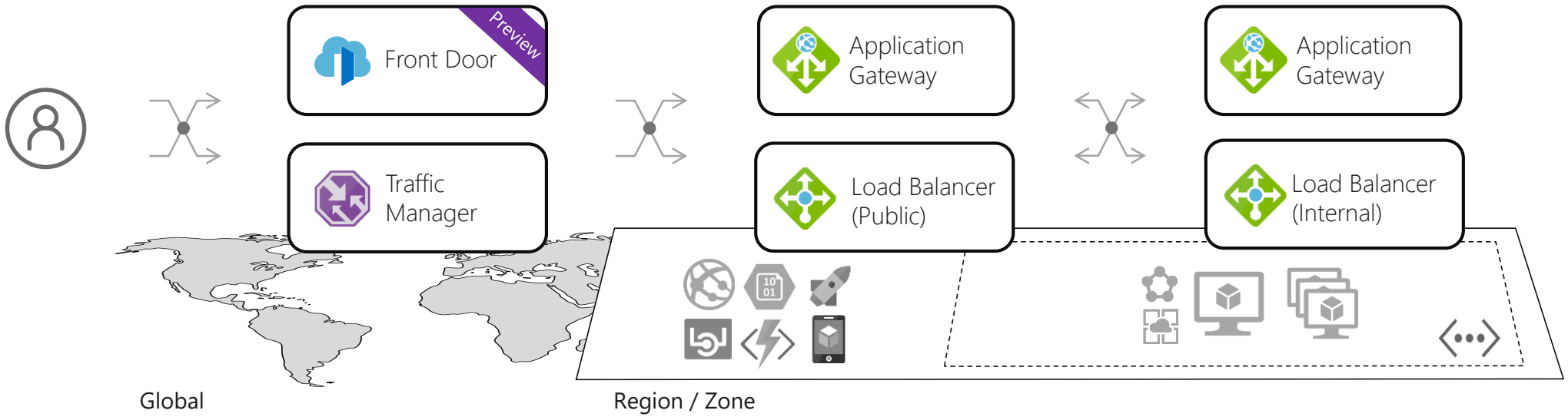
Identify patterns & detect threats

What's new

- Add your endpoints using IPv4 / IPv6 addresses
- Multi-value responses for increased availability
- Route traffic to multi-tenant endpoints using custom headers
- Specify custom HTTP response codes to indicate endpoint health
- Subnet routing: Deliver customized content for ISPs or corporate offices



Load balancing in Azure



Global

Route to your closest available service region or your on-prem DC. Offload SSL, improve performance / accelerate websites at the Edge.

Regional

Route across zones and into your VNET. Offload SSL and build your application-specific logic.

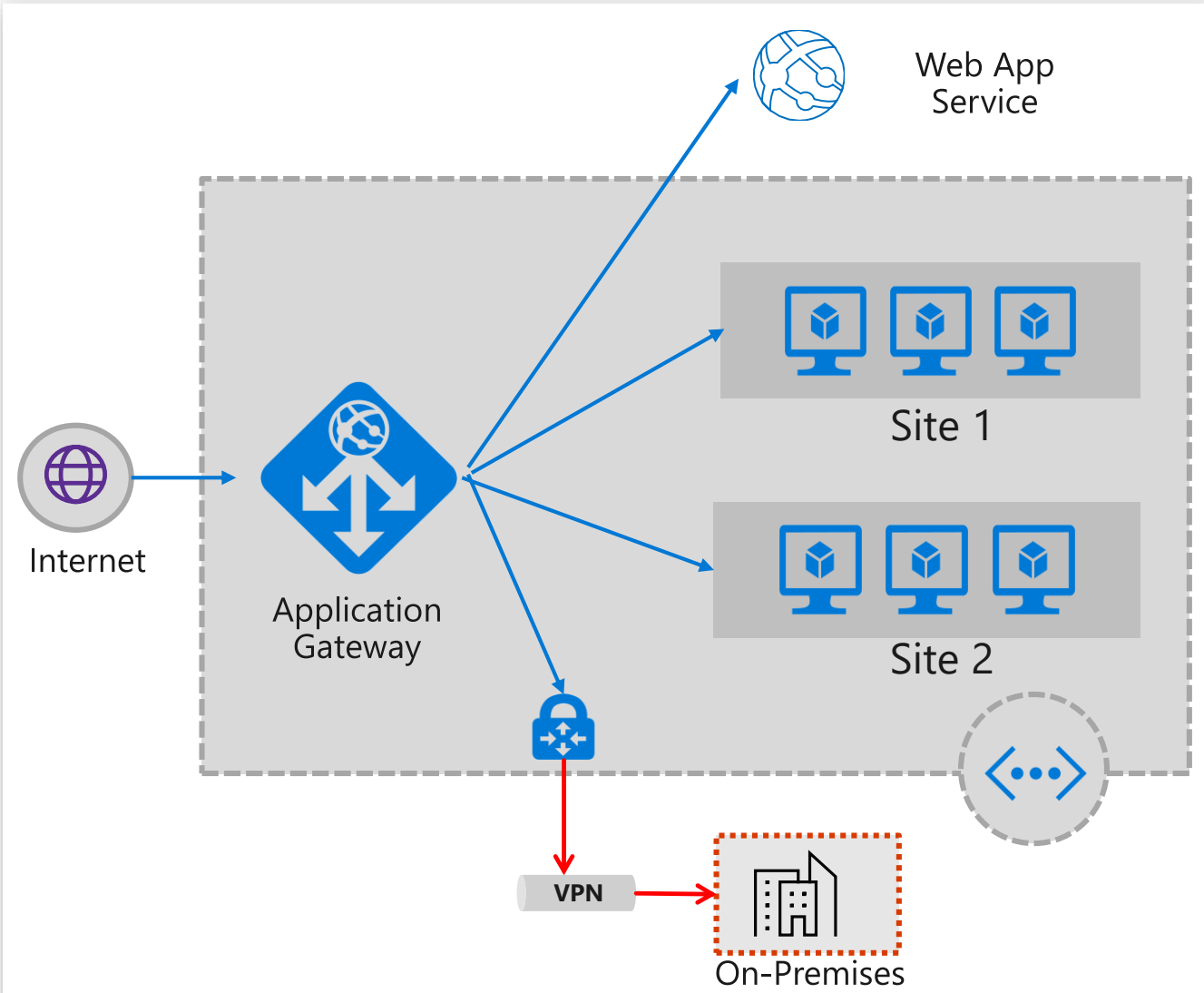
Internal

Route across and between your resources to build your regional application.

Application Gateway

Layer 7 load balancer for web applications

Platform managed built in high availability and scalability
Layer 7 load balancing URL path, host based, round robin, session affinity, redirection
Centralized SSL management SSL offload and SSL policy
Public or ILB public internal or hybrid
Rich diagnostics Azure monitor, Log analytics



What's New

Features

Connection draining support
Custom error pages
Ingress Controller for Azure Kubernetes Service (AKS) preview

Diagnostics

Enhanced multi dimensional metrics
Diagnose connectivity issues with Network Watcher integration

Portal enhancements

Complete API Parity
SSL policy, VMSS, Web App Services, Custom error pages, Redirection, Connection draining

And more features ...

Application Gateway continued what's new

Preview

Performance and scalability

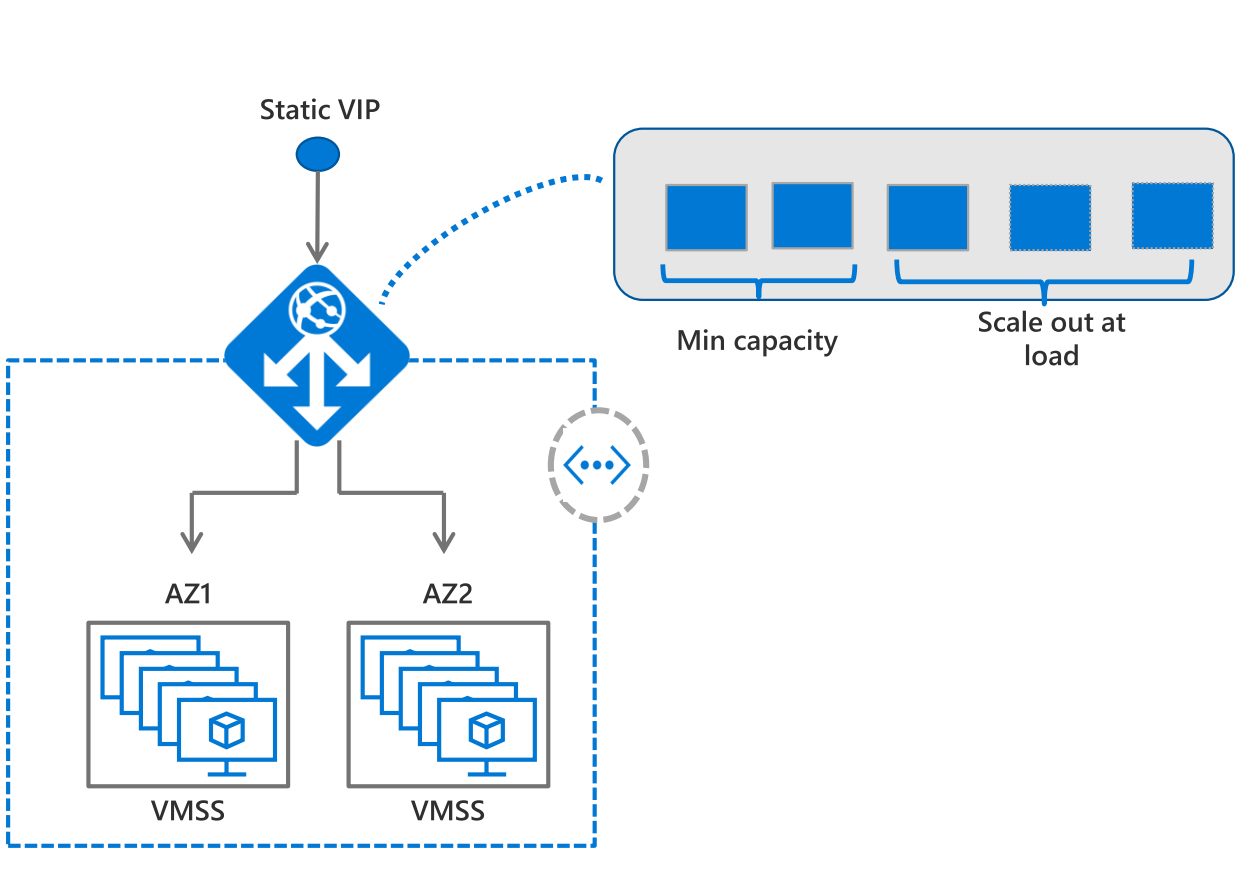
Autoscaling
Grows and shrinks based on application traffic requirements
Reduce operating cost

Better performance 5X better SSL offloads
550 connections/sec with RSA 2048 bit key Certs
30,000 persistent connections
2500 HTTP req/sec

Faster provisioning and configuration update
75% reduction in provisioning time (~5 mins)
85% reduction in config updates time (~40 secs)

Enhanced resiliency
Built in Azure zone redundancy
Choose single zone or multi zone Application Gateway

Feature enhancements
Robust Application Gateway IP static VIP
More features upcoming (Key Vault integration, modify headers)



Azure Load Balancer

Cloud native network load balancer

Built-in high-availability and performance

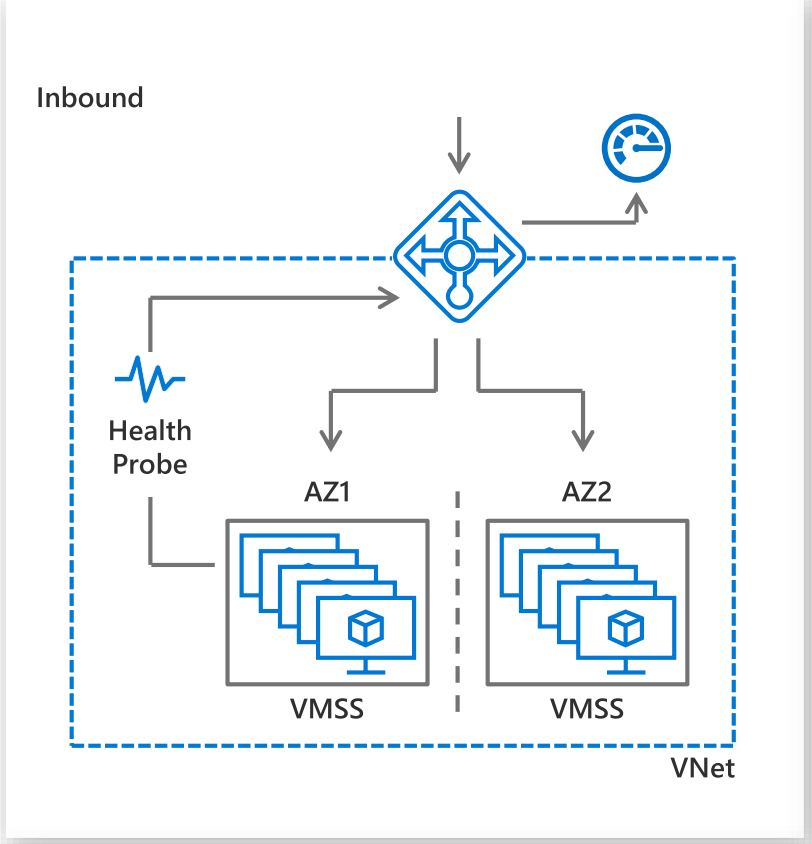
- Inbound and Outbound
- Public and Internal load balancing
- Availability Zones

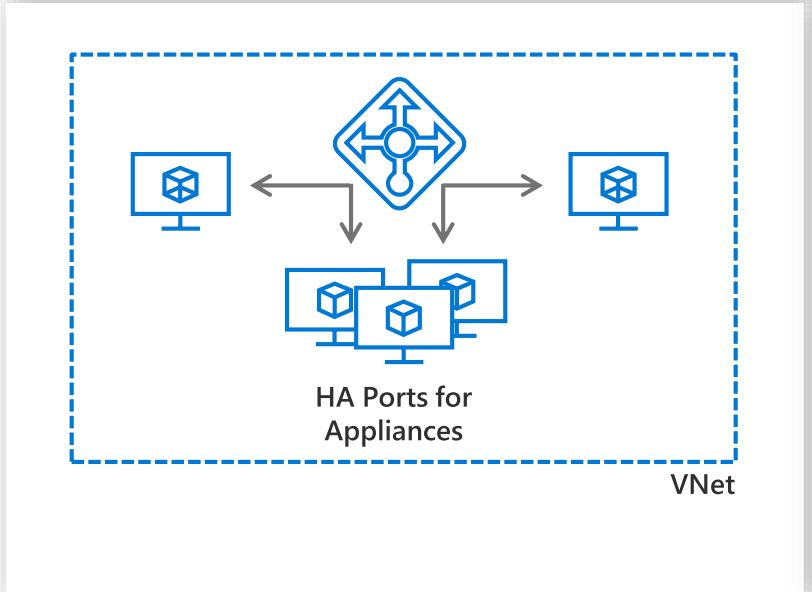
Flexible for all TCP or UDP applications

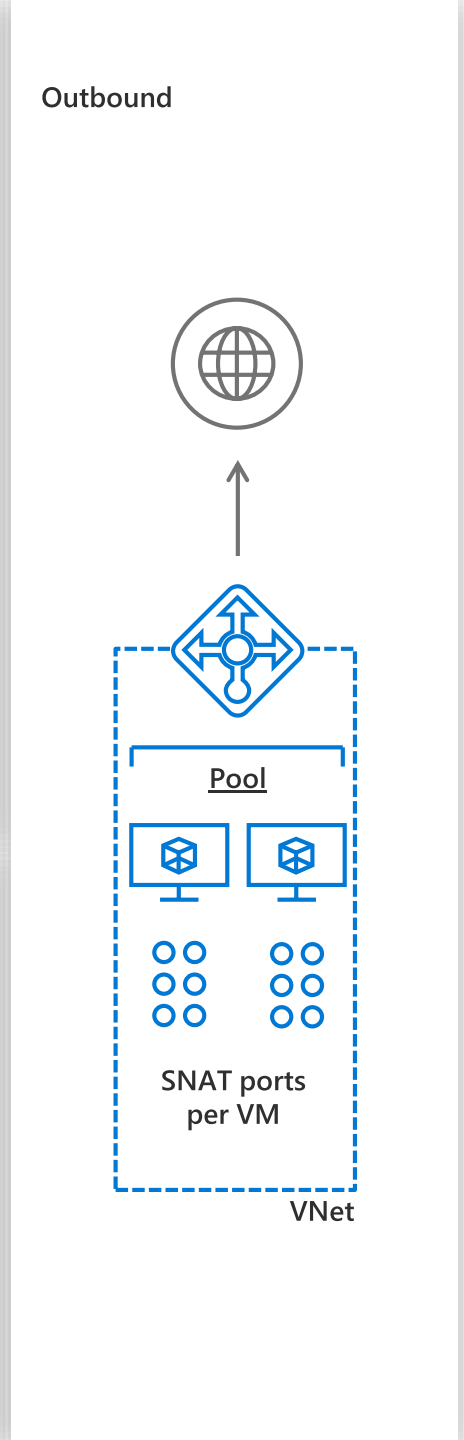
- Any VM in a VNet
- HA Ports for n-active resiliency
- Health probe for TCP, HTTP, and HTTPS

Metrics in Azure Monitor

- Multi-dimensional
- 3rd party integration







Azure load balancer

What's new

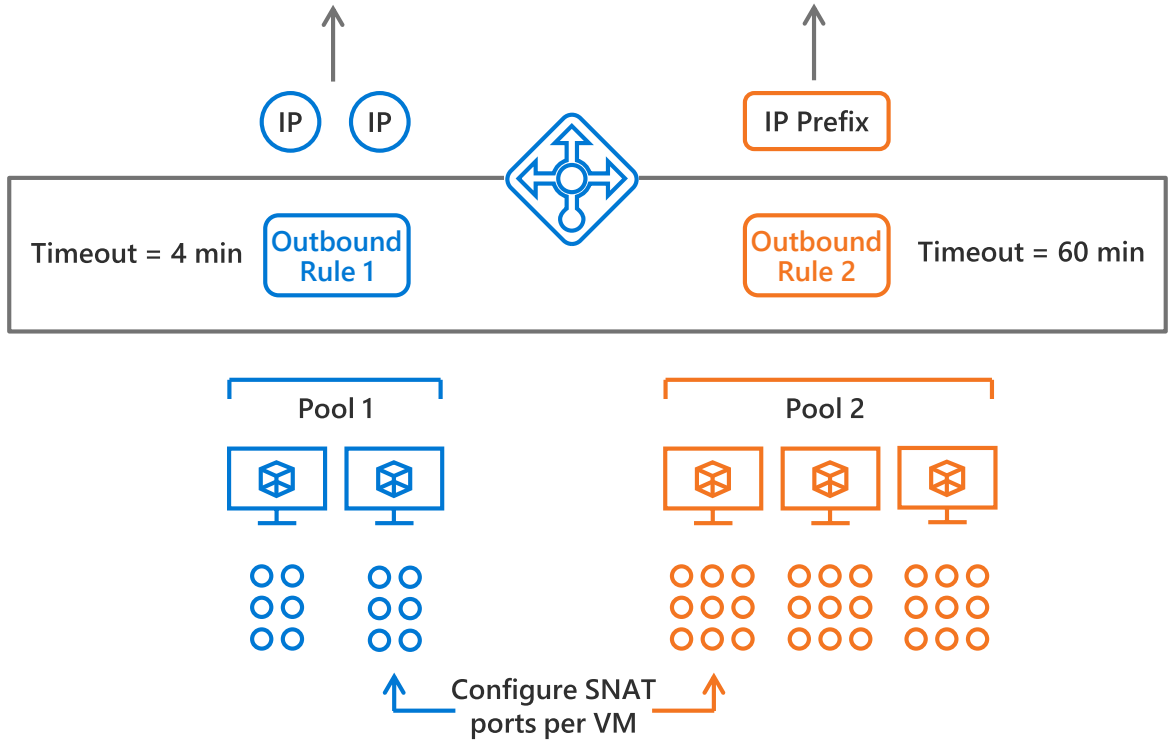
GA

Define, scale, and tune your outbound NAT configuration

Pool-based outbound NAT

- Declarative configuration
- Configure outbound idle timeout & TCP Reset
- Customer-defined SNAT port allocation

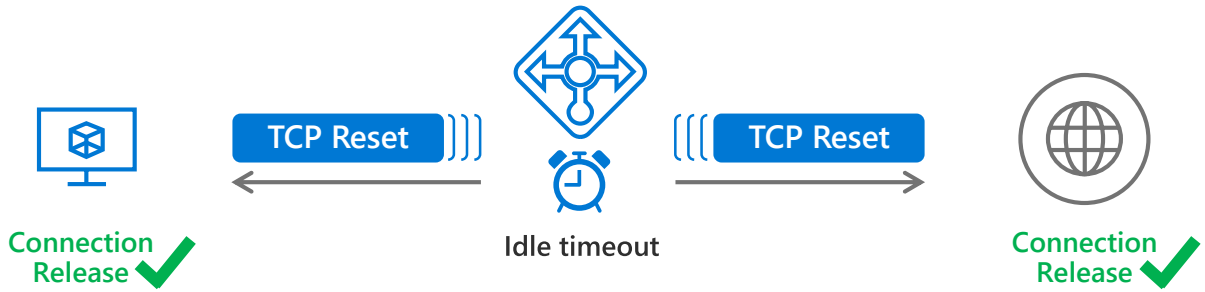
Simplify whitelisting with public IP prefix



Optimize application performance with clean connection releases

Preview

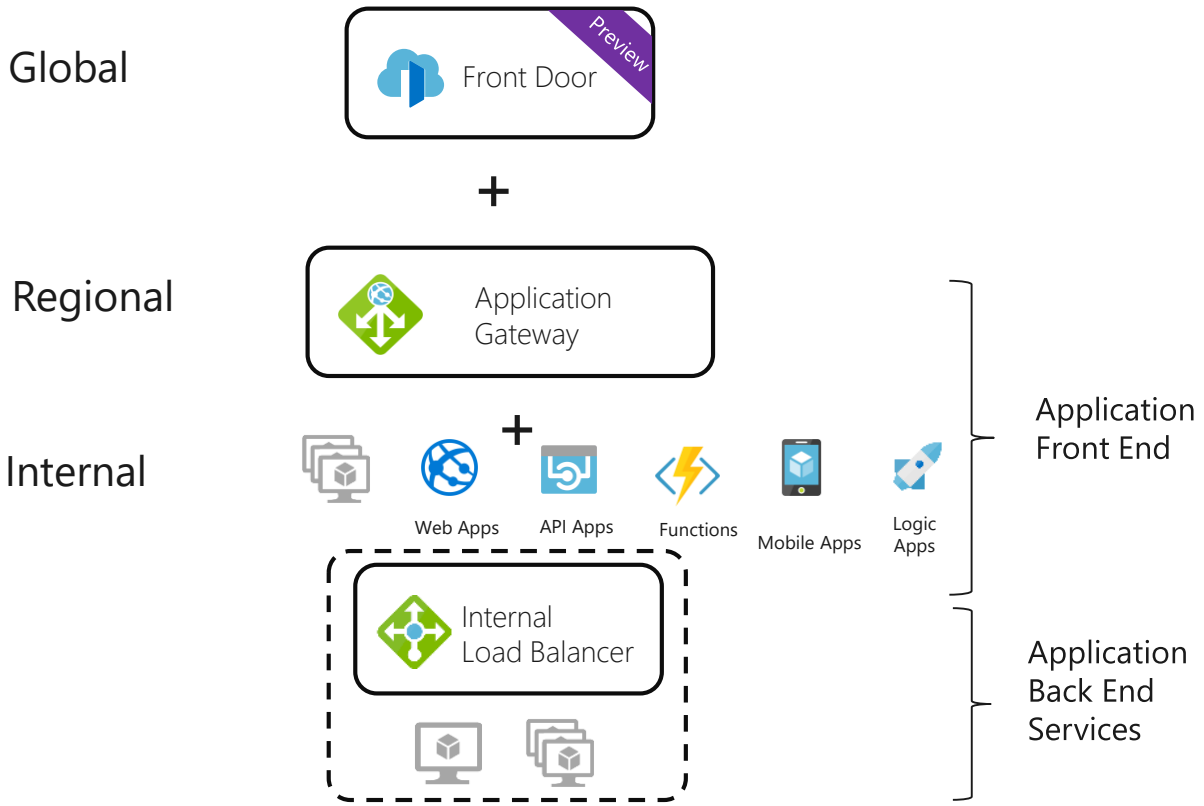
- No application changes required
- Instant release for both server and client
- Use on any rule



Building for global scale

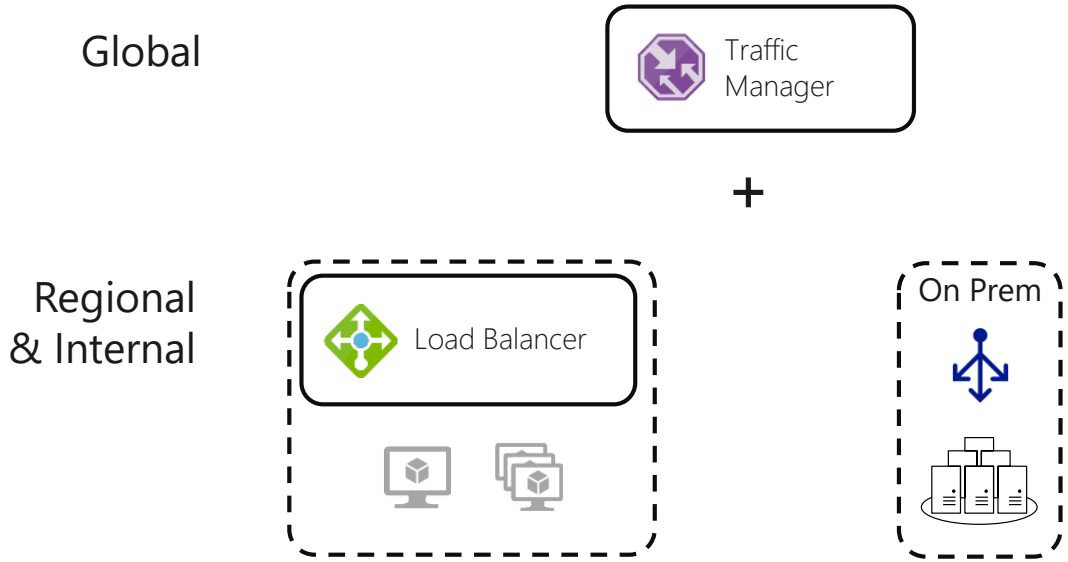
Web applications

Maximize global reliability and performance with cross-region and zonal redundancy.



Streaming, Gaming & Cross premises

Maximize availability of non http workloads globally OR migrate to the cloud across regional and on-prem resources for all protocols



Azure CDN

Microsoft's global multi-CDN ecosystem

Built-in multi-CDN

Choose from multiple top global CDN providers

verizon Akamai

CDN made simple

Few clicks to deploy, enable/disable on demand

Developer friendly

Use REST APIs, CLI, PowerShell to manage CDN

Deep integration

Automatically discovers other Azure services

Global scale

Easily handle traffic spikes and heavy load, supports IPv6

Integrated portal

Custom domain SSL, bring your own

GeekWire

"Our page load times are very low, and we're able to do it on a more powerful and scalable infrastructure that costs us 45 percent less."

Kevin Lisota, Geekwire

NBCSports

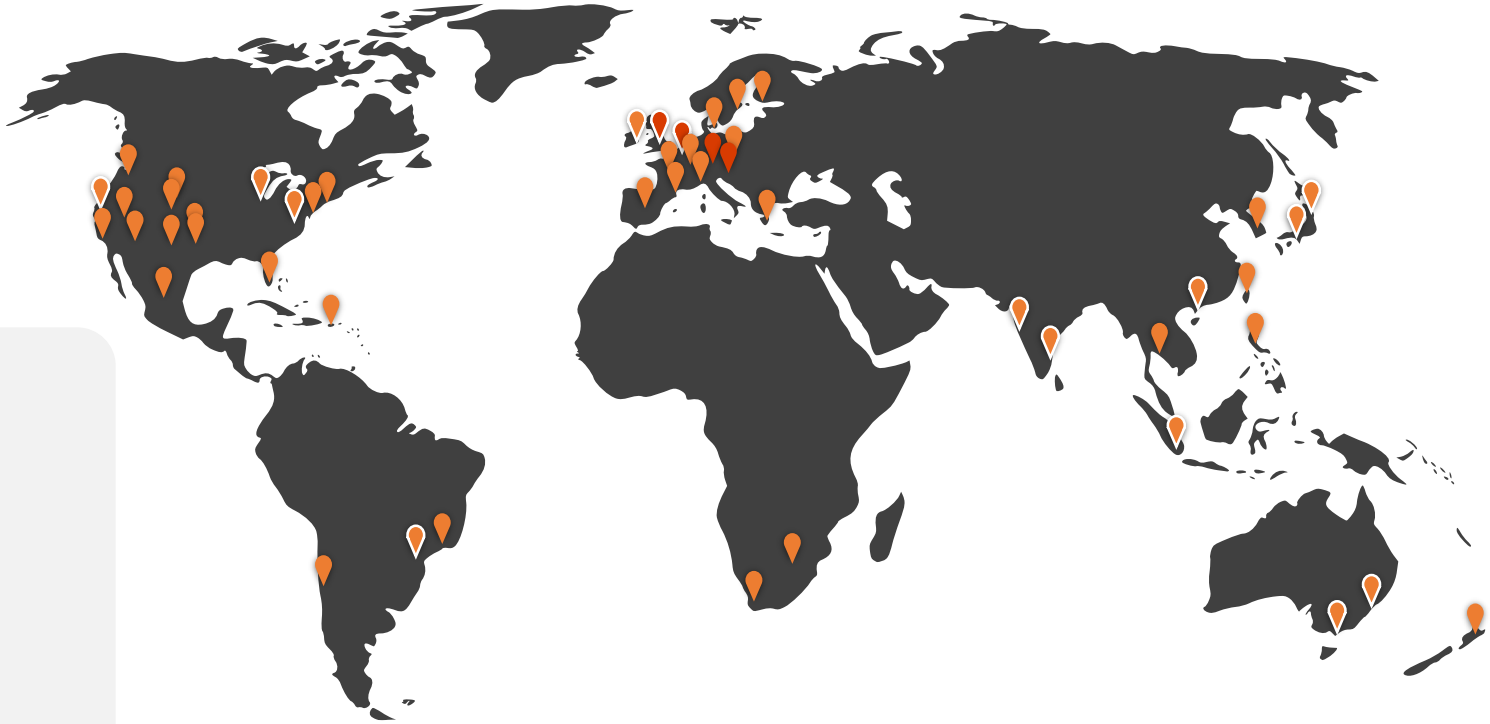
"Our partnership with Microsoft Azure was critical in extending our reach to more people and more devices via cloud streaming than ever before."

Eric Black, NBC Sports Group

Azure CDN

GA

Cloud native CDN offering giving access to Microsoft global WAN



Azure Key Vault for custom certificates

Adding to Azure CDN's choice of top CDNs

- Mix and match CDN infrastructures
- Increase global reach
- Redundant CDNs for your service

64 GLOBAL METROS
and growing!

36 COUNTRIES

130+ EDGE SITES

Azure DNS

Host DNS Zones with High Availability

100% Availability SLA

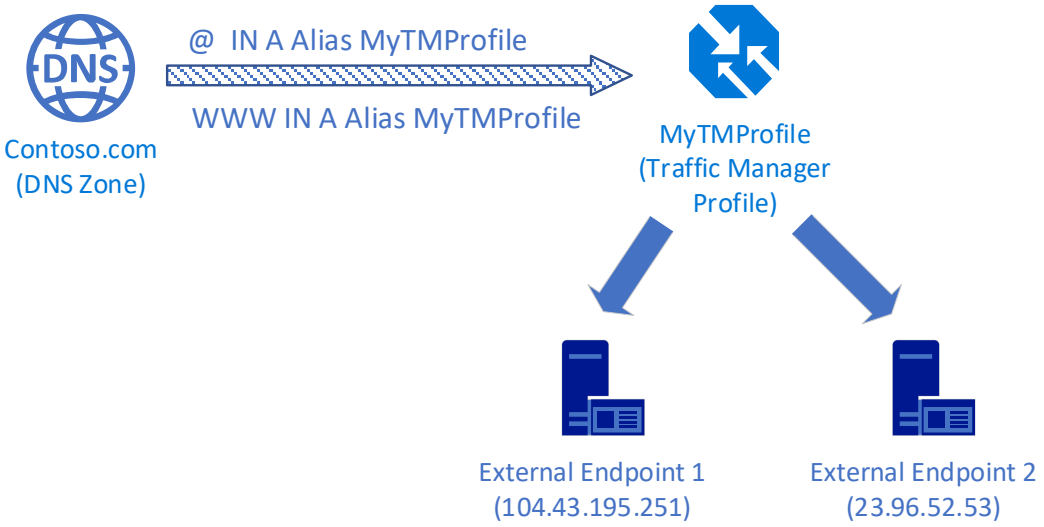
Our redundant data plane gives **100% reliability** for your DNS zones.

Reliability via Global anycast network

Multiple nodes around the world advertise a given IP address providing reliable responses even in event of a node failure.

Announcing DNS Alias records

- Keep your DNS records automatically updated when IPs change for your ARM resources.
- Dynamic, instantaneous updates to your DNS zone ensures zero downtime for your applications.
- Run a load balanced application directly at your Zone Apex by Alias to Traffic Manager, or any Public IP fronted service such as Application Gateway.



What we did today!

Business Problems Solved:

✓ Contoso's branch office Ops Personnel are connected to their Azure deployments.

✓ Contoso has a web site in Azure that is secure in a modern architecture.

You should now be better able to…

- discuss Azure Networking options in general
- describe how virtual networks can be used, including VNet Peering
- describe connectivity options from on-premises to Azure
- know how to implement and configure Azure Firewall
- understand and describe the three rule types associated with Azure Firewall
- understand how to monitor and track events on the Azure Firewall

Thanks!!!

Please fill out feedback/comments for this session, your feedback is how these workshops get better.