Microsoft

Mastering Azure networking concepts – ExpressRoute and Azure Firewall

Jon Ormond, Principal PM
Azure Networking

Session learning objectives

Business Problem:

- Contoso wants to host a web site in Azure but is concerned about security.

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

Azure PowerShell SDK - Az

- Azure PowerShell SDK Module - Az
  - Not compatible with the older AzureRM SDK (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

- AzureRM commands should work with `Enable-AzureRmAlias`

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

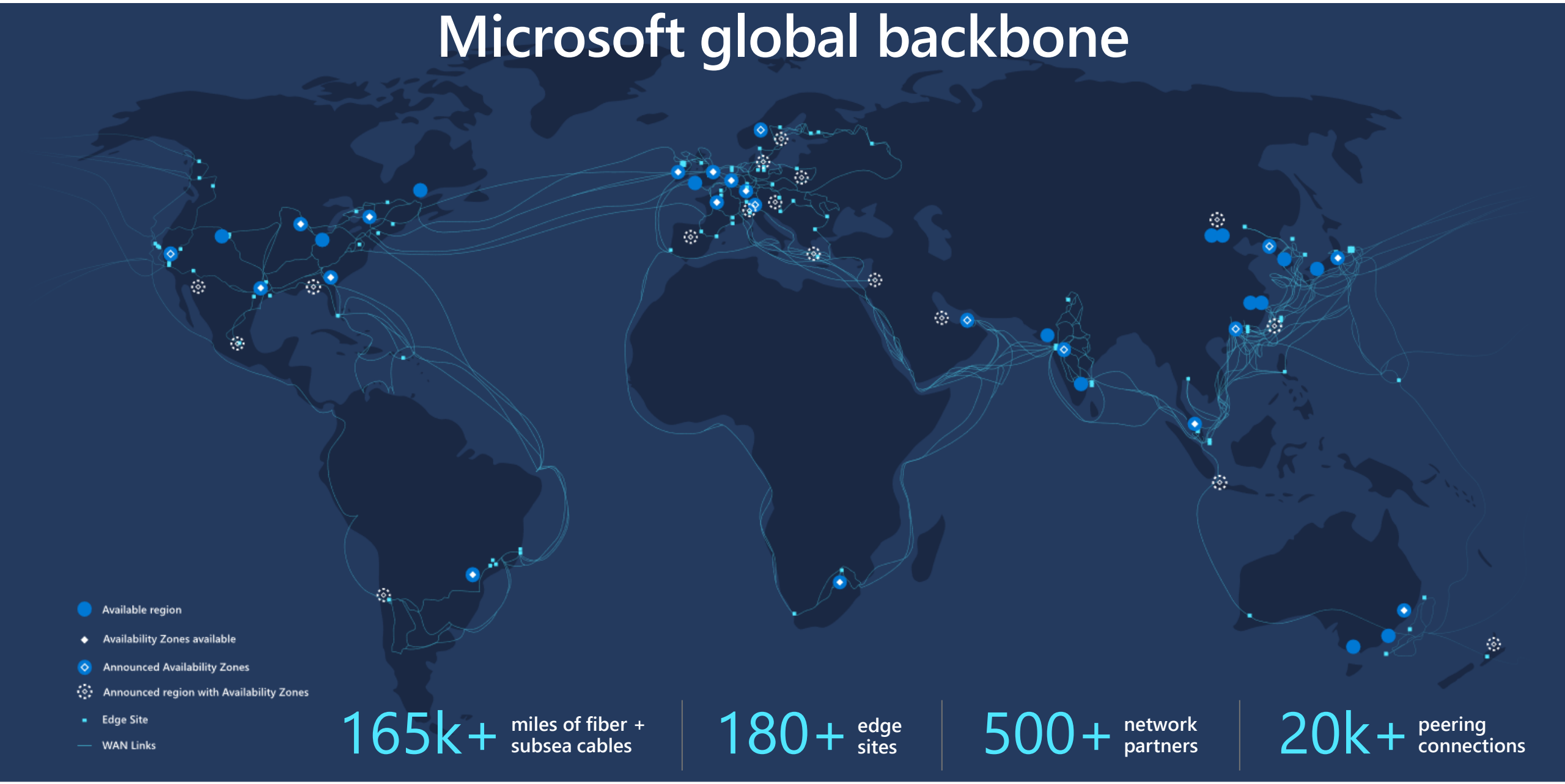
Idempotent PowerShell Operations

```
# 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’
       }
```

Microsoft Global Footprint

Microsoft global regions

Microsoft global backbone



Best performing cloud network

170+ Network POPs placed within 25 milliseconds from 85% of GDP

Once the traffic enters the Microsoft network, it stays on the network by default*

99.05% of Azure inter-region pairs beat the Internet*

*Claims based on the results from the ThousandEyes 2020 "Cloud Benchmark Performance" report. The findings are based on data gathered within and between multiple global regions of the five public cloud providers over a four-week period.

Zero Trust based network security

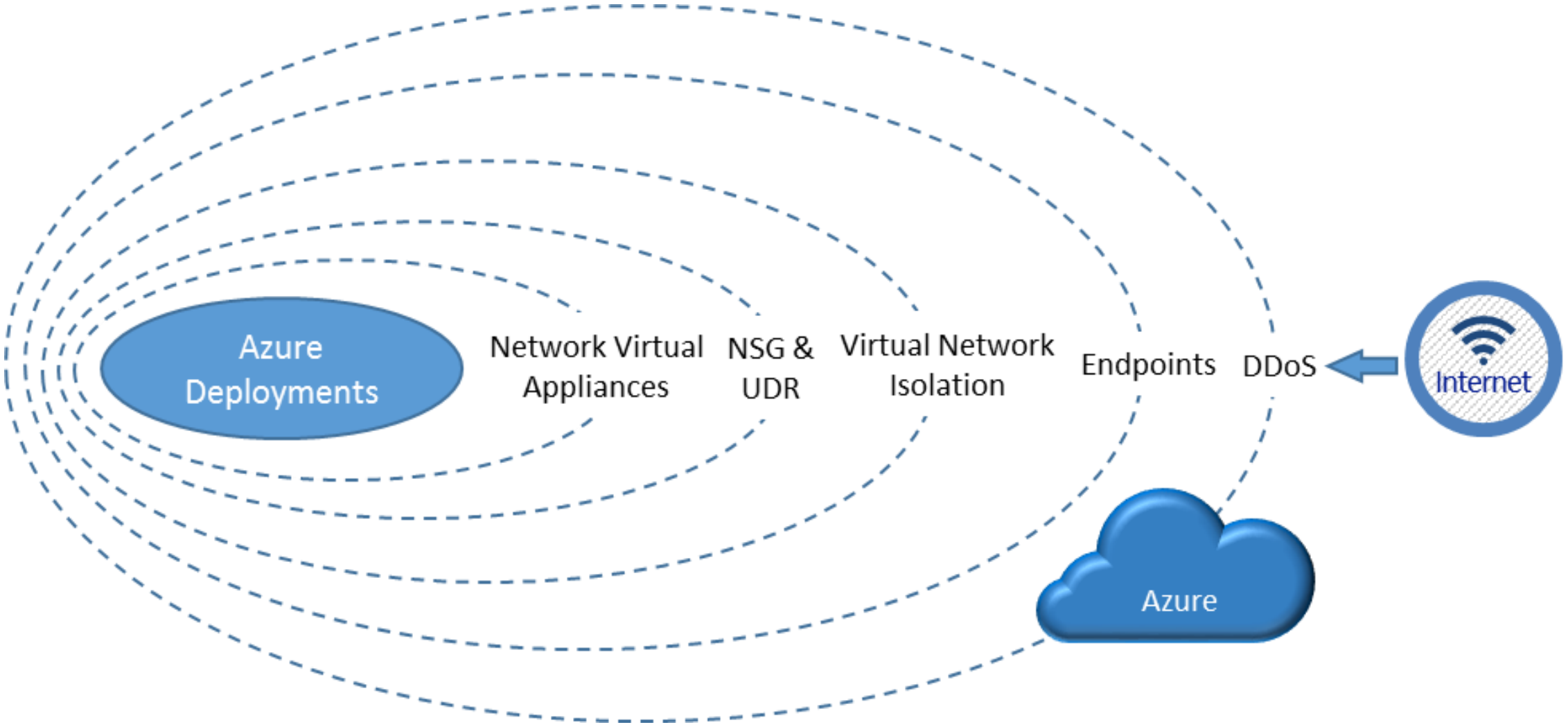
All Azure DC-DC traffic encrypted by default

A diverse set of network segmentation controls available to create isolated environments

Private and dedicated connectivity

Intelligent threat protection and secure app delivery

Visualizing layers of security



The Five Pillars of Azure Networking Services

Azure Networking Services

Secure network infrastructure

Build, protect, and monitor your network infrastructure

On-prem and branch connectivity

Connect on-premises datacenter and branches to the cloud

Remote work at scale

Enable remote users to access internal resources

Secure global app delivery

Build, secure, and deliver application to serve global user base

5G and edge computing

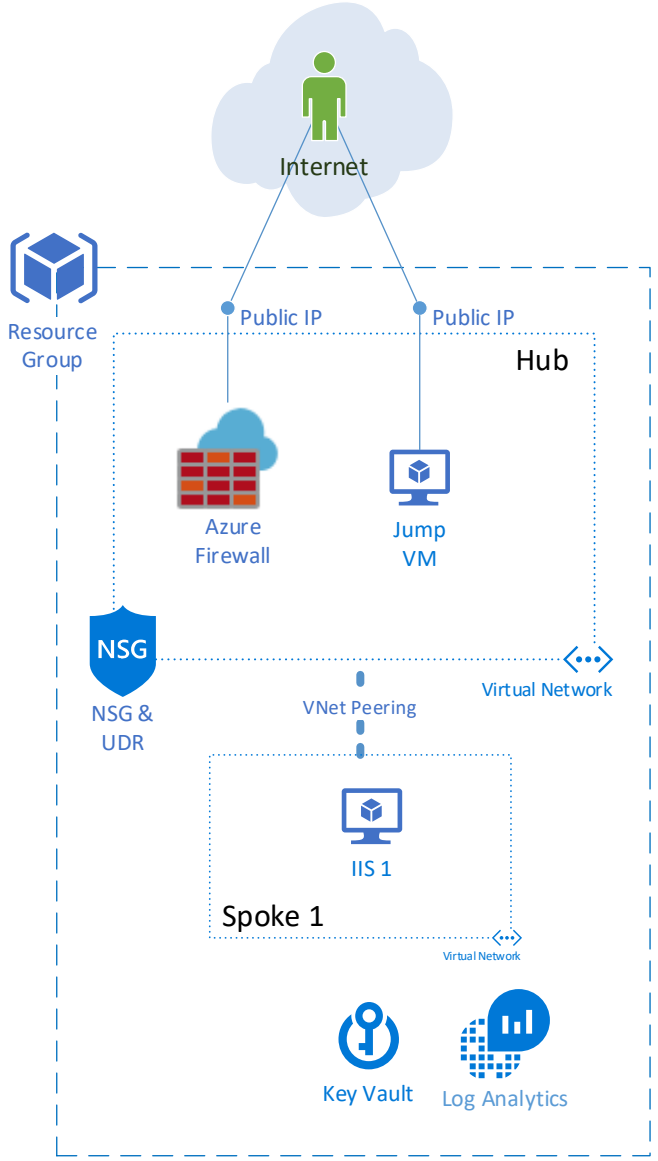
Enable edge computing platforms and apps

Workshop: Building the Environment

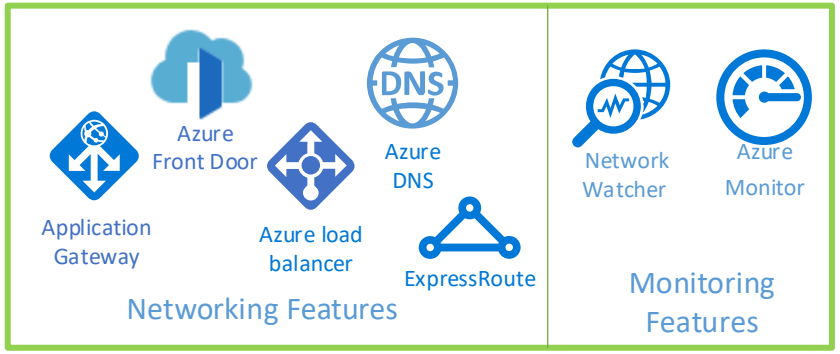
Final Environment

The resources in the blue Resource Group will be built by you today in the workshop

The green box resources won't be built but will be discussed in this deck

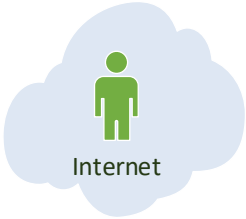


Features to be built



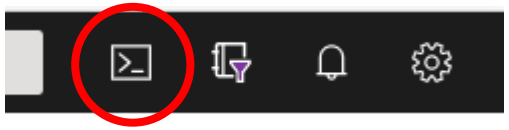
Features to be discussed

Step 0 – Initialize Cloud Shell

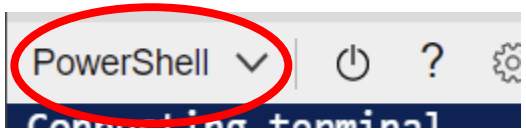


Execution:

1. Connect to the internet
2. Login to https://portal.azure.com
3. Start Cloud Shell (select or create a storage account if prompted)



4. Ensure Cloud Shell is set to PowerShell



5. In the cloud shell run

```
Connect-AzAccount -UseDeviceAuthentication
```

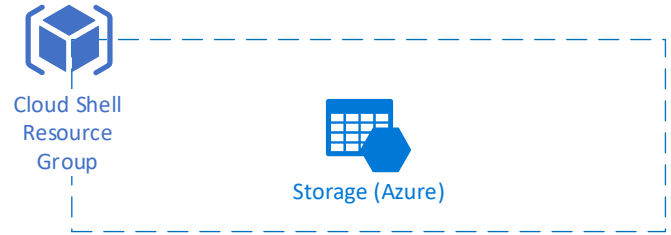
and follow the instructions. Login using your Azure Portal credentials

6. In Cloud Shell run the following to download the workshop files

```
(IWR aka.ms/1).Content | IEX
```

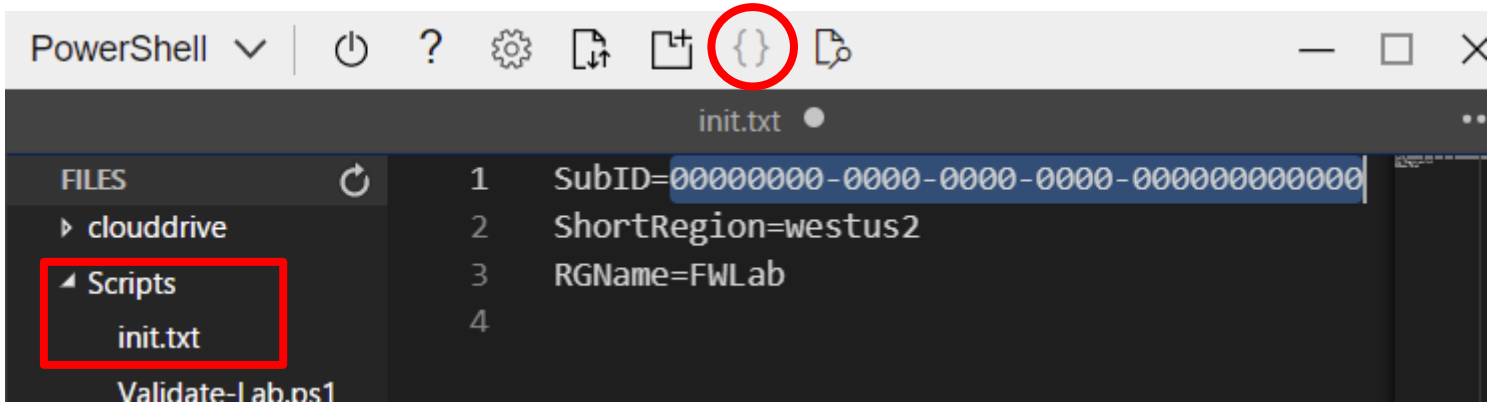
A warning about the subscription ID will be shown, we'll fix this next

NOTE: The Cloud Shell is where all workshop PowerShell scripts should be deployed.



Step 0 (cont) – Update init.txt

All scripts pull critical information from the init.txt file, so it's important to update this file to reflect the resource group name and subscription you'll be using for this deployment of the firewall workshop.

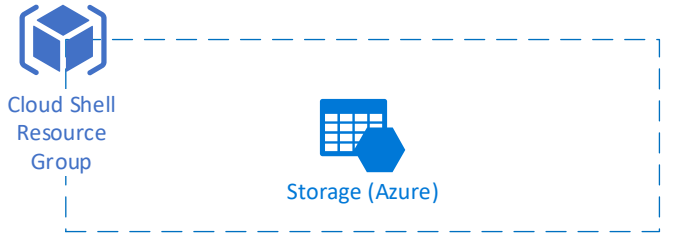


Execution:

1. Open the Cloud Shell editor (red circled icon)
2. Navigate to init.txt (red boxed item in file hierarchy)
3. In the right-hand pane, update the Subscription ID to your Subscription ID and optionally the RGName to use the resource group name you wish to use inside your subscription.
4. Once updated, press CTRL+S to save the init.txt file.
5. Rerun the validation script, ensuring no errors and that the File Variables are as intended.

```
./Scripts/Validate-Lab.ps1
```

NOTE: In the init.txt file there must be no quotes or spaces



Step 1

Execution:

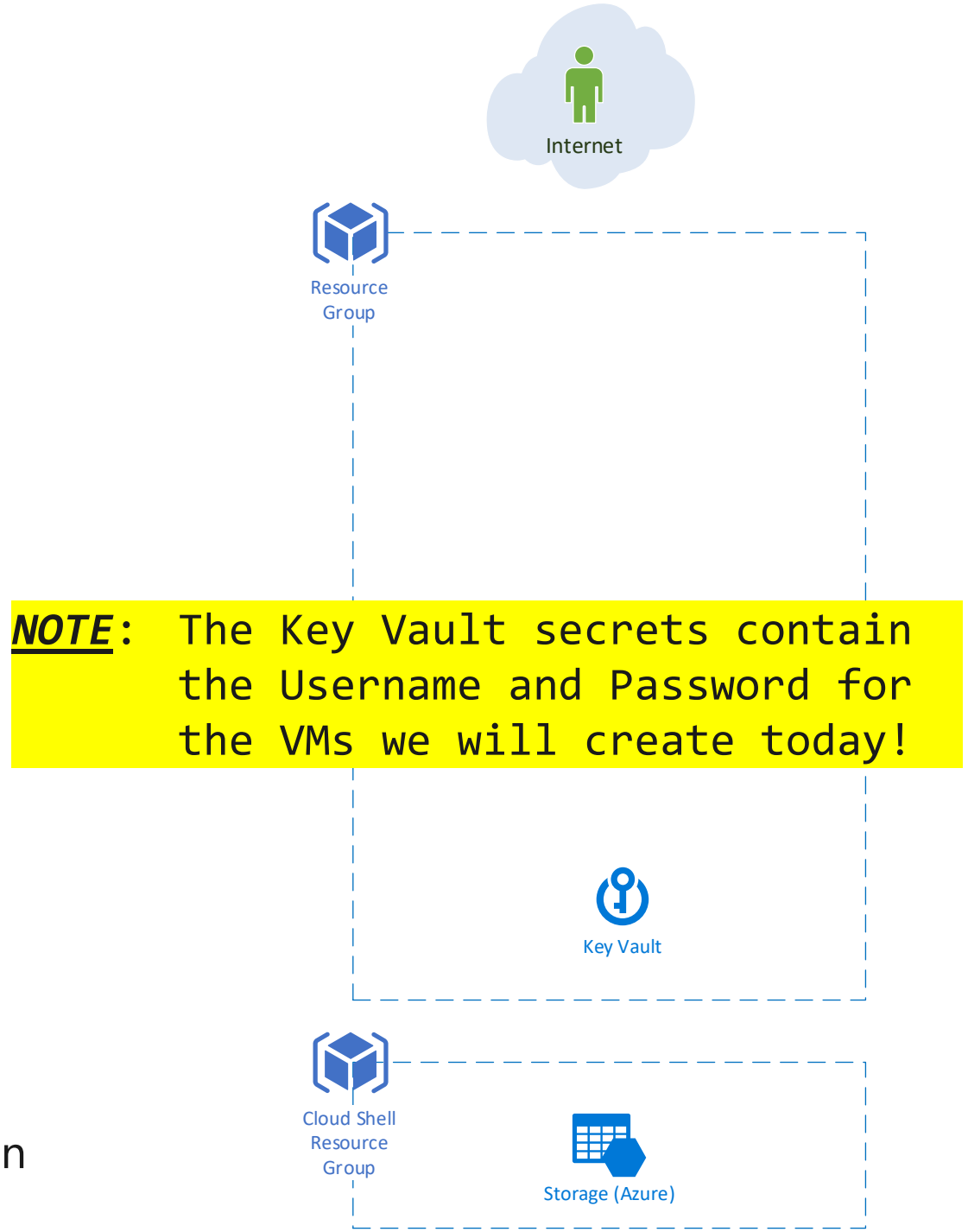
1. Change to the Scripts folder
   ```
   cd Scripts
   ```
2. (Optional) in the editor pane you can select and view the script before running
3. Run step 1 with the following:
   ```
   ./WorkshopStep1.ps1
   ```

Validation:

1. Browse to your Resource Group in the Portal
2. You should see a Key Vault resource
3. Explore the Key Vault, and the secrets therein

Take Away:

You now have a Resource Group in Azure to which you can now deploy resources!



Secure network infrastructure

- Azure Virtual Network
- Azure Virtual Network NAT
- Azure Private Link
- Azure DNS
- Azure Firewall
- Azure Firewall Manager
- Azure DDoS Protection
- Azure Bastion
- Network Watcher
- Azure Monitoring

Virtual Networks

Your virtual private network in the cloud

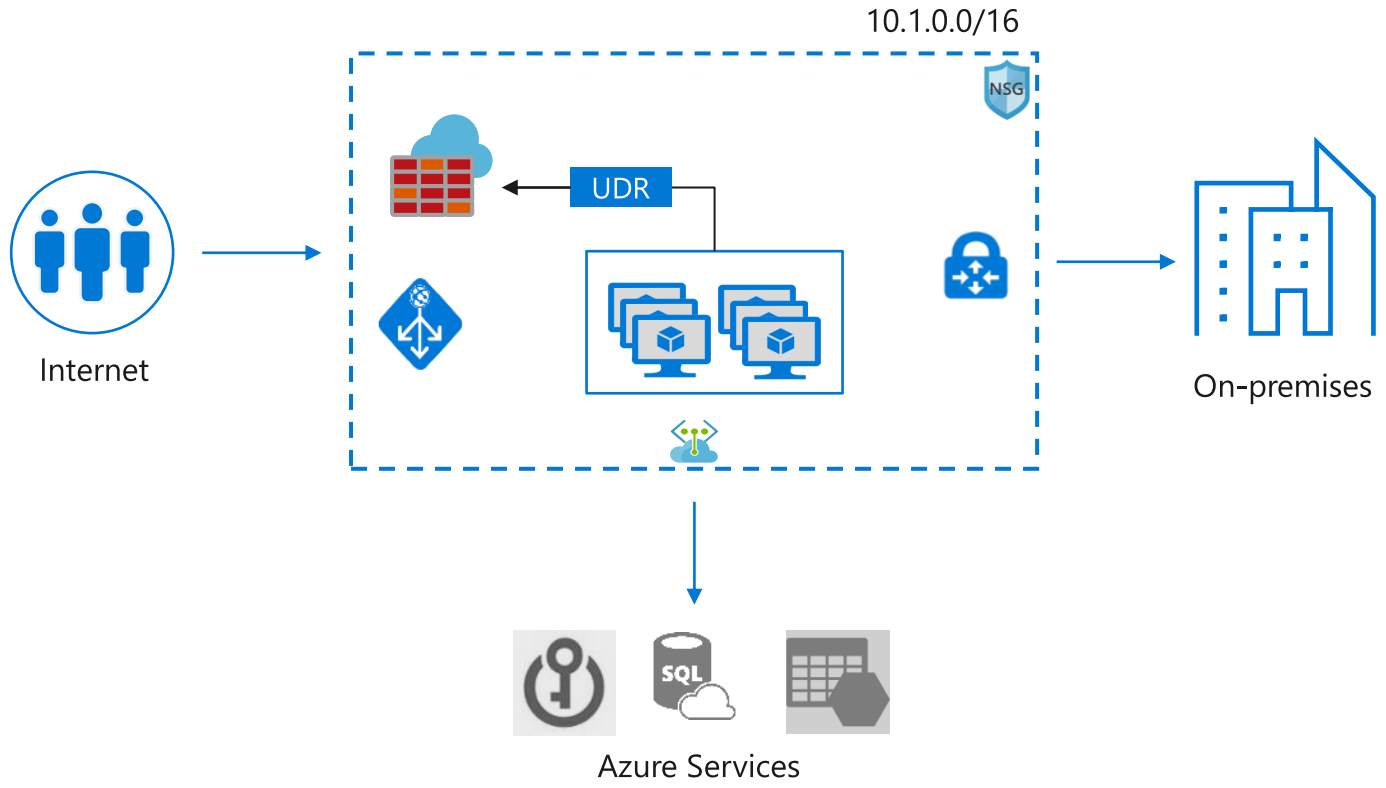
Private isolated logical network

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

Azure Virtual Network

Customer's Private Network in The cloud

Azure Private Link

Azure services made available inside customer's Virtual Network

In-built protection against data exfiltration from the network

Extends to customer's own services

36 Azure services now available over Private Link

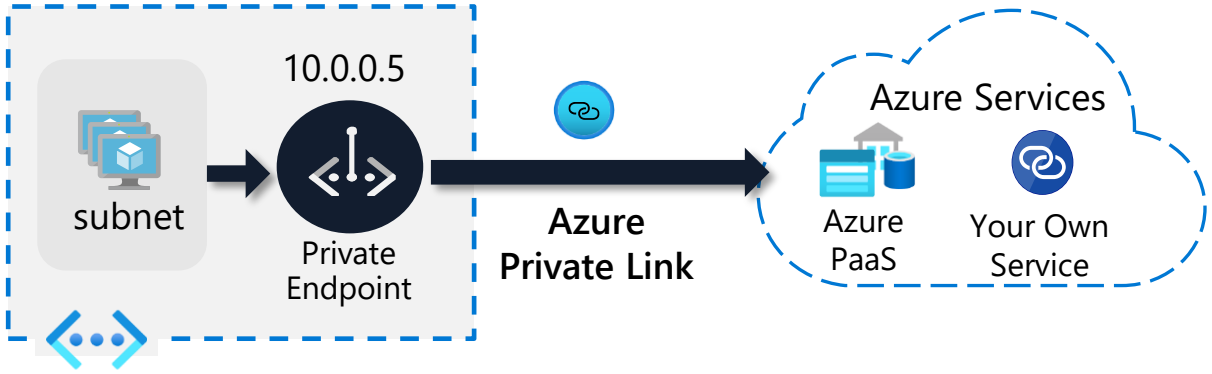
Azure Virtual Network NAT

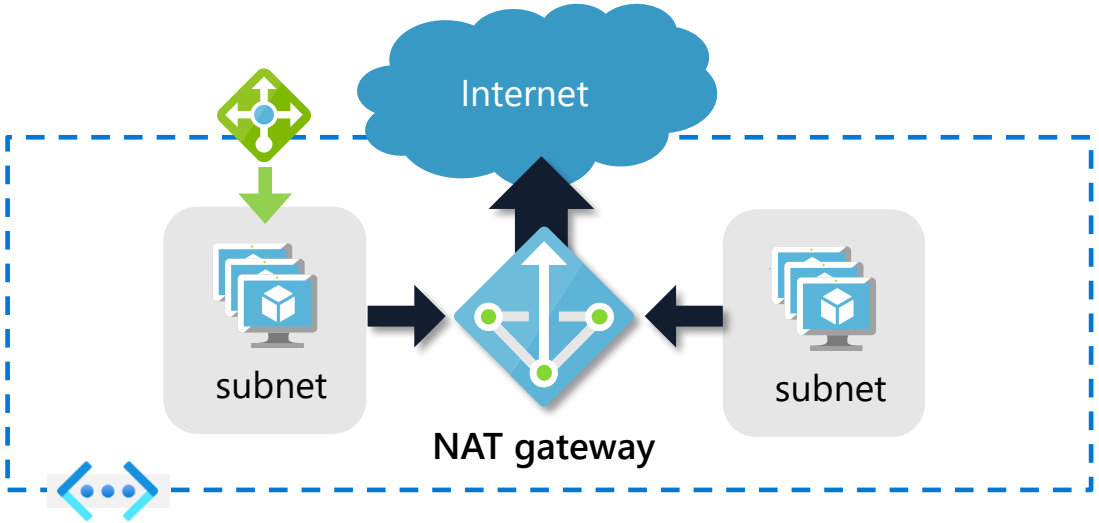
Fully managed and highly available service for Internet access from Virtual Network

Configurable at subnet level

Built-in auto scale with support for IP prefixes

Easy whitelisting with Static IP Address





Step 2

Execution:

1. In the Scripts folder run
   `./WorkshopStep2.ps1`
2. (Optional) in the editor pane you can select and view the script before running

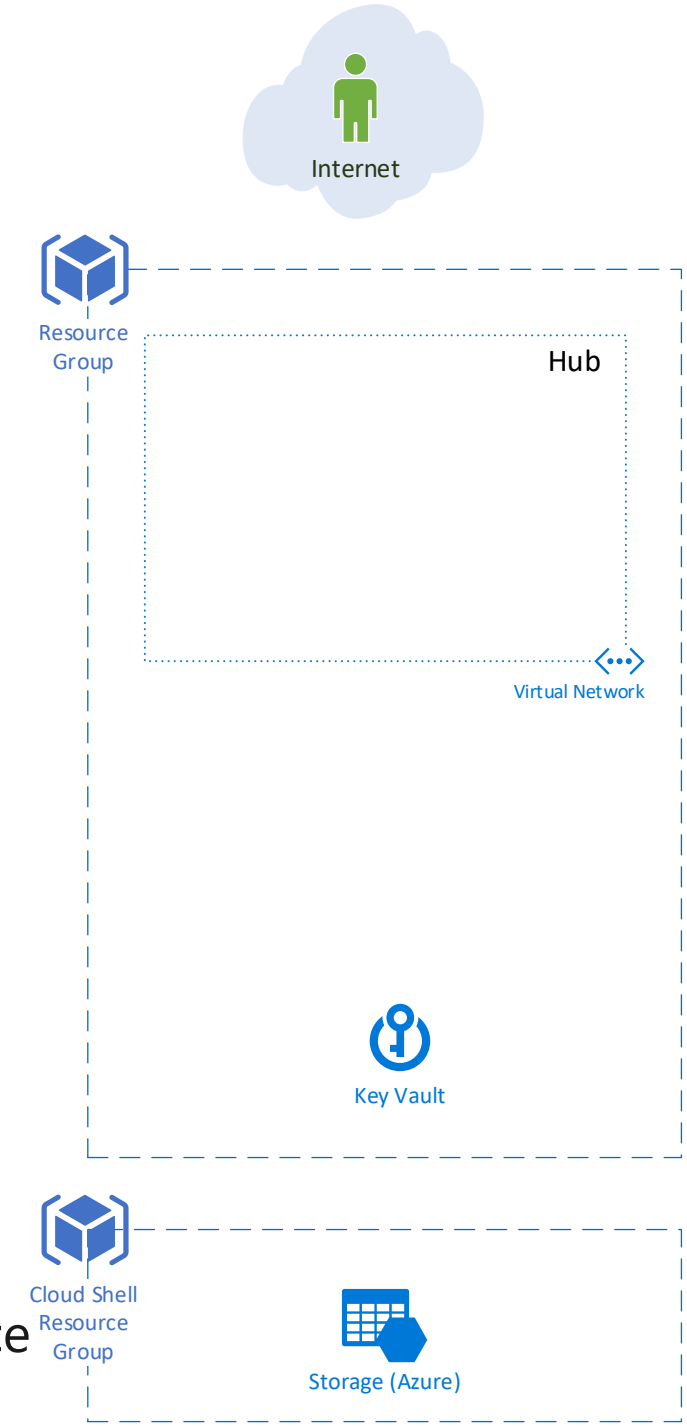
> ***NOTE*:** You may see “warnings” from PowerShell about upcoming changes. These warnings do not affect running of the scripts.

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 resource



Step 3

Execution:

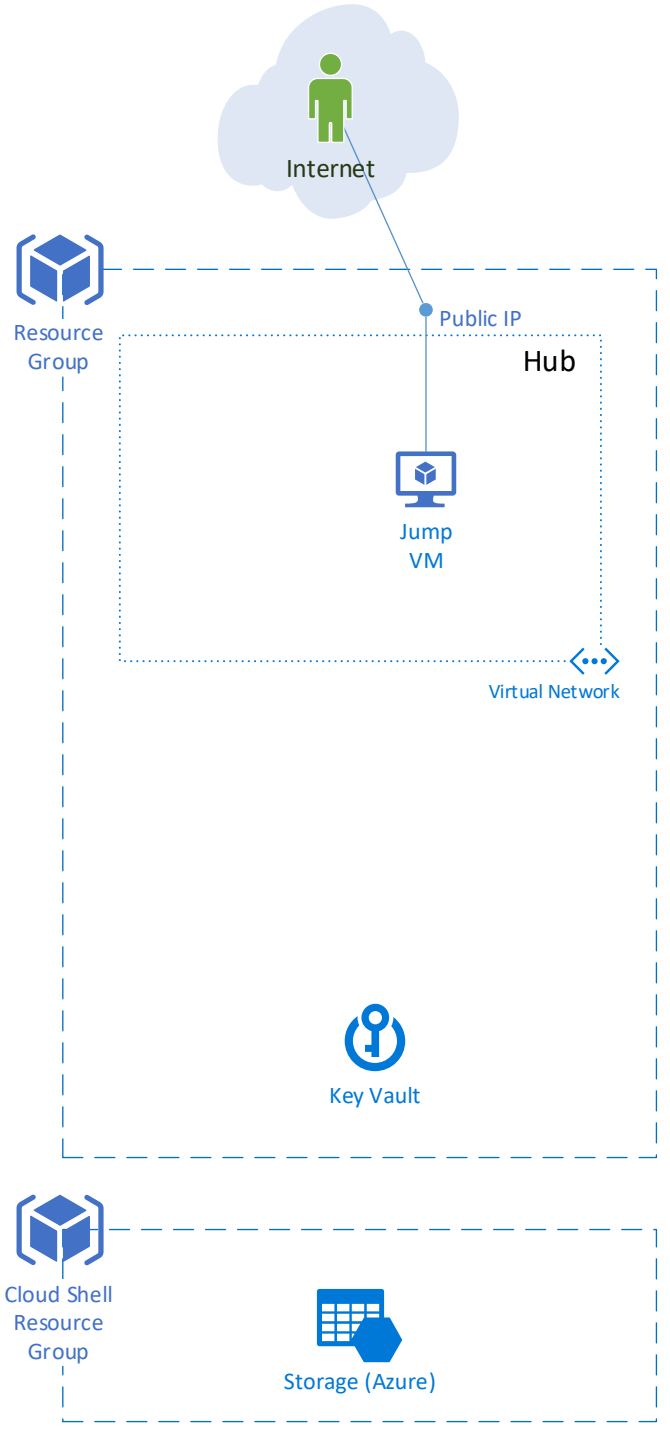
1. In the Scripts folder run
   `./WorkshopStep3.ps1`
2. (Optional) in the editor pane you can select and view the script before running

Validation:

1. Review the VM components
2. (optional) RDP to the VM's Public IP using the User01 password from the Key Vault secret

Take Away:

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



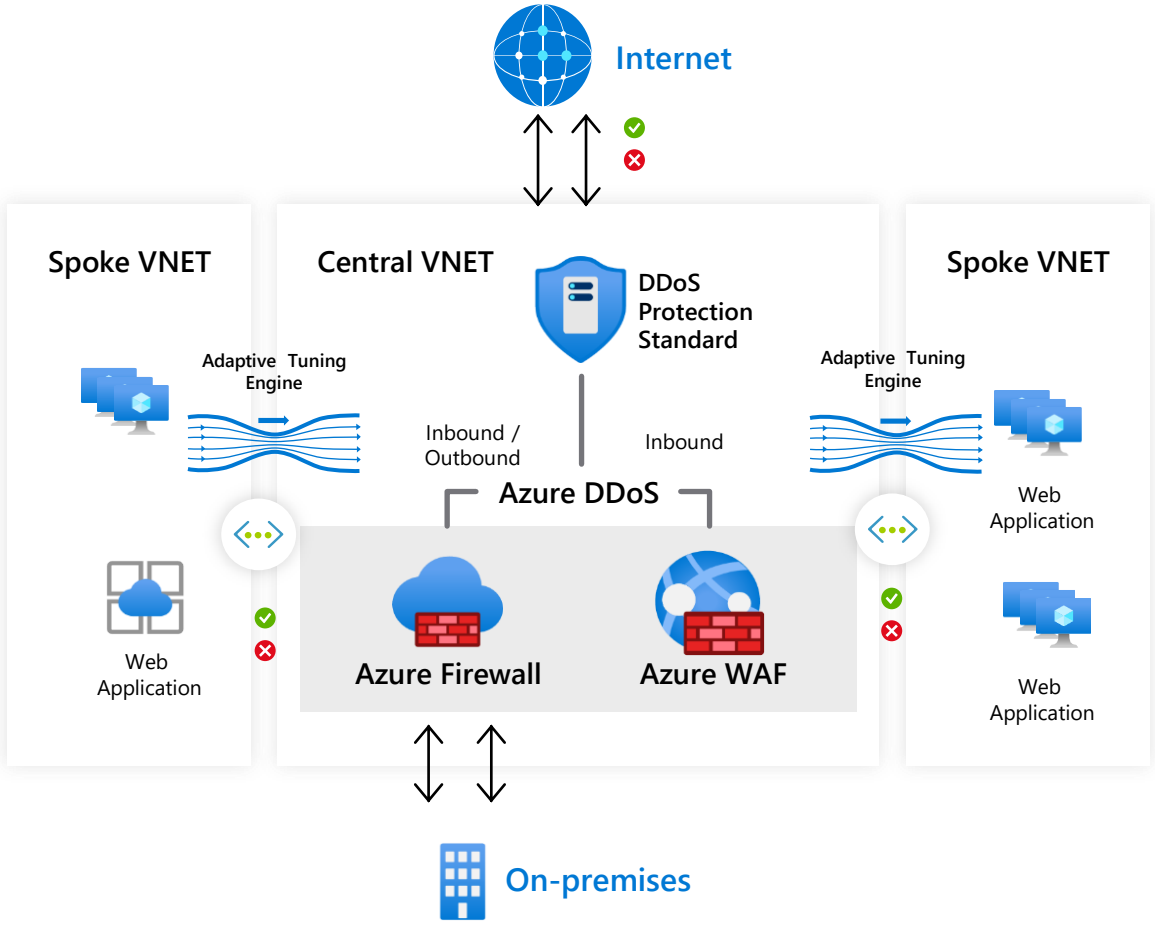
Azure Firewall, DDoS

Azure Firewall

- Cloud native network security to protect networks, and resources
- Central governance of all traffic flows
- SQL filtering, IP Groups, Auto SNAT, Forced Tunneling
- DNS proxy, custom DNS, FQDN filtering in network rules (all ports/protocols)

Azure DDoS

- Cloud scale DDoS protection for Azure resources
- Global shared mitigation capacity increased to 45 Tbps



Azure Bastion

Secure and seamless RDP and SSH access to your virtual machines without public IP address

Access to Azure VMs in peered VNet in same subscription

Access to on-premises VMs via VM's IP address or DNS hostname

Feature announcements

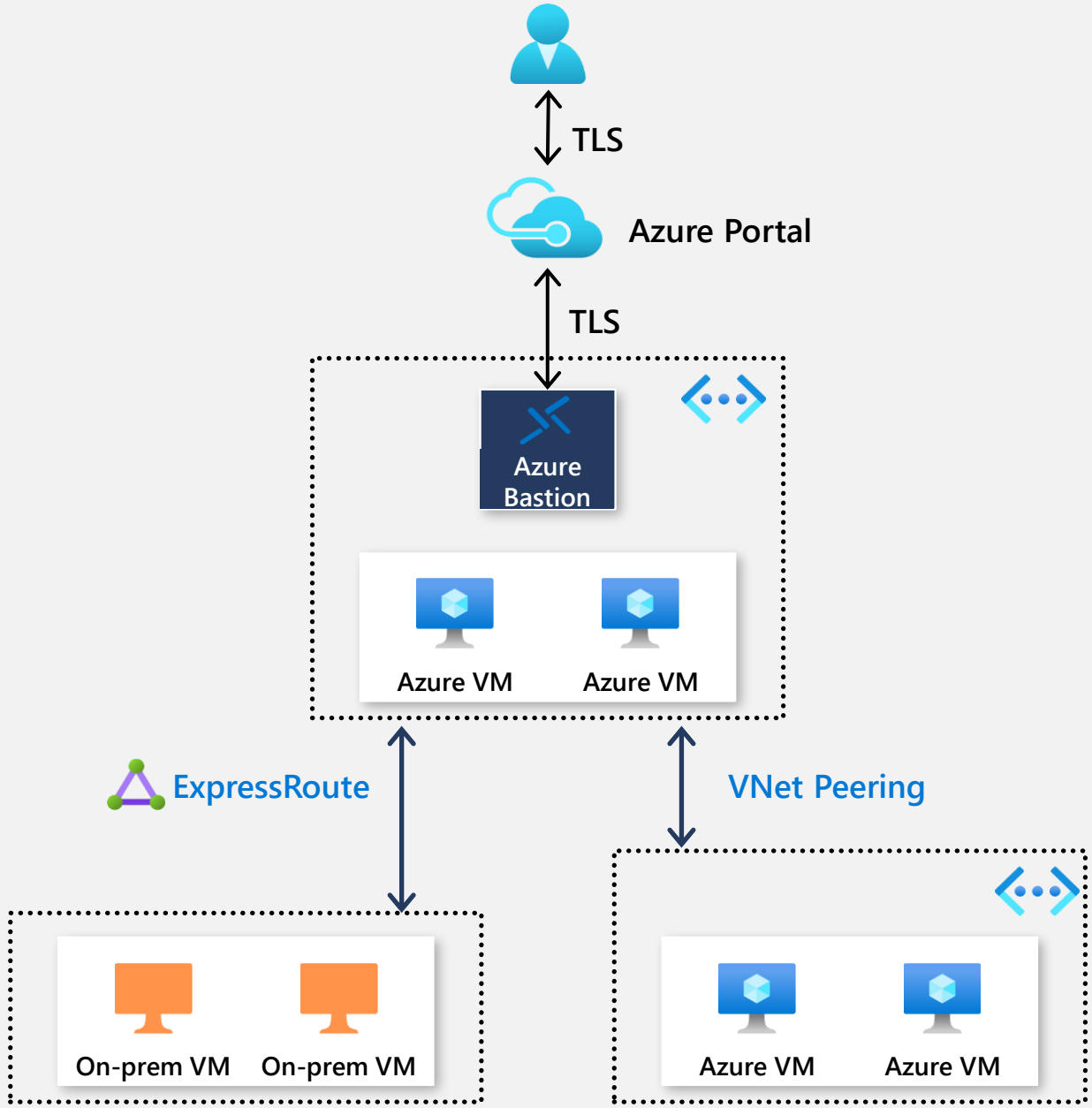
Azure Key Vault Integration (GA)

RDP/SSH access to AKS nodes (GA)

Bastion Health metrics (Public preview)
Session | CPU | Memory

Bastion Scalable Gateway (Coming mid 2021)
Support as many as 500 concurrent sessions

Ability to decrease the gateway size



Monitoring

Simplified and centralized network monitoring

Azure Monitor for Networks

Single health, metric, alert and diagnostic console for all network resources across your subscriptions

On by default

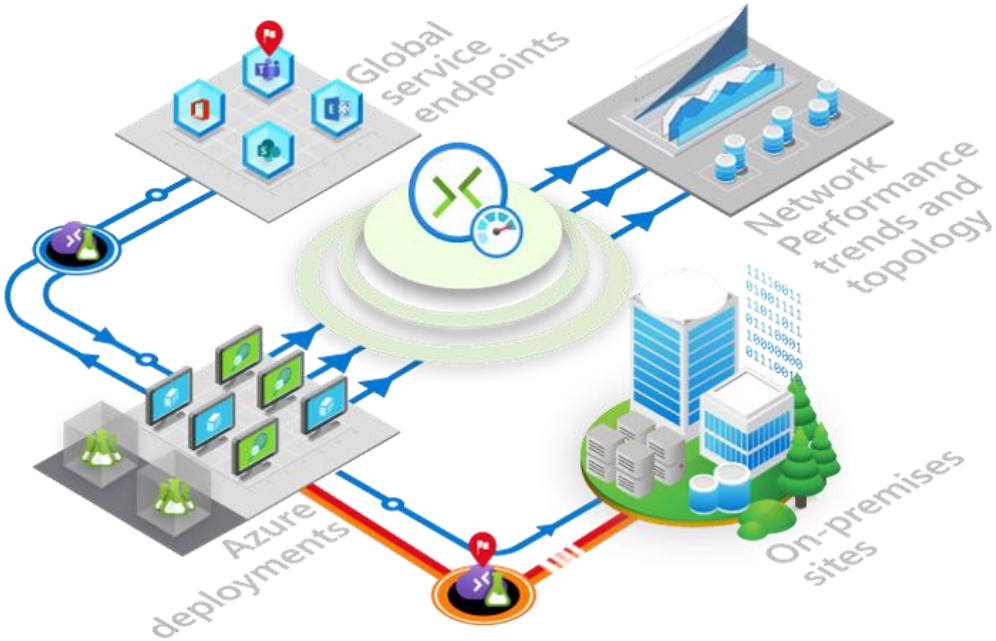
Connectivity, traffic and diagnostic features seamlessly integrated

Connection Monitor

Monitor endpoints within and across Azure regions, on-prem sites and global service locations

Visualize end-to-end network topology, loss and latency across on-prem and Azure locations

Mitigate connectivity issues faster with metric-based alerts and built-in diagnostics



Step 4

Execution:

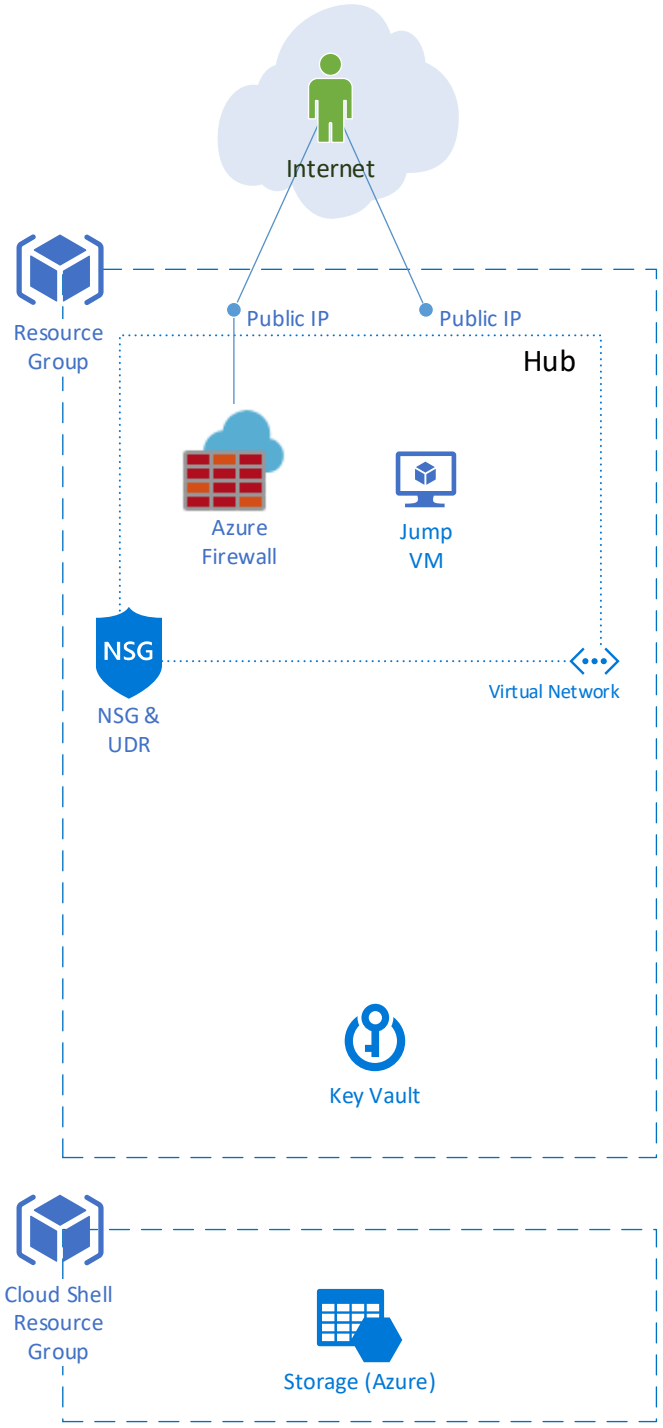
1. In the Scripts folder run
   `./WorkshopStep4.ps1`
2. (Optional) in the editor pane you can select and view the script before running

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 5

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

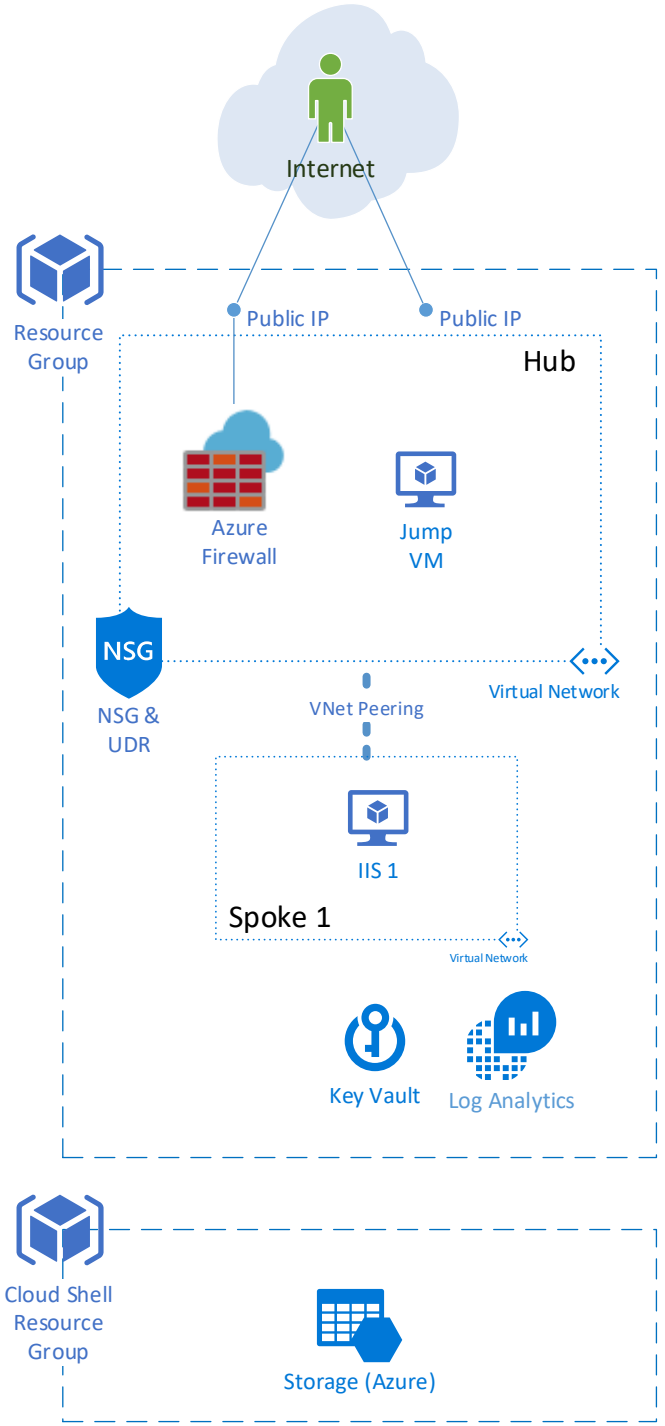
Execution:

1. In the Scripts folder run `./WorkshopStep5.ps1`
2. (Optional) in the editor pane you can select and view the script before running

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. (optional challenge) Add a Firewall rule to allow RDP to the Jump box. Then RDP to the Jump VM and hit the private IP of the IIS server (the firewall network rules should allow the page to be visible)

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



On-prem and branch connectivity

Azure ExpressRoute

Azure VPN Gateway

Azure Virtual WAN

Azure Route Server

Azure Peering Service

Azure routing preference

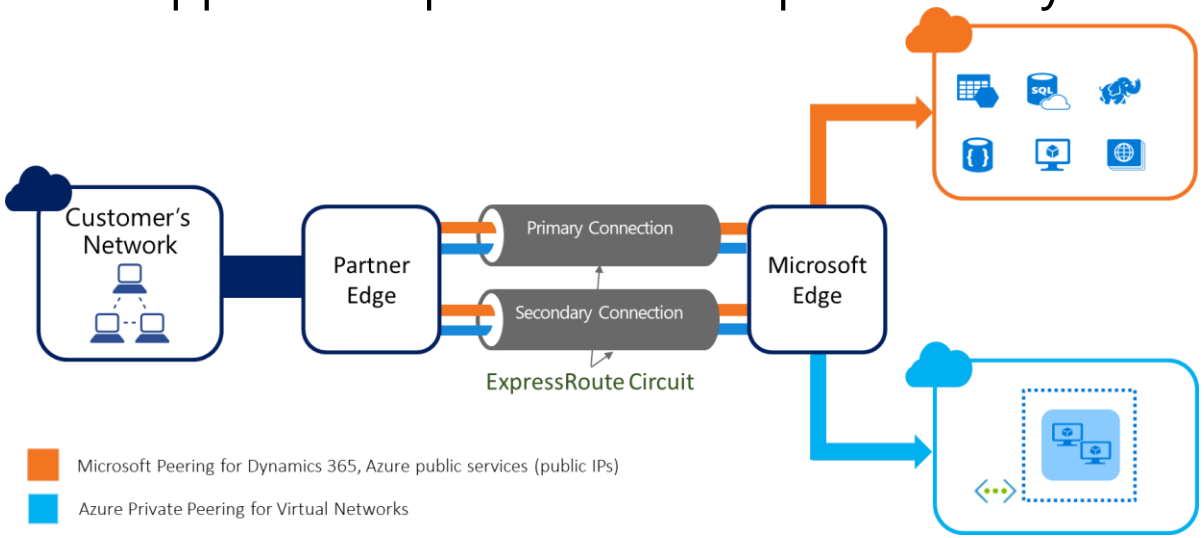
Azure Orbital

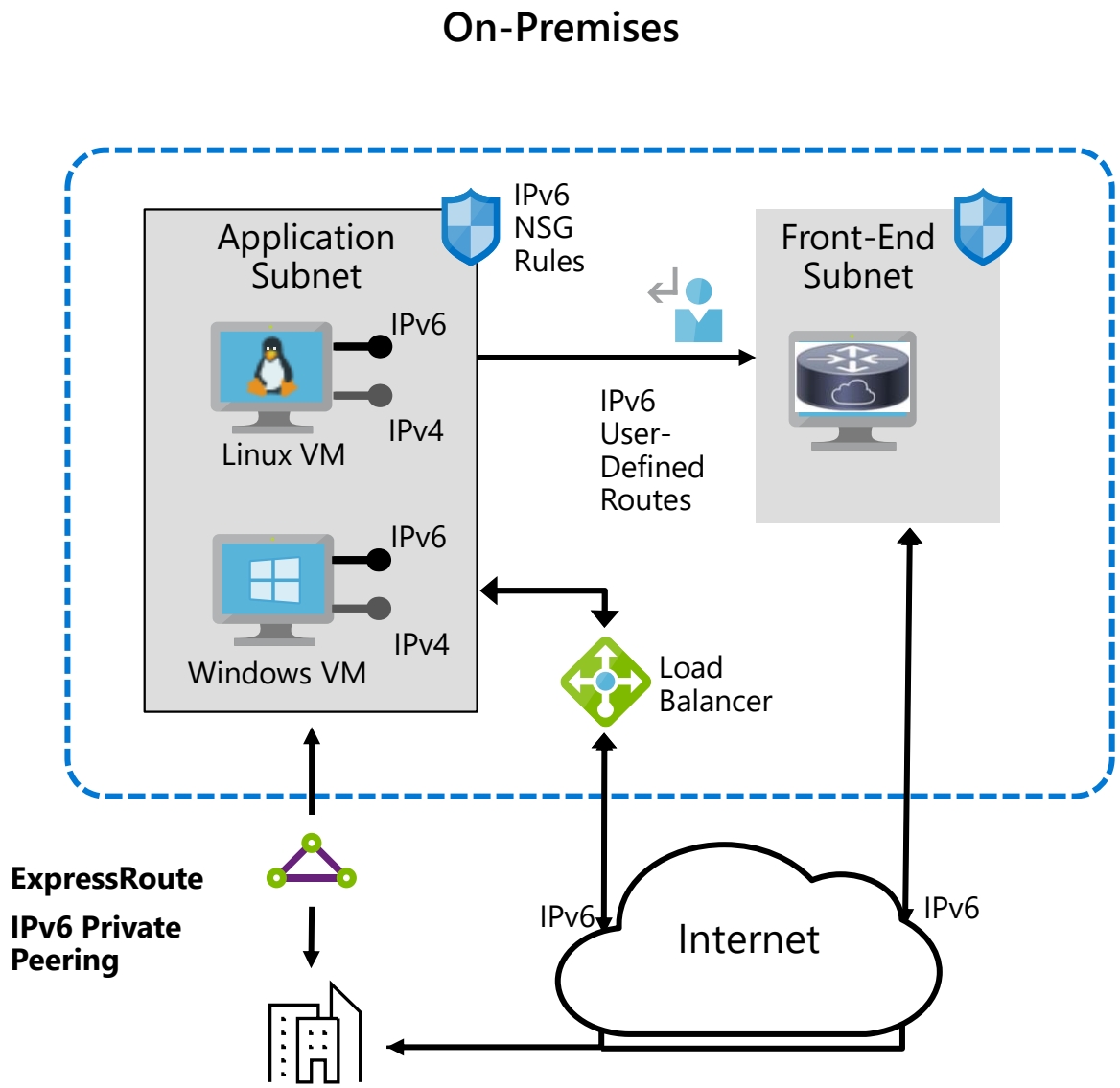
ExpressRoute

Private connectivity to Microsoft

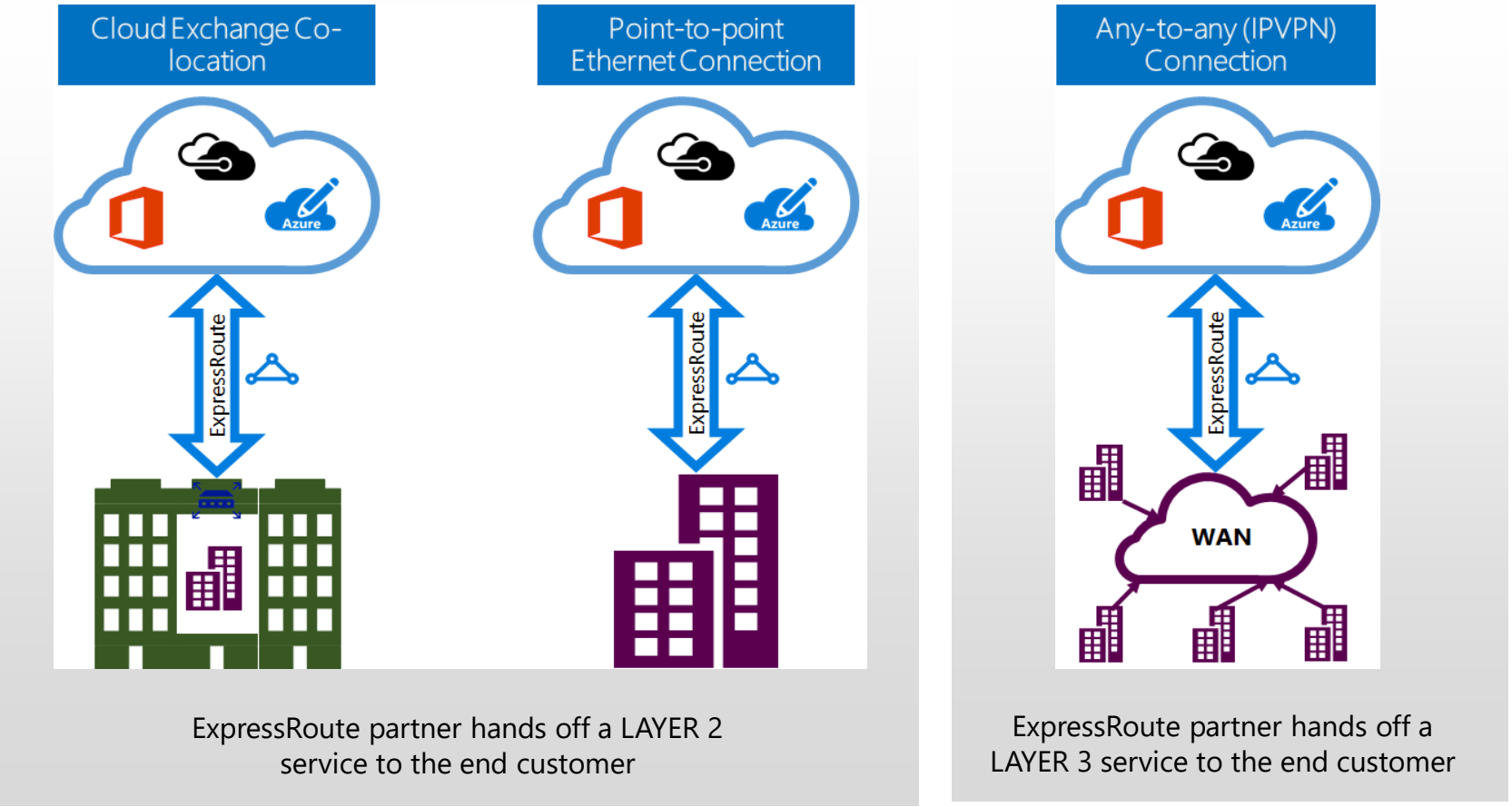
ER Gateway metrics: packets per second and CPU utilization, with native alerting via Azure Monitor

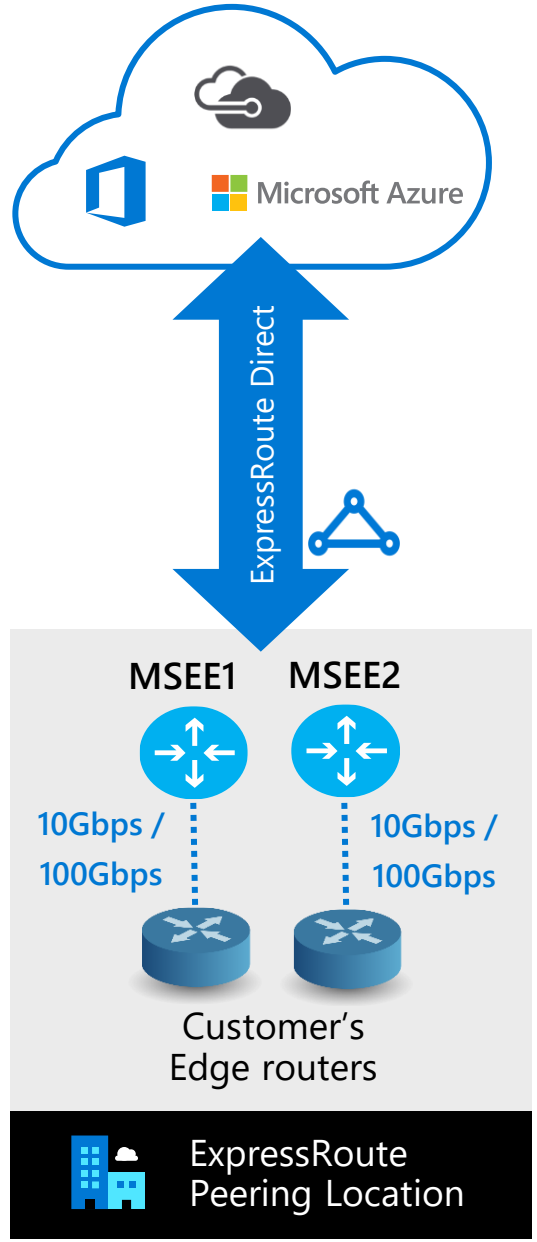
Support for up to 16 circuits per Gateway





ExpressRoute Connectivity Models





Service Provider Model

Azure Virtual WAN

Unified and ubiquitous connectivity, routing and security

Transit connectivity

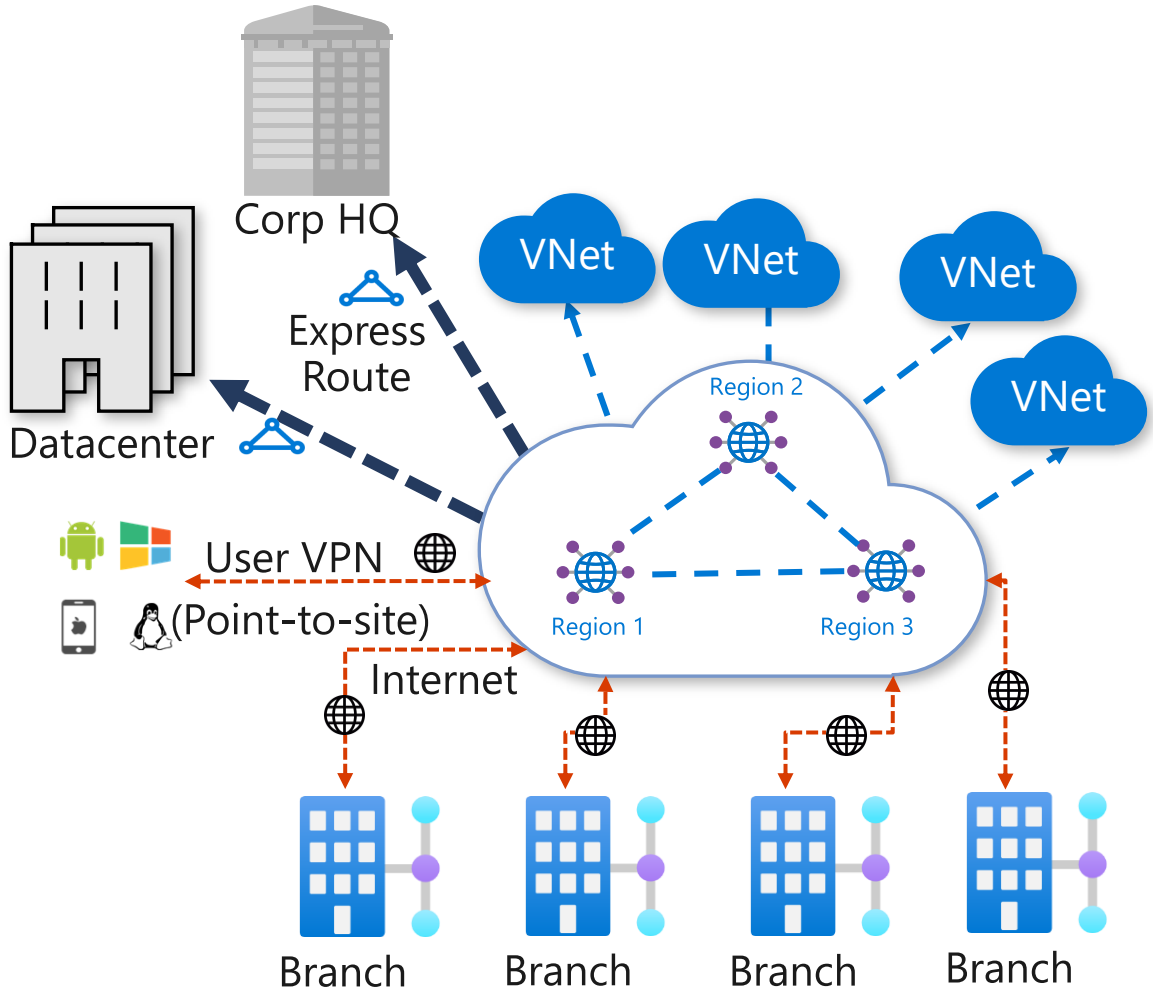
VPN <-> Remote Users

VPN <-> ExpressRoute

VNET <-> VNET

Customized Routing

Security with Azure Firewall and Firewall Manager



Virtual WAN Ecosystem

Announcing: Virtual Appliances in the VWAN hub

VPN & Remote work connectivity

Azure Route Server

Provide BGP* endpoints for network virtual appliance to connect

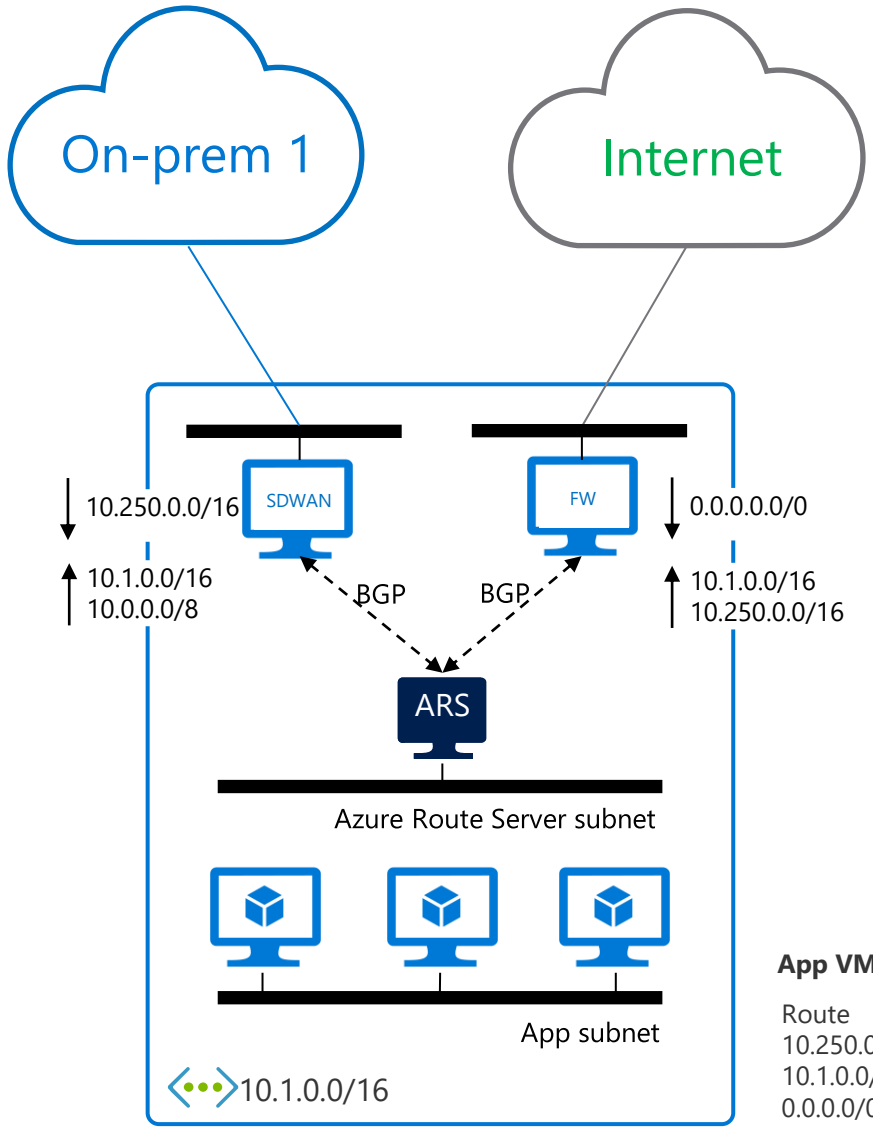
Enable dynamic routing between NVA and Azure virtual network

Simplify NVA deployment on Azure

Support any NVA**

Network topology agnostic (e.g., single VNet, hub-and-spoke, full-mesh)

Integrated with ExpressRoute and VPN gateway



App VM effective routes

Route	Next hop
10.250.0.0/16	SDWAN
10.1.0.0/16	Virtual Network
0.0.0.0/0	FW

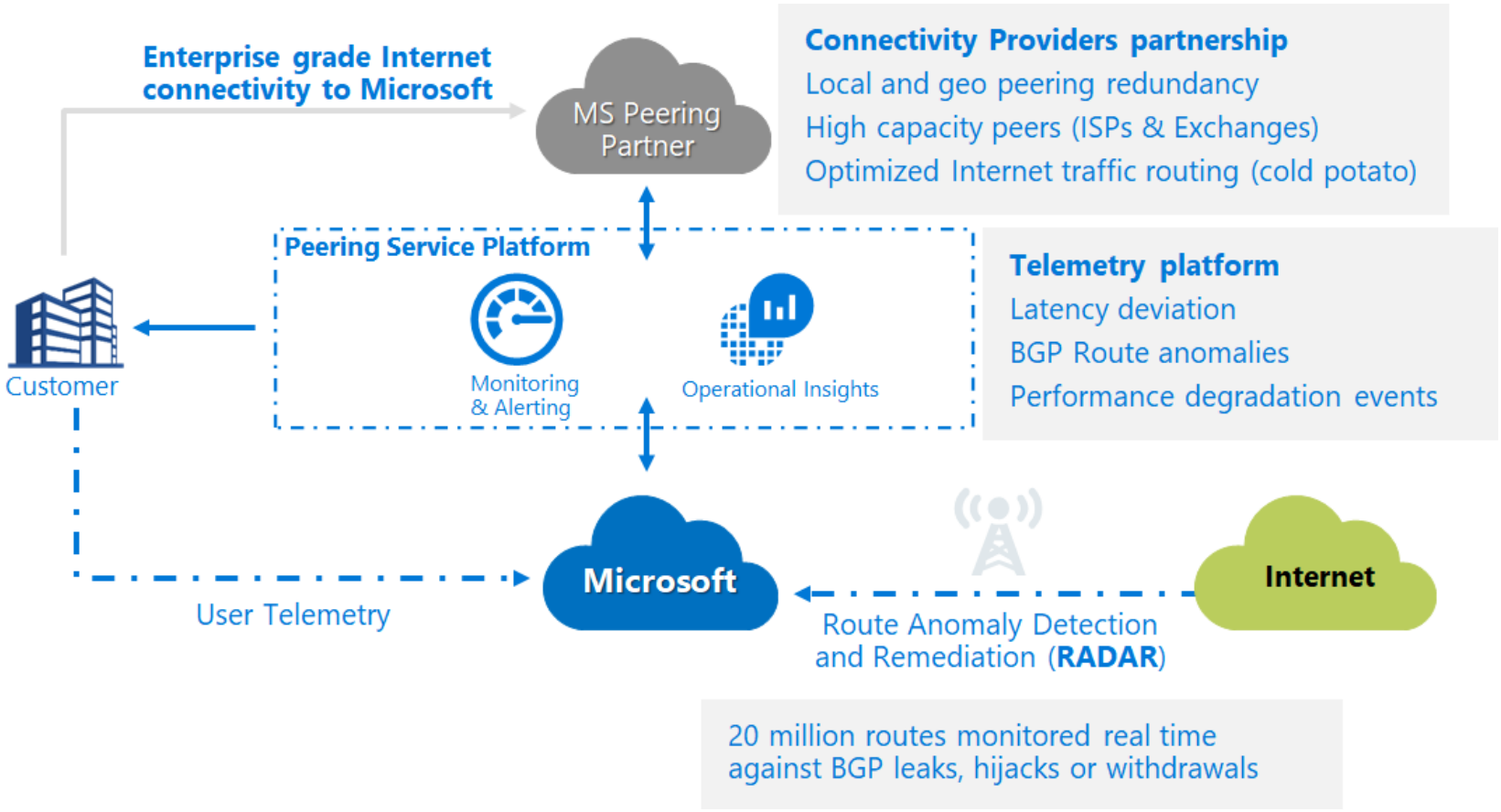
* Border Gateway Protocol is a standard routing protocol

** NVA must support multi-hop BGP

Azure Peering Service

Delivering enterprise grade internet connectivity to Microsoft Cloud Services

- **Optimized Routing**
  - High Capacity ISPs/Exchange partners
  - QoS for voice/video
  - Local and Geo redundancy
  - Cold Potato routing – guaranteed one hop from Microsoft
- **Performance Insights**
  - End to end latency deviation
  - Connection Monitor integration
  - Monitoring & Alerting
- **Route Protection**
  - Route Anomaly Protection with *RADAR* (Route Anomaly Detection & Remediation)
  - Millions of routes monitored for BGP hijacks, leaks, & withdrawals.
  - Route Signing with RPKI

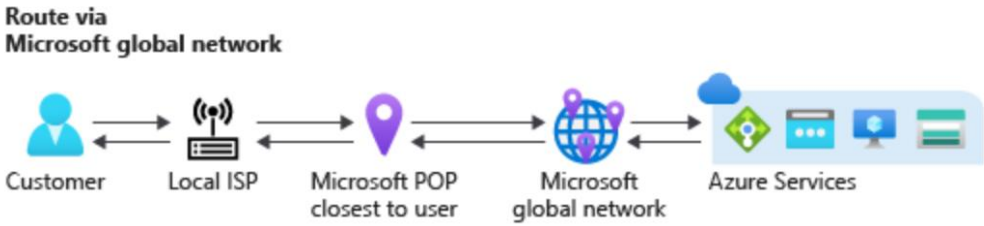


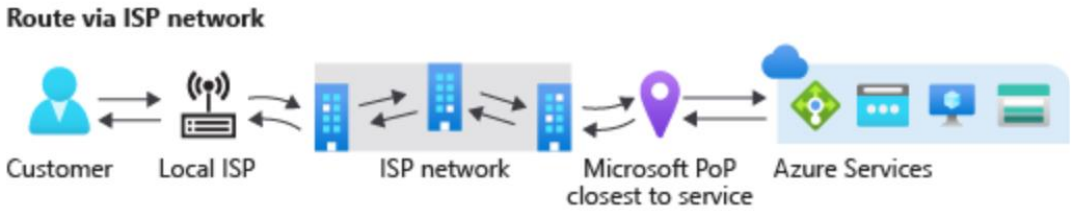
Routing Preference

Enables network choices for internet bound traffic

PREVIEW

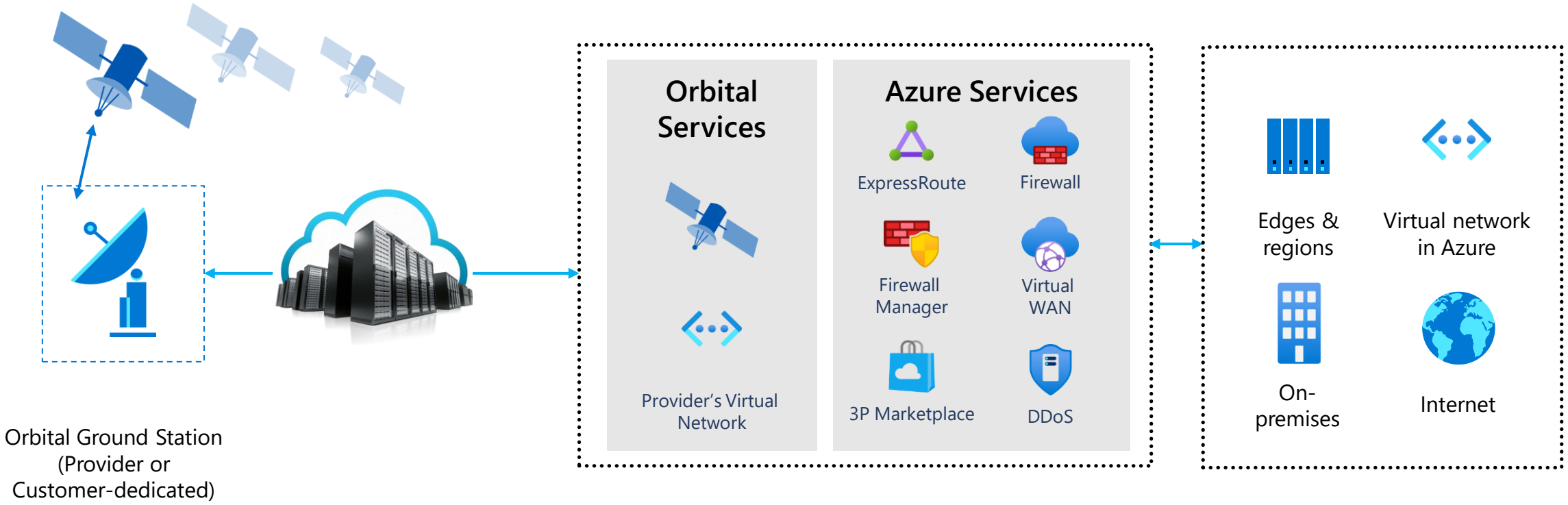
	Routing via Microsoft Network	Routing via ISP Network
Routing	Traffic rides on premium Microsoft network for bulk of its journey	routed via ISP network (public internet)
Performance	Premium performance, high reliability	ISP network performance & reliability
Use case	• high network reliability • global customer base	• egress cost optimization • regional customer base





Azure Orbital

Ground Station as a Service



KSAT KONGSBERG SATELLITE SERVICES · Viasat · KRATOS READY FOR WHAT'S NEXT · AMERGINT TECHNOLOGIES · US ELECTRODYNAMICS, INC. INTERNATIONAL GATEWAYS · SES · KUBOS

VPN & Remote work connectivity

Azure VPN Gateway

VPN

S2S – cross-premises connectivity

VPN over ExpressRoute private peering

IPsec encrypted ExpressRoute

FQDN S2S

Customers without static public IP addresses

BGP with APIPA addresses

Legacy device, AWS/GCP interop

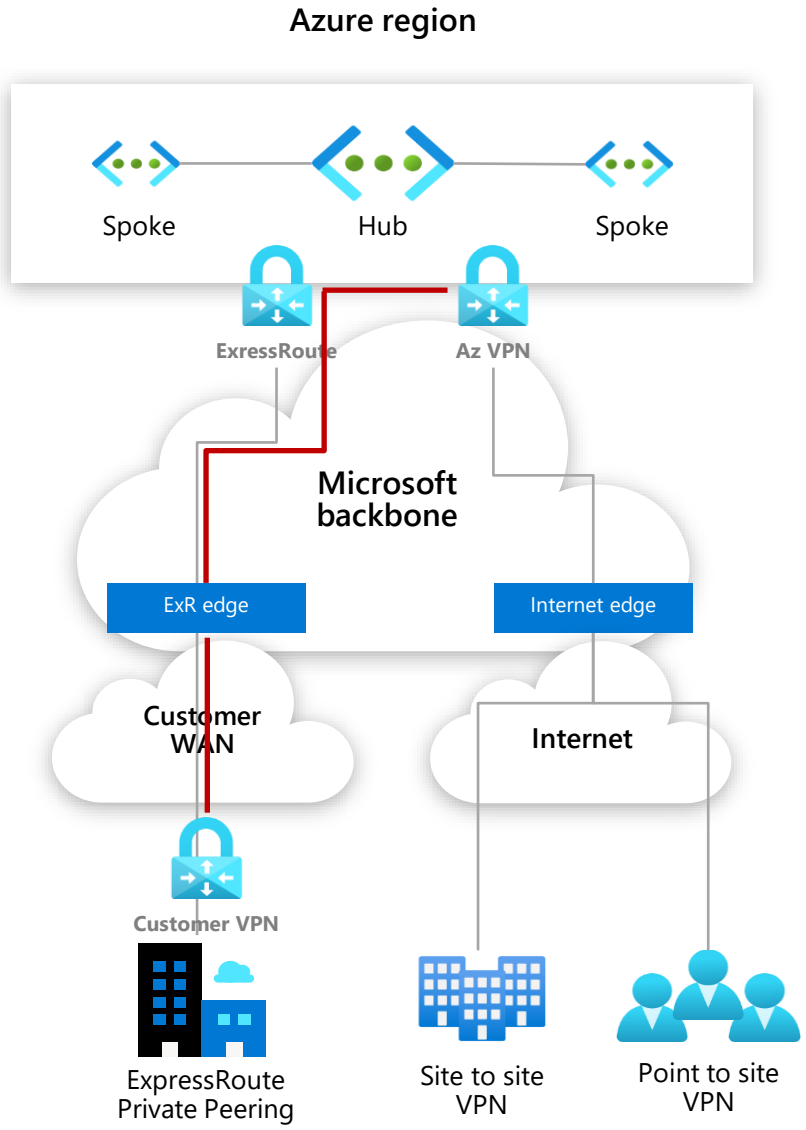
P2S – user SSL VPN connectivity

COVID-19 remote VPN usage surge

94% increase in daily P2S connections

P2S session management & revocation

List & disconnect user connections



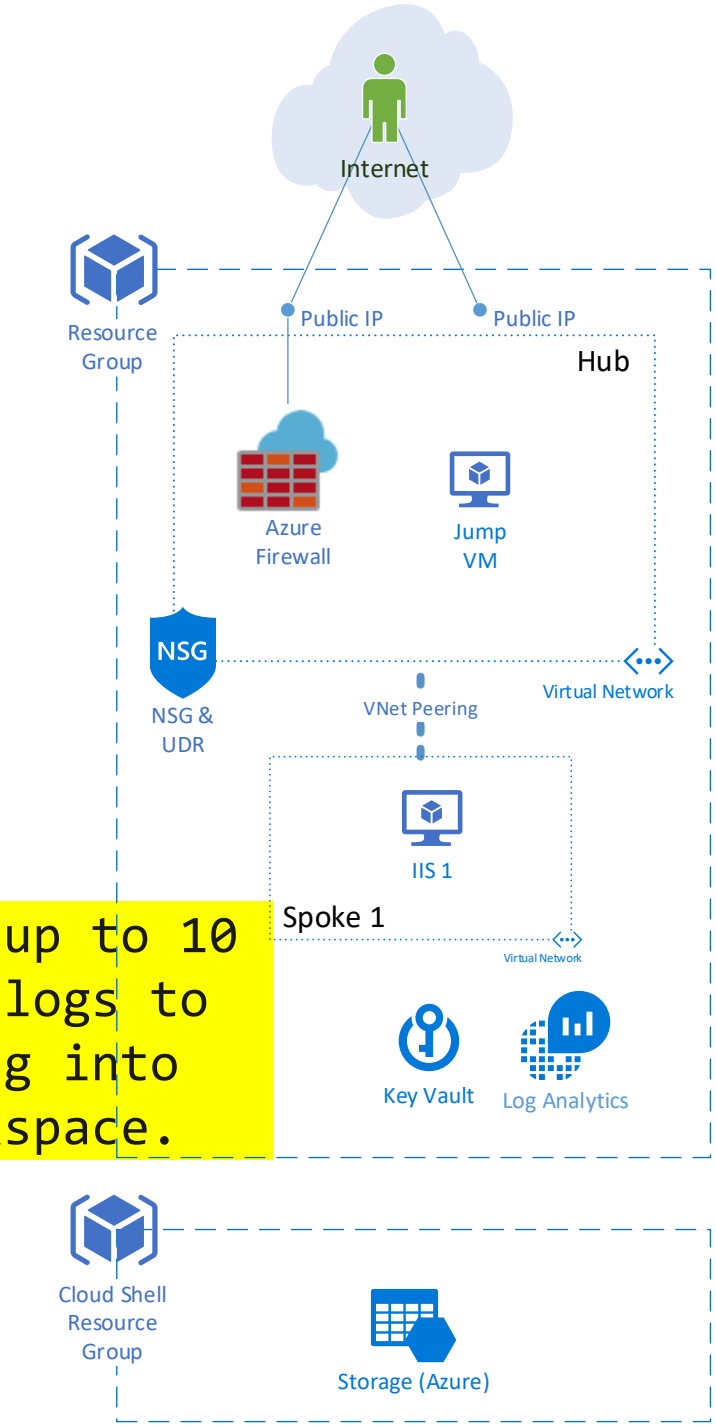
Step 5 (cont)

Execution:
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

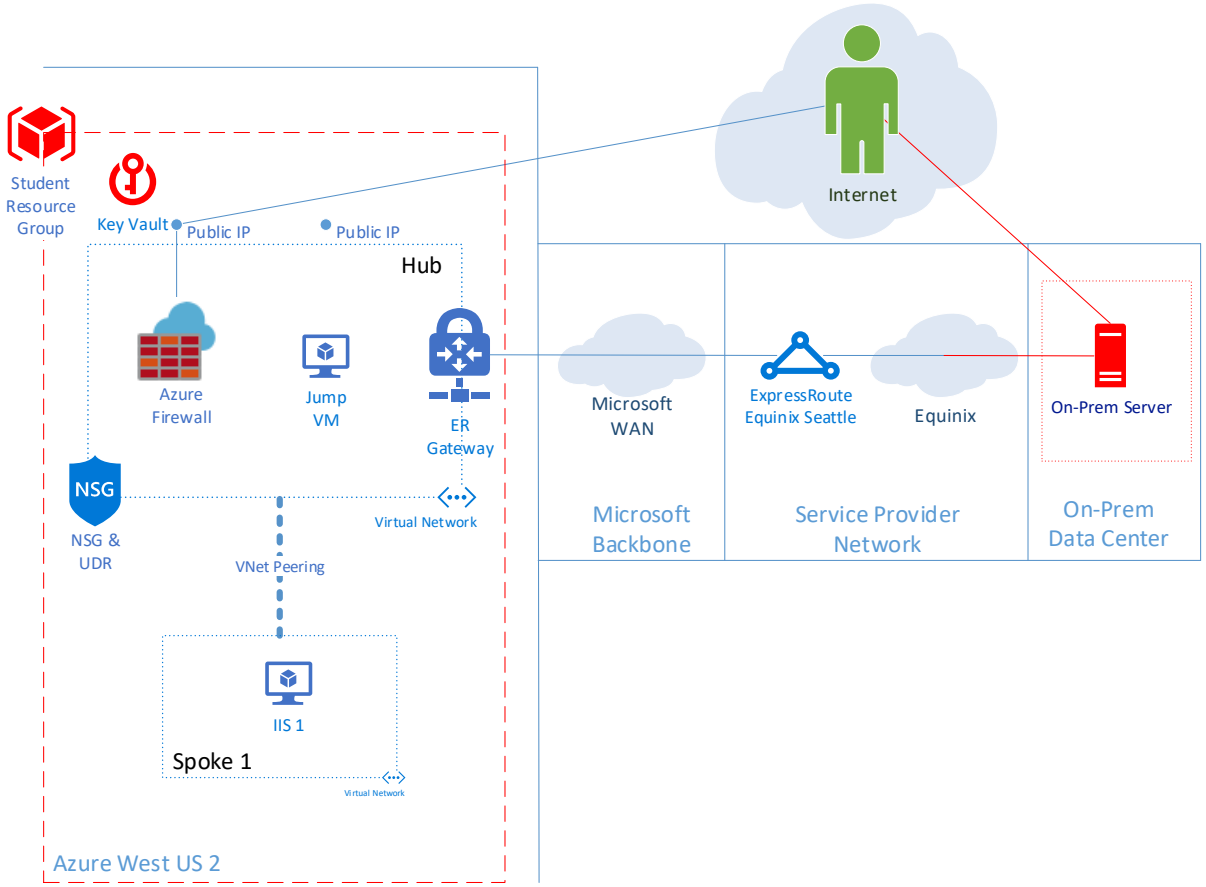
Validation:

1. In your Resource Group open your “Log Analytics workspace”
2. Open the “Logs” tab
3. Review the slide notes below to see some example queries

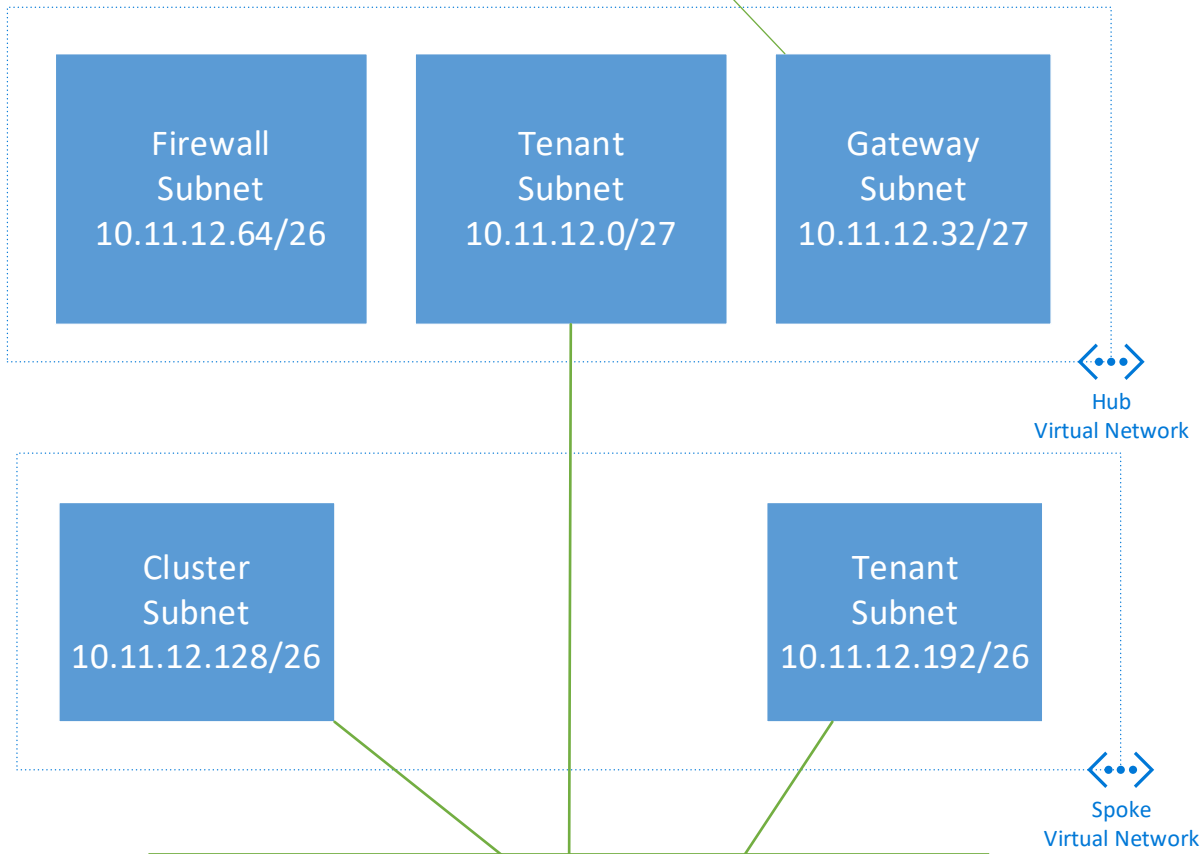


NOTE: It may take up to 10 minutes for logs to begin flowing into the log workspace.

UDR



Prefix	Description	Next Hop
10.11.12.0/27	Hub Tenant	Firewall
10.11.12.128/25	Spoke VNet	Firewall



Prefix	Description	Next Hop
0.0.0.0/0	All Addresses	Firewall

(BGP propagation turned off on this table)

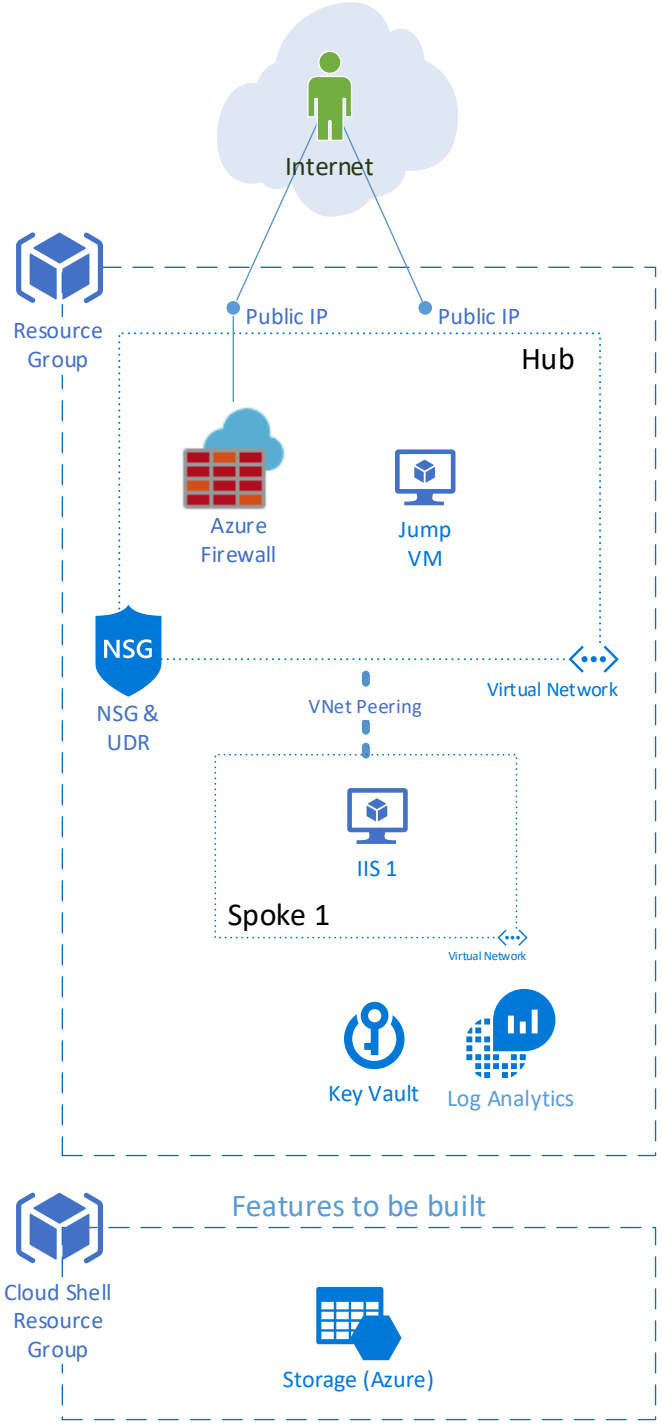
Final

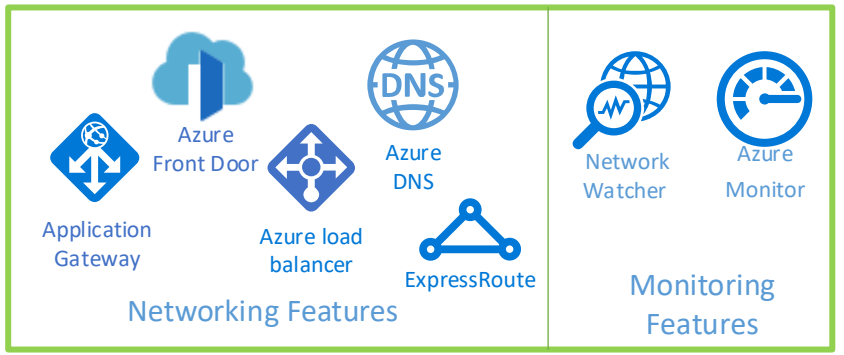
Review these additional features in this deck:

- Virtual WAN

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

- Azure DNS





Features to be discussed

Secure global app delivery

Azure Load Balancer

Azure CDN

Azure Front Door

Azure Web Application Firewall

Azure Application Gateway

Azure Traffic Manager

Internet Analyzer

Azure’s load balancing options

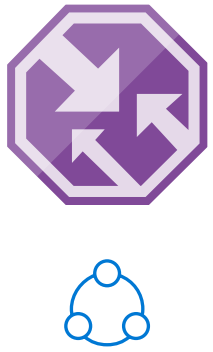
Load Balancer

- Network Layer (TCP/UDP)
- Extreme perf sensitive
- Ultra-low latency

Application Gateway

- Application Layer (HTTP/HTTPS)
- TLS/cert based auth

Traffic Manager

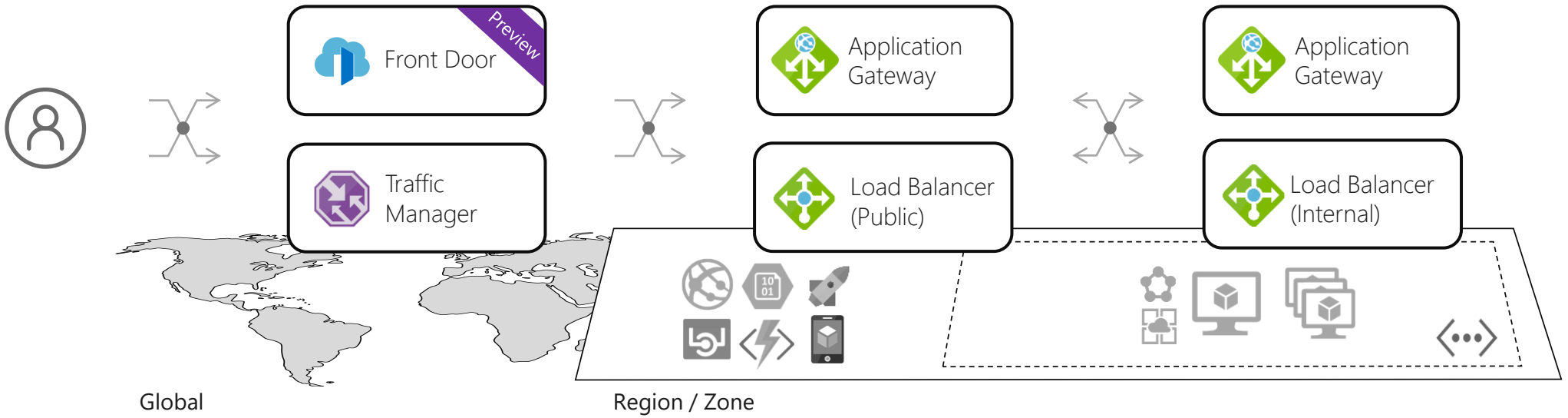


- DNS-based load balancing
- Variety of routing options

Front Door

- Application Layer(HTTP/HTTPS)
- Load balancing at the edge

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.

Azure Load Balancer

Build highly performant, ultra-low latent, global, applications in Azure

PUBLIC PREVIEW

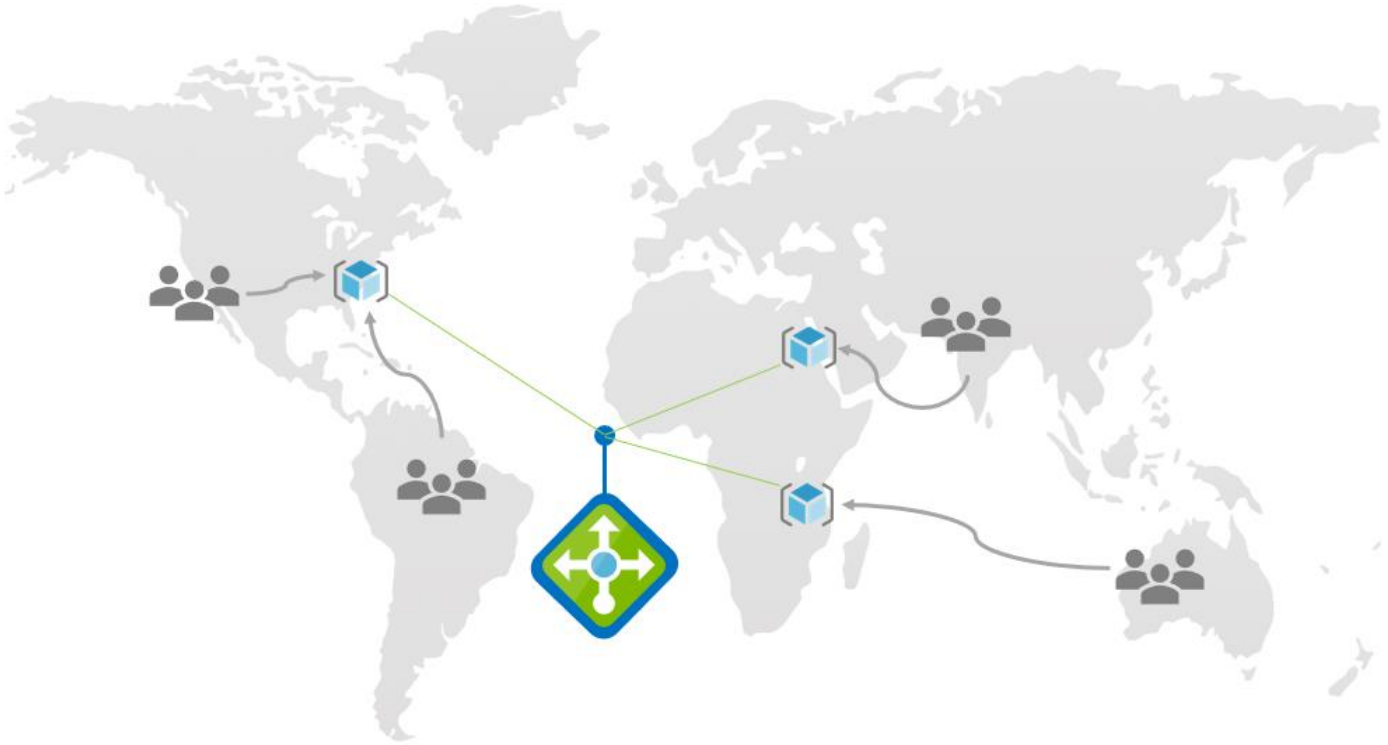
Cross-region load balancing New!

Scales across regions behind a single anycast IP address

Preserves Client's source IP Address

Optimized latency-based routing with seamless failover

Easy to adopt – works with existing regional load balancer



Application Gateway

Application/Layer 7 load balancer

HTTP/HTTPS applications

WebSocket and HTTP/2 support

TLS termination

Terminates connections

Source IP is changed

Auto scaling support

Availability zones support

HTTP to HTTPS redirects

Routing

Regional

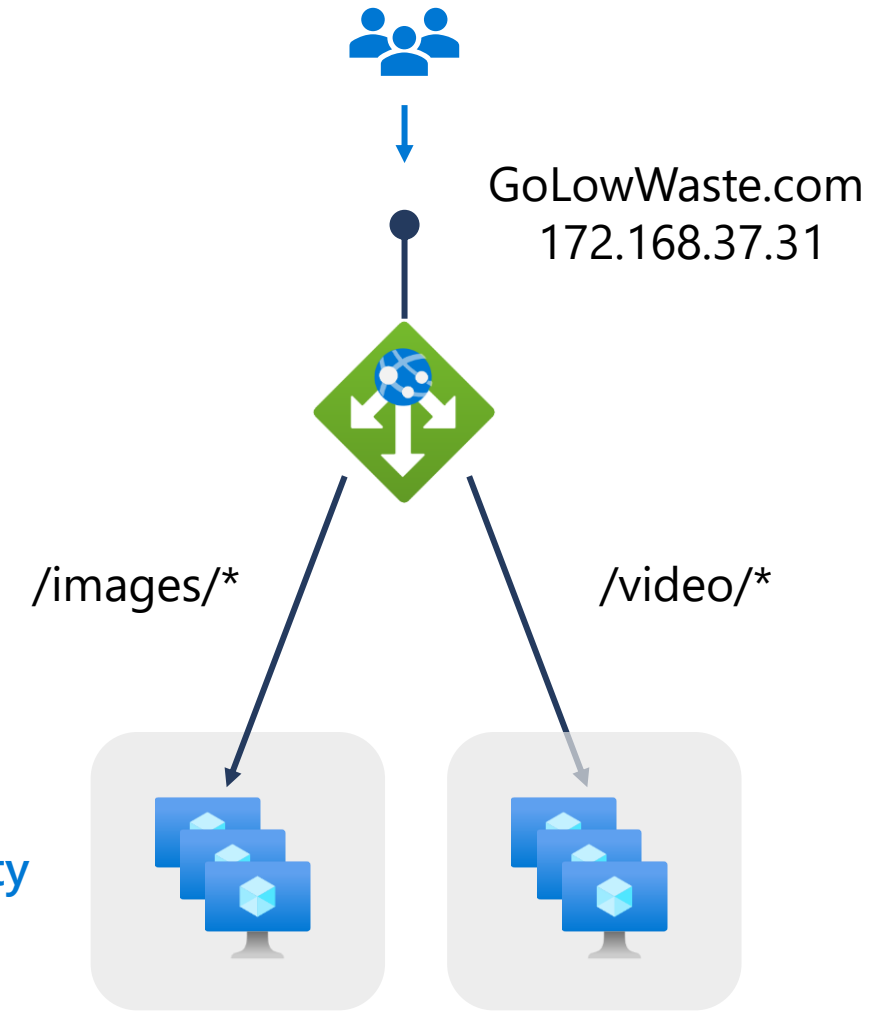
Across Availability Zones

Content based

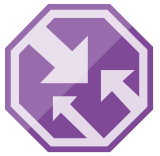
Incoming URL attributes

Host/domain name based

Cookie based session affinity



Traffic Manager



DNS-based load balancer

Supports external, non-Azure endpoints

Hybrid cloud and on-premises deployments

Public facing endpoint

Routing methods

Priority, weighted, performance, geography, subnet, multi-value

Delivery services (AFD, CDN, Application Gateway)

Scalable and secure entry point for your global applications

Cloud native, platform managed global and regional application delivery with integrated WAF and Bot protection

What's New

Rules Engine for AFD/CDN

Wildcard domains for AFD

WAF Sentinel Integration

Public Preview

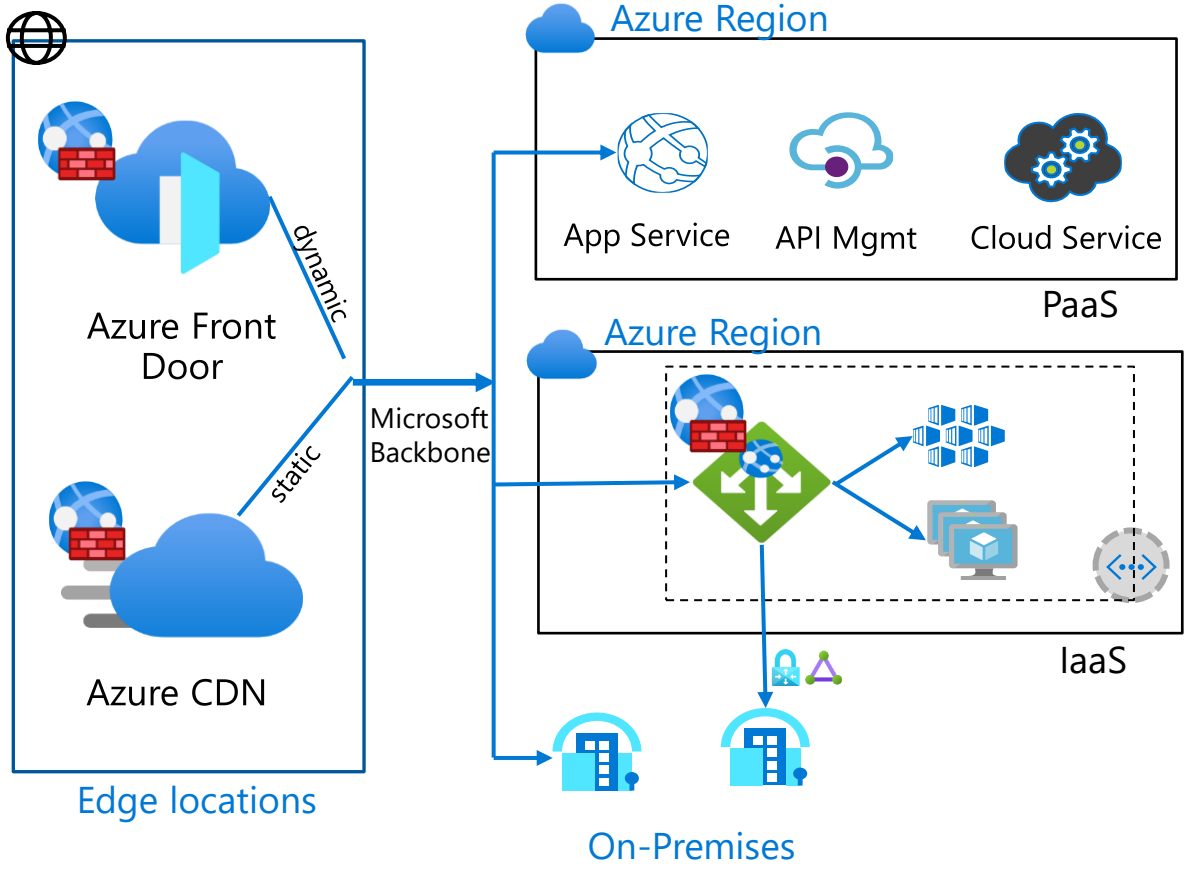
Per URI WAF policy

Multi Origin support for CDN

AKS Ingress Controller add-on support for Application Gateway

URL rewrite support for Application Gateway

Wildcard listener support for 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 current 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