



Microsoft Ignite The Tour





Building a scalable and secure Azure network

Andreas Sobczyk
Partner, Consultant & Azure MVP @
CTGlobal



Andreas Sobczyk



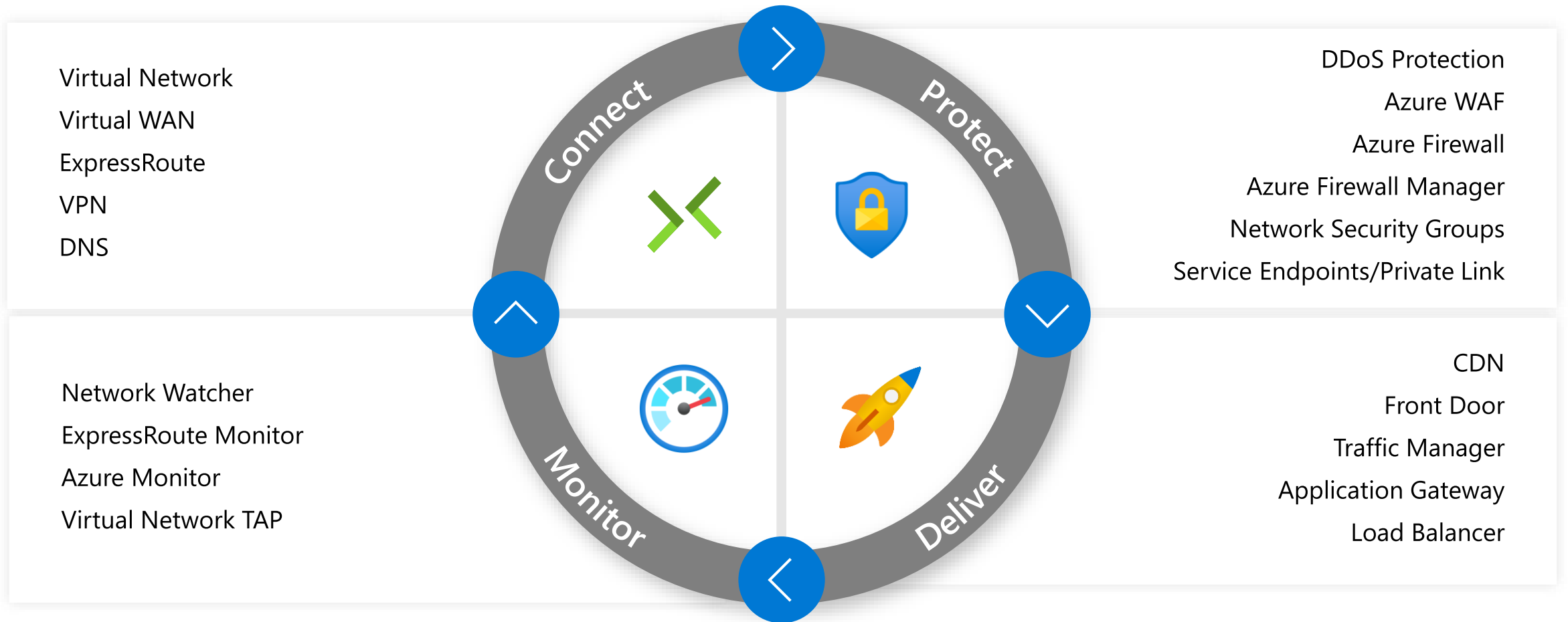
- Senior Consultant @ CTGlobal
- Microsoft Azure MVP
- Focus Areas
 - Azure
 - Azure Stack
 - Automation



- Co-Founder Cloud & Datacenter User Group
- @Andreas_Sobczyk
- Blog: CloudMechanic.net
- Sparetime: Racing



Azure networking services



Network Announcements the past 2 weeks

- Unified network monitoring with connection monitor 2.0
- New Azure Firewall Features
 - ICSA Labs Corporate Firewall Certification
 - Forced tunneling support now in preview
 - IP groups now in preview
 - Customer configured SNAT private IP address ranges now generally available
 - High ports restriction relaxation now generally available
- Azure Firewall Manager support for Virtual Networks
- Private Link GA
- ARM template support for NSG flow logs

Virtual Networks

Your virtual private network in the cloud



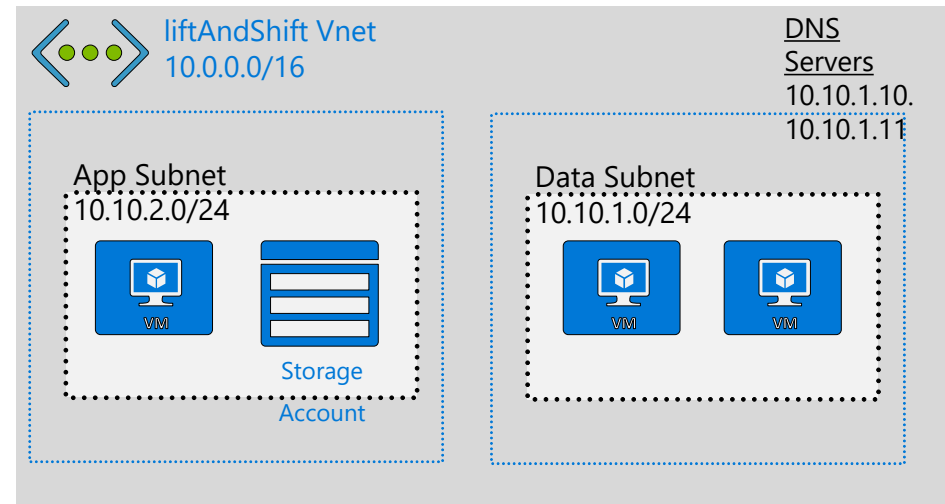
Private isolated logical network

Subnets to enable micro-segmentation

Connects resources within the same subscription

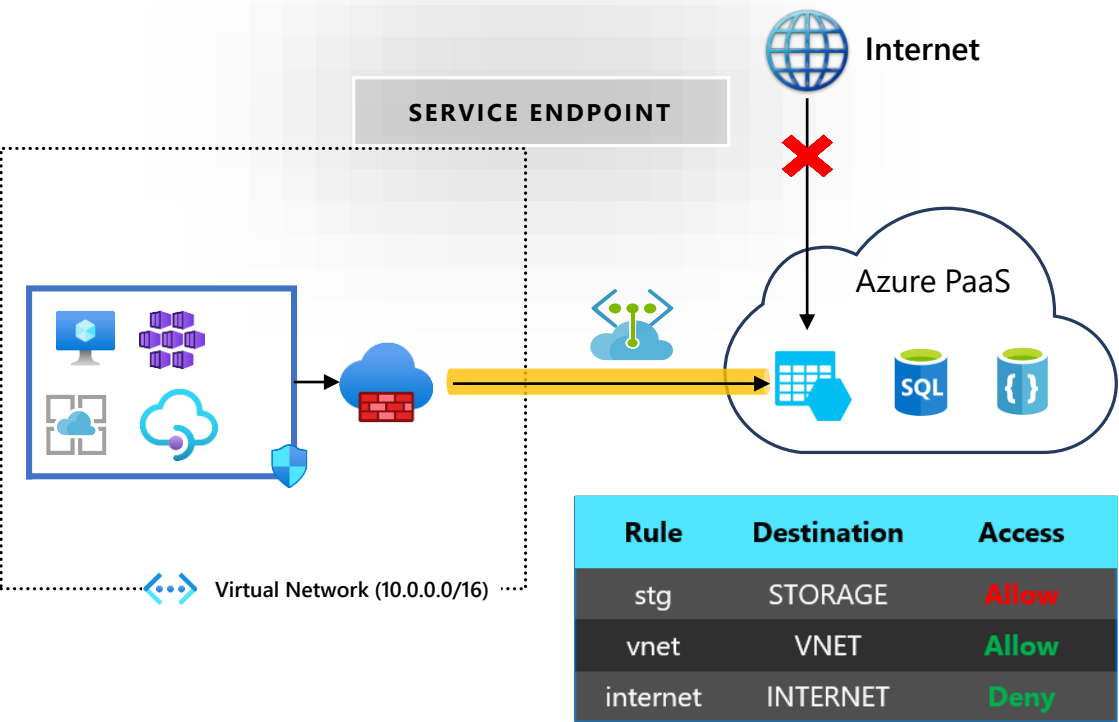
Private connectivity for virtual machines and Azure Resources (service endpoints)

Bring your own DNS or use Azure-provided DNS server

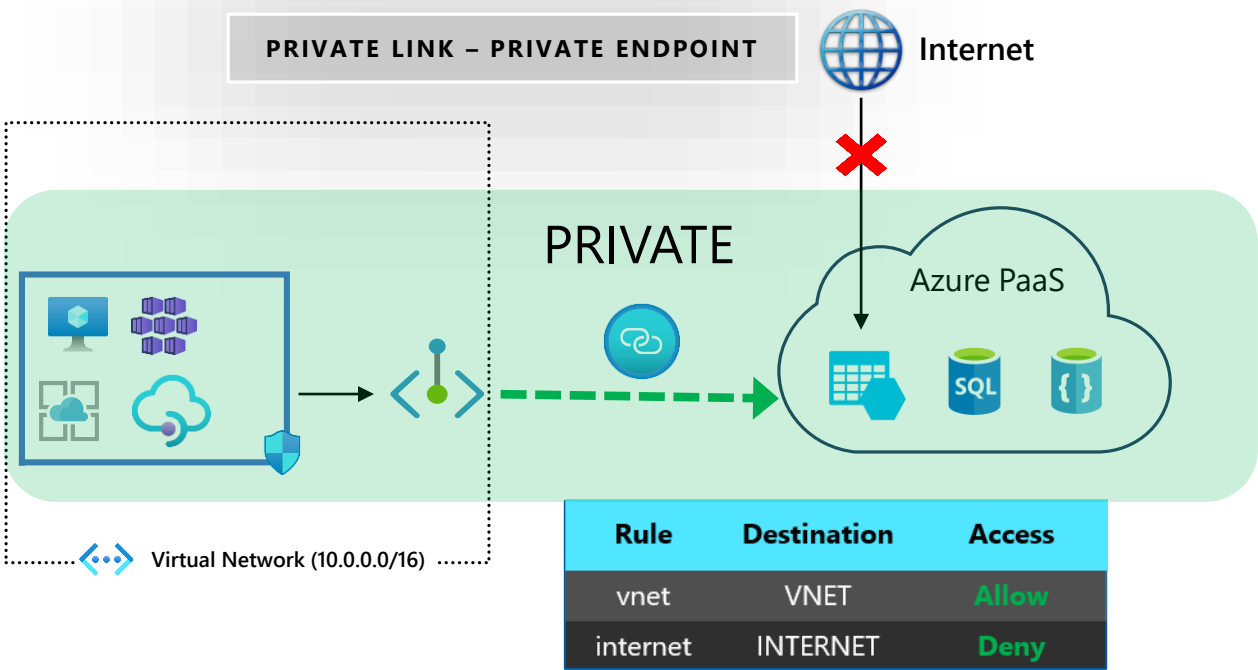


Service Endpoint & Private Link

Secure Azure PaaS Resources



VNet to PaaS service via the Microsoft backbone
Destination is still a public IP address. NSG opened to Service Tags
Need to pass NVA/Firewall for exfiltration protection



VNet PaaS via the Microsoft backbone
PaaS resource mapped to Private IP Address. NSGs restricted to VNet space
In-built data exfiltration protection

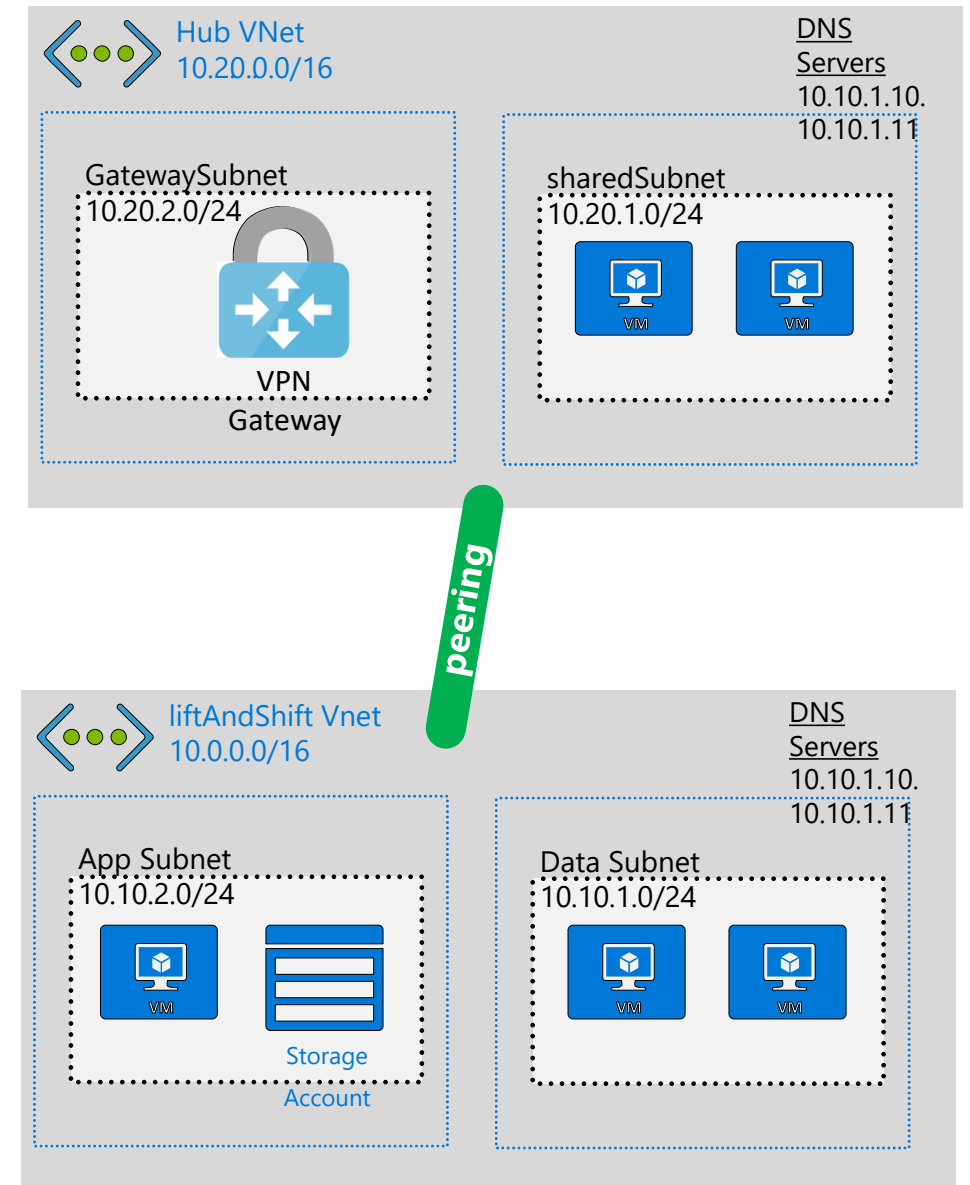
VNet Peering

Direct L3 connectivity between VNets

Bypass VPN Gateway to deliver high throughput, low latency connectivity

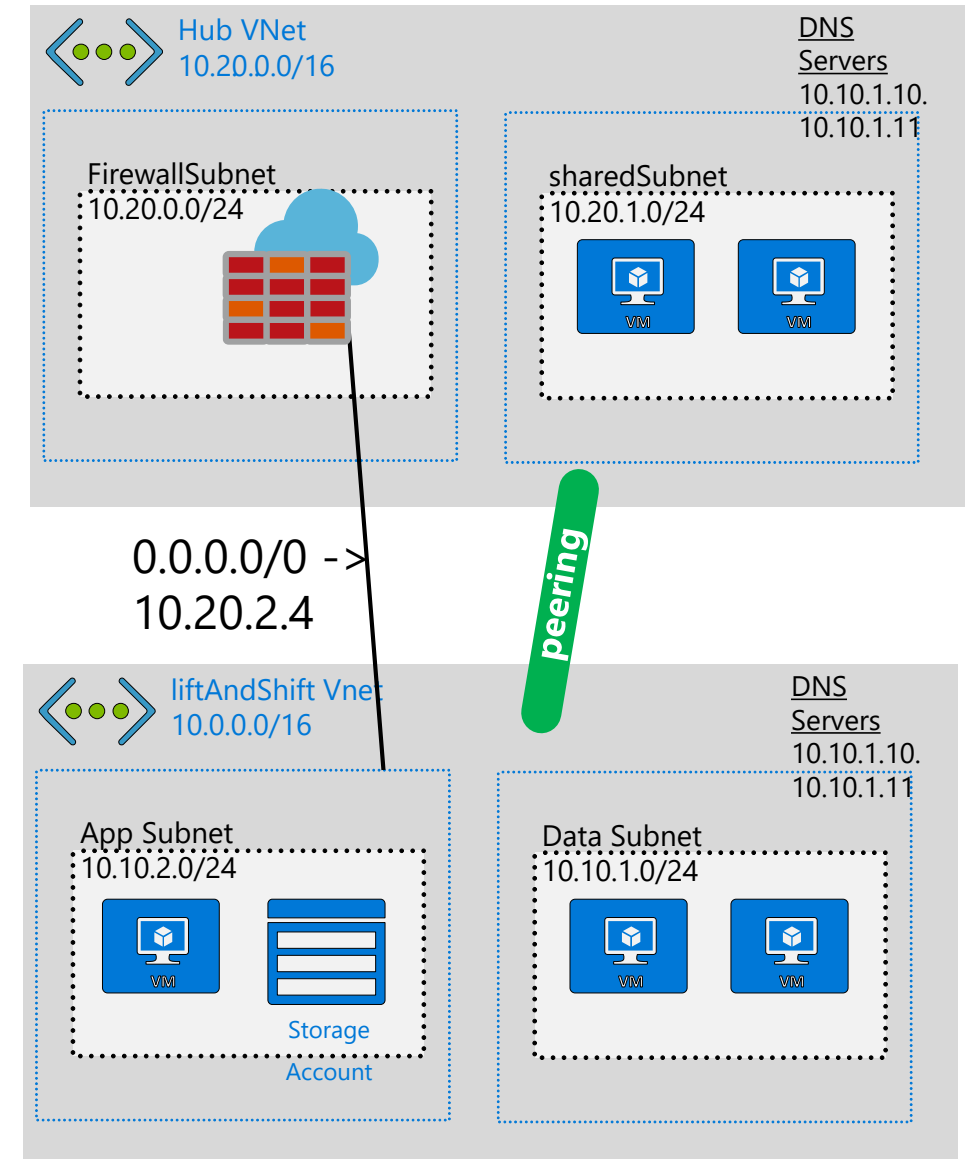
Peer across subscriptions, regions and even tenants

Support for Gateway Transit and NVAs in same region peering



User Defined Routes

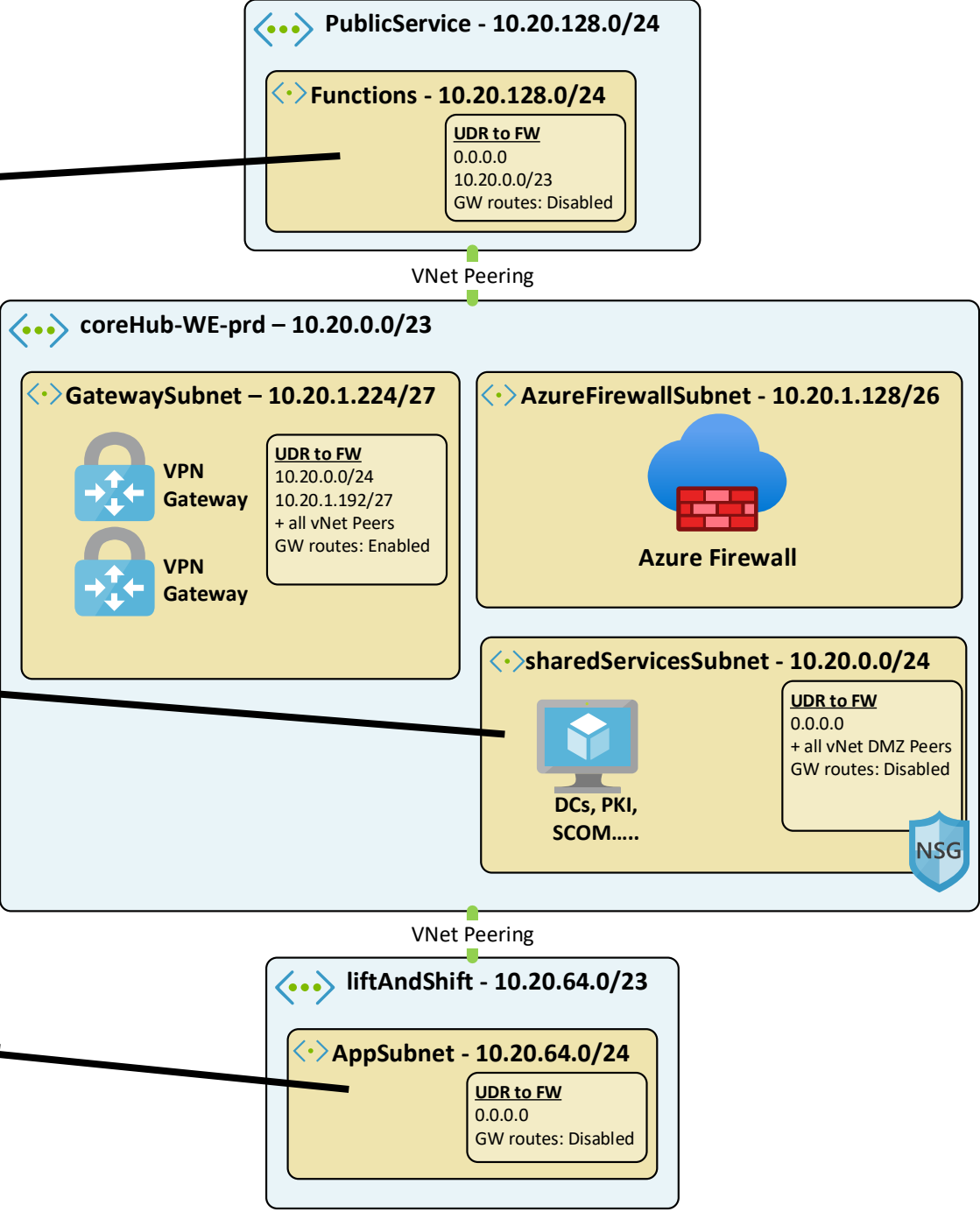
- The hardest and most important part!
- Attach route tables to Subnets
- Specify next hop for any address
- User-defined -> BGP - System
- The most accurate route wins



Effective routes					
Source ↑↓	State ↑↓	Address Prefixes ↑↓	Next Hop Type ↑↓	Next Hop ...↑↓	User Defined Route Name ↑↓
Default	Active	10.20.128.0/25	Virtual network	-	-
User	Active	0.0.0.0/0	Virtual appliance	10.20.1.132	defaultRouteToFW
User	Active	10.20.0.0/23	Virtual appliance	10.20.1.132	fw-To-coreHub-WE-tst
Default	Invalid	10.20.0.0/23	VNet peering	-	-
Default	Invalid	0.0.0.0/0	Internet	-	-

Effective routes					
Source ↑↓	State ↑↓	Address Prefixes ↑↓	Next Hop Type ↑↓	Next Hop ...↑↓	User Defined Route Name ↑↓
Default	Active	10.20.0.0/23	Virtual network	-	-
Default	Active	10.20.124.0/23	VNet peering	-	-
User	Active	0.0.0.0/0	Virtual appliance	10.20.1.132	defaultRouteToFW
User	Active	10.20.128.0/17	Virtual appliance	10.20.1.132	fw-To-DMZ-WE
User	Active	10.20.128.0/25	Virtual appliance	10.20.1.132	fw-To-spokeDMZ-dev
Default	Invalid	10.20.128.0/25	VNet peering	-	-
Default	Invalid	0.0.0.0/0	Internet	-	-

Effective routes					
Source ↑↓	State ↑↓	Address Prefixes ↑↓	Next Hop Type ↑↓	Next Hop ...↑↓	User Defined Route Name ↑↓
Default	Active	10.20.124.0/23	Virtual network	-	-
Default	Active	10.20.0.0/23	VNet peering	-	-
User	Active	0.0.0.0/0	Virtual appliance	10.20.1.132	defaultRouteToFW
Default	Invalid	0.0.0.0/0	Internet	-	-



Network Security Groups

Your virtual private network in the cloud








Controls inbound and outbound access to Subnets and VM NICs

Rules are based on source IP, source port, destination IP, destination port, and protocol

Micro-segmentation of services instead of creating subnets

Dynamic endpoints using Application Security Groups and Service Tags

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
1000	 myNetworkSecurityGroupRul...	3389	TCP	AzureCloud.WestEur...	Any	 Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	 Deny	...

Network Security Groups

Lessons learned



- One NSG per subnet for general protection and logging
- One NSG per service for micro-segmentation
- Control only inbound
- Use Service Map to figure out rules
- Enable flow log for troubleshooting

VPN Gateway

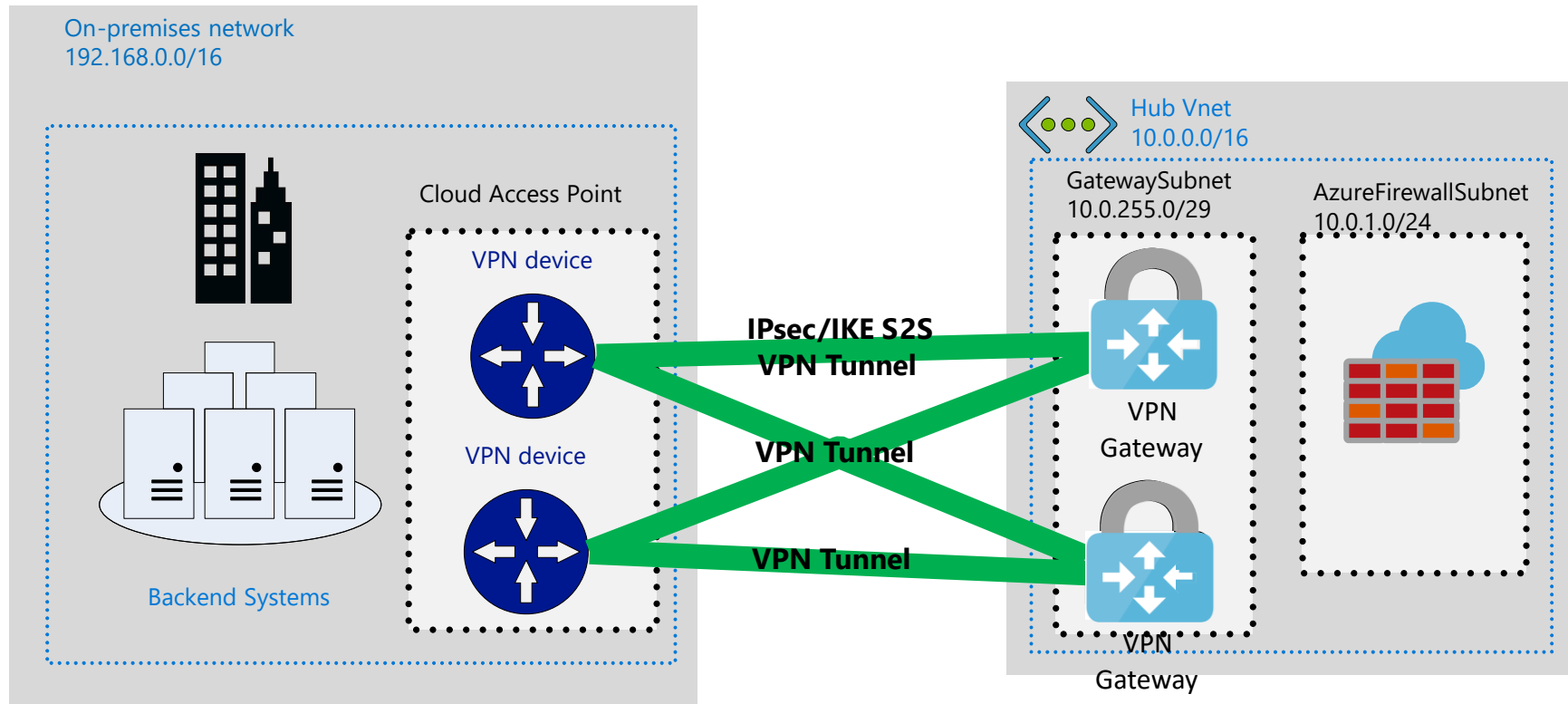


Encrypted traffic between an Azure network and on-premises locations over the public Internet

Up to 10 Gbps

Fast and cheap to deploy

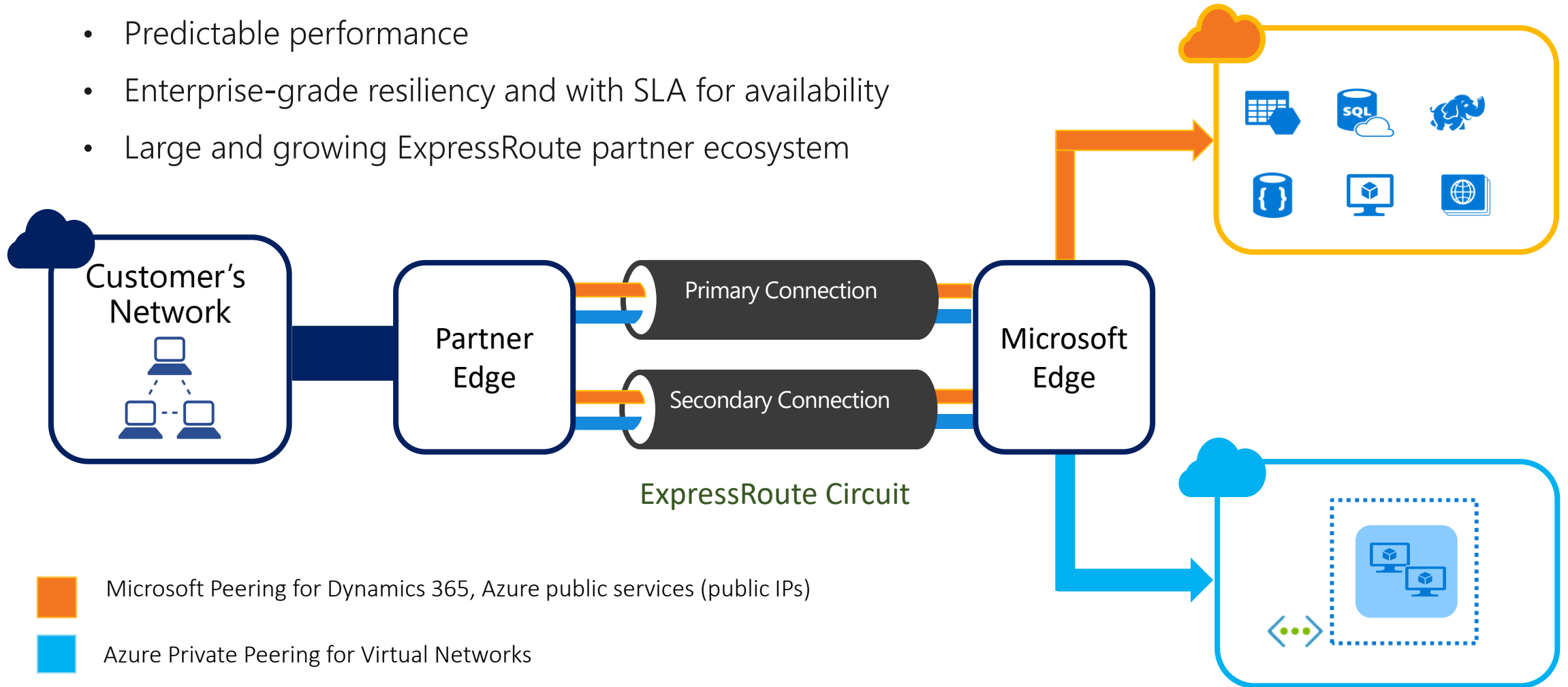
Thrid-party VPN Gateways available

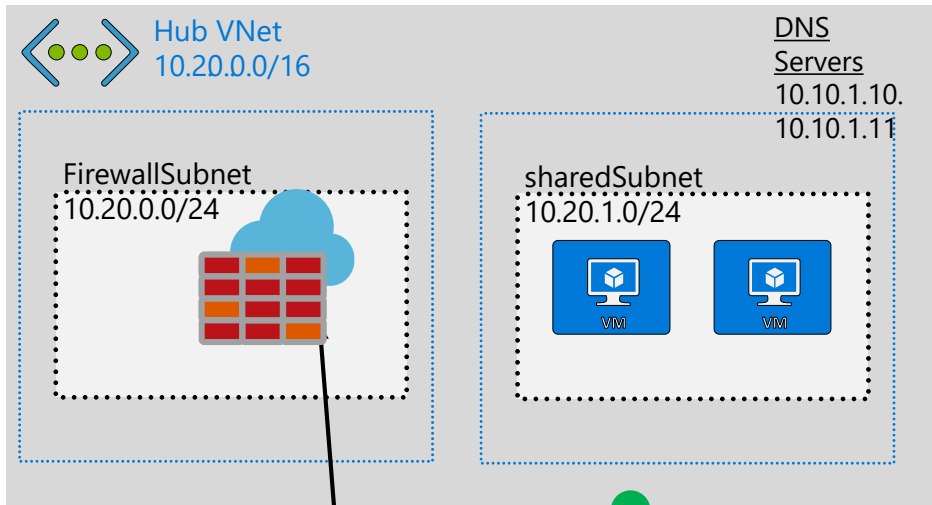


Azure ExpressRoute



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

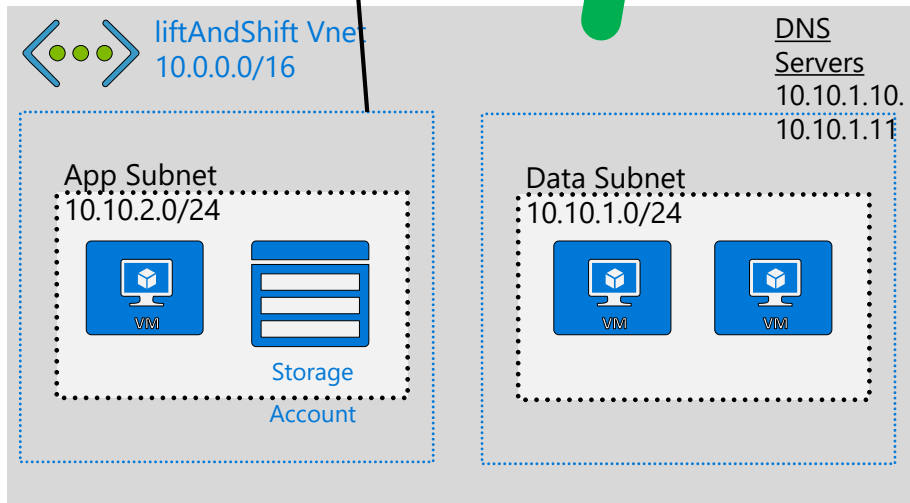




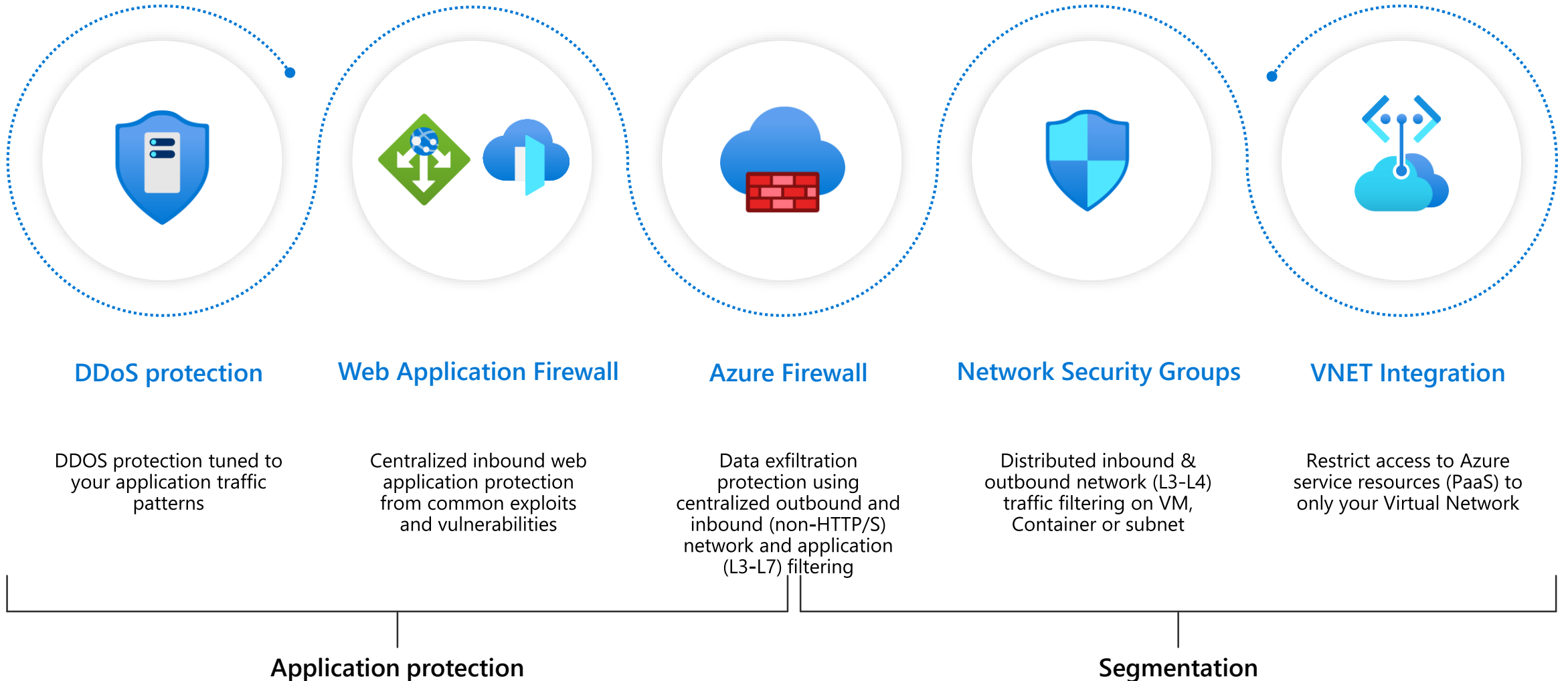
0.0.0.0/0 ->
10.20.2.4

peering

Demo!



Protection services enabling zero trust



Azure DDoS Protection

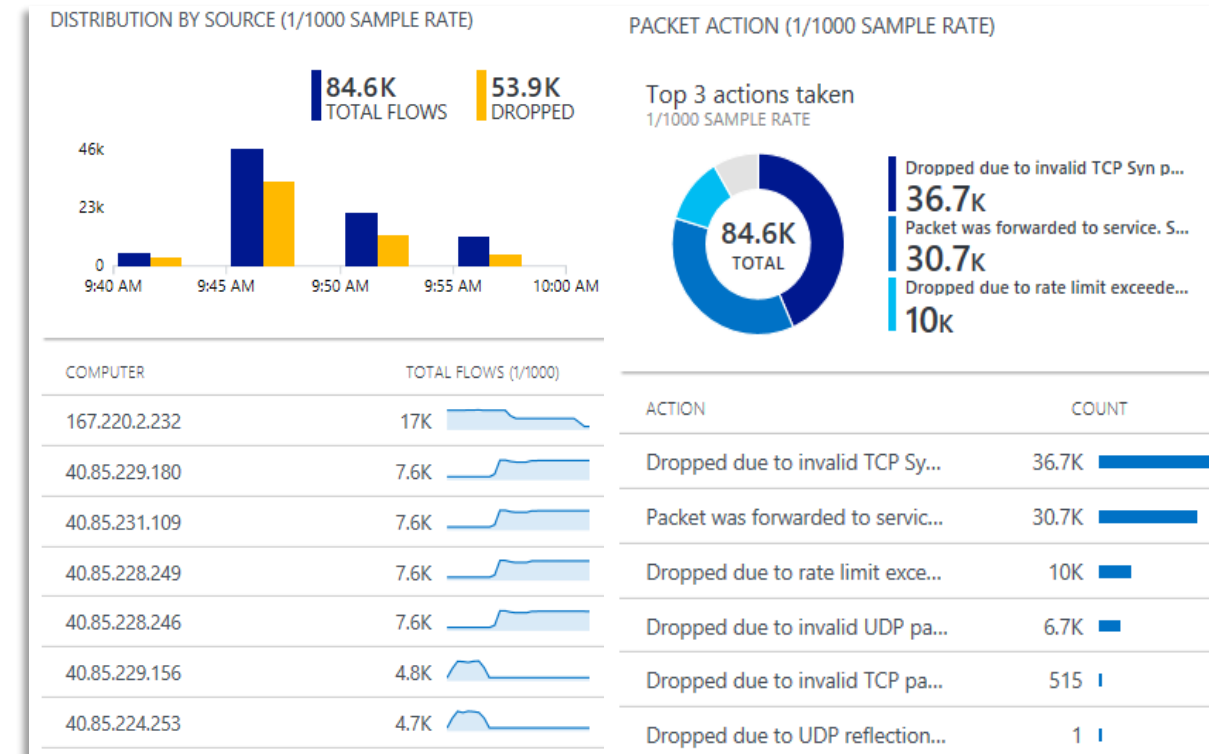
Cloud scale DDoS protection tuned to applications



- 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

Standard Features

- **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

Azure Web Application Firewall

Protect web sites from common application vulnerabilities

Platform managed WAF

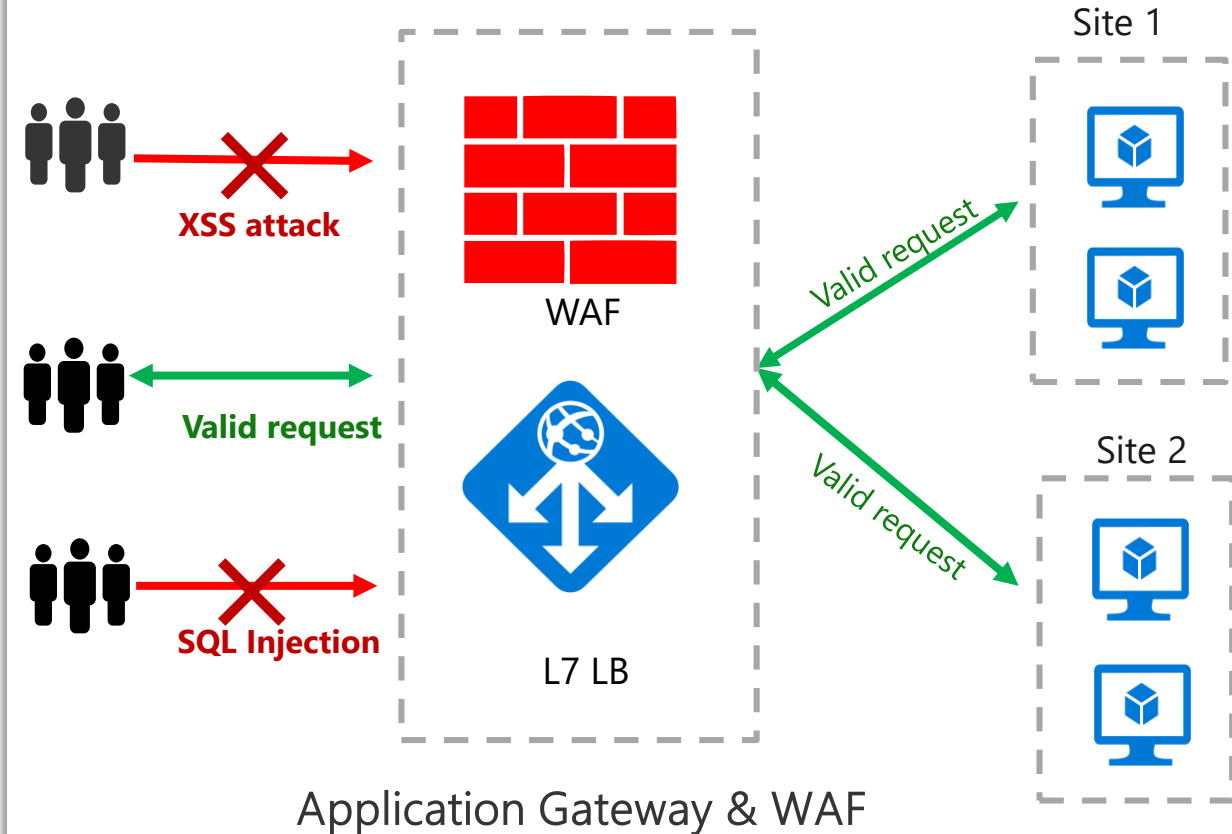
Built in high availability and scalability

Protect application

SQL Injection, XSS, protocol violation & others

Near real time monitoring

Azure Monitor & Azure Security Center



Azure Firewall

Cloud native stateful Firewall as a service



Central governance of all traffic flows

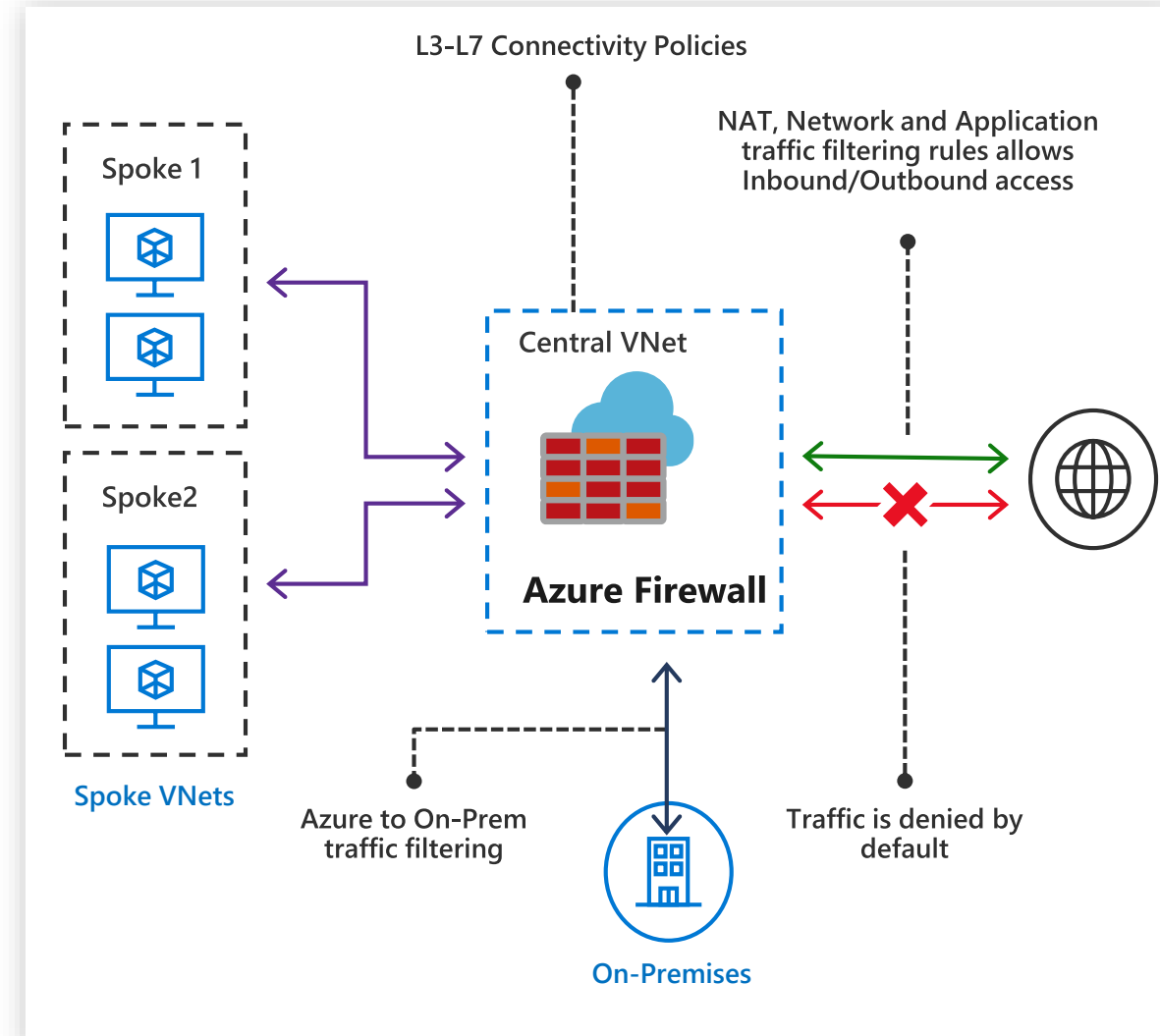
- Built-in high availability and auto scale
- Network and application traffic filtering
- Inbound DNAT and Multiple Public IP Addresses
- Centralized policy across VNets and subscriptions

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





Azure Firewall Manager

Central network security policy and route management for globally distributed, software-defined perimeters

PREVIEW

Central deployment and configuration

- Deploy and configure multiple Azure Firewall instances
- Optimized for DevOps with Hierarchical policies

Automated routing

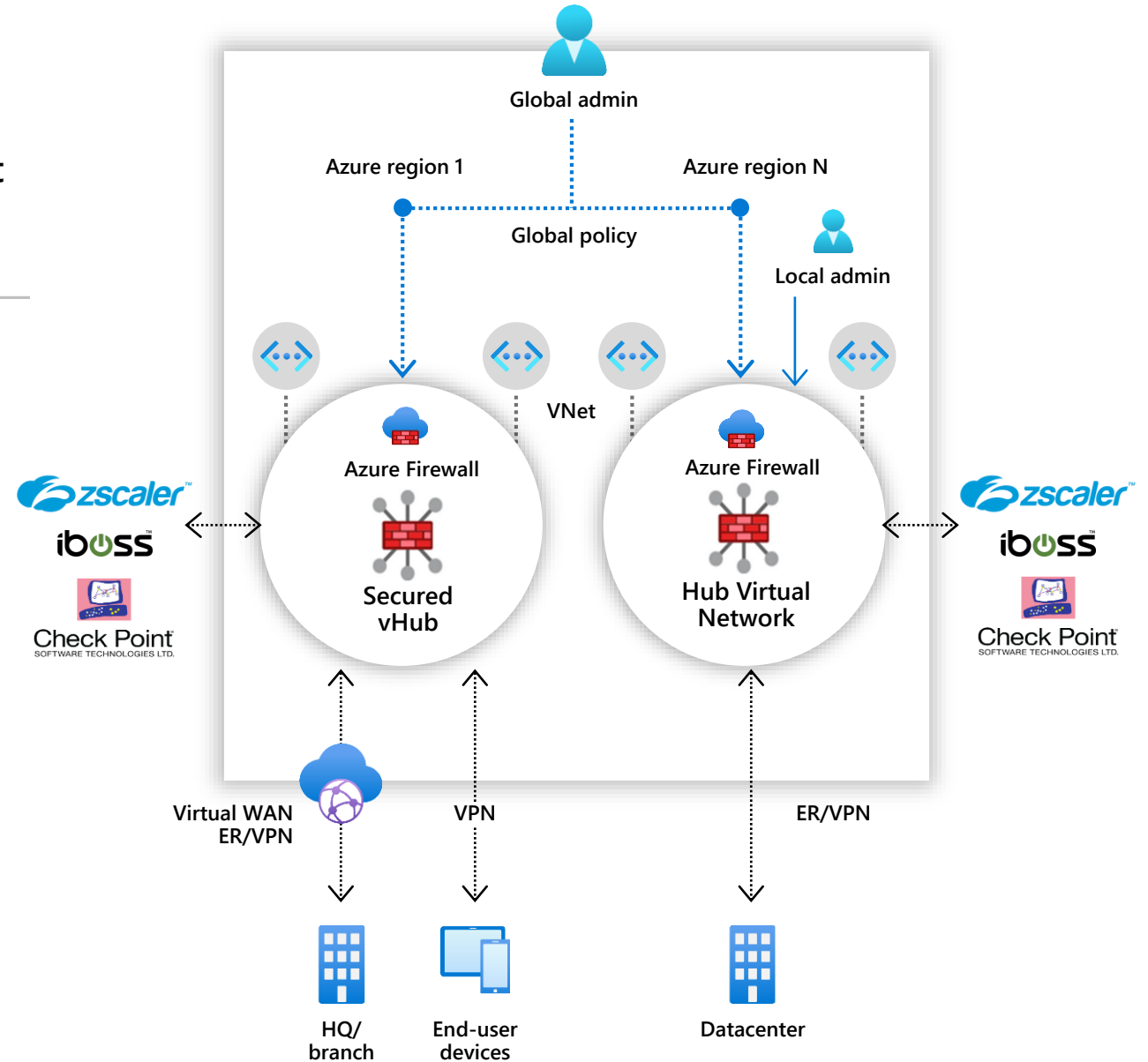
Easily attract traffic to your secured hub for filtering and logging using central routing configuration

Virtual Network support, Split routing

- Support Azure Firewall in a Virtual Network
- Optimized O365 and Azure public PaaS access

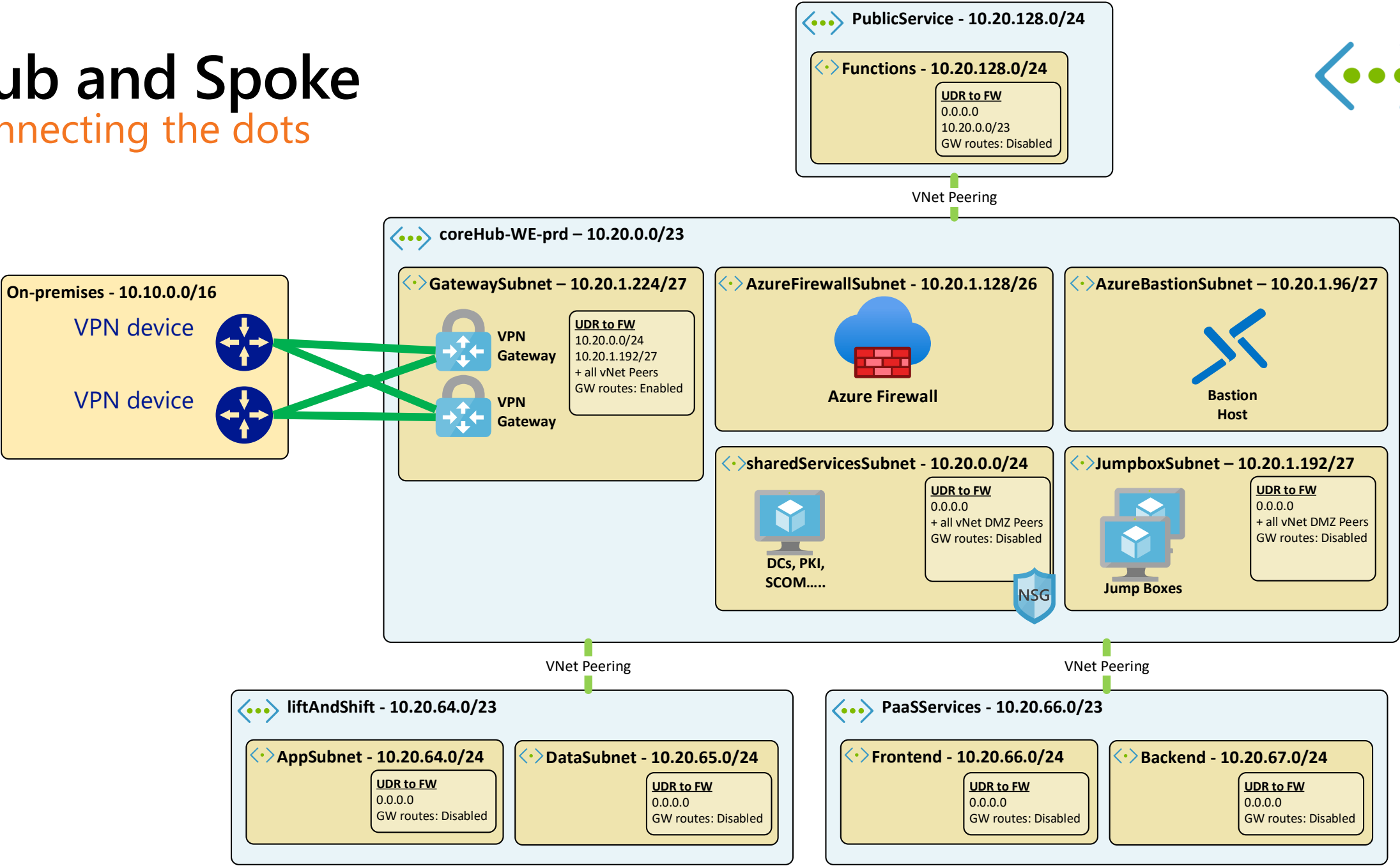
Advanced security with 3rd party SECaaS

- Use best-in-breed third party Security as a Service (SECaaS) partners for advanced internet security
- Combine with Azure Firewall for private traffic

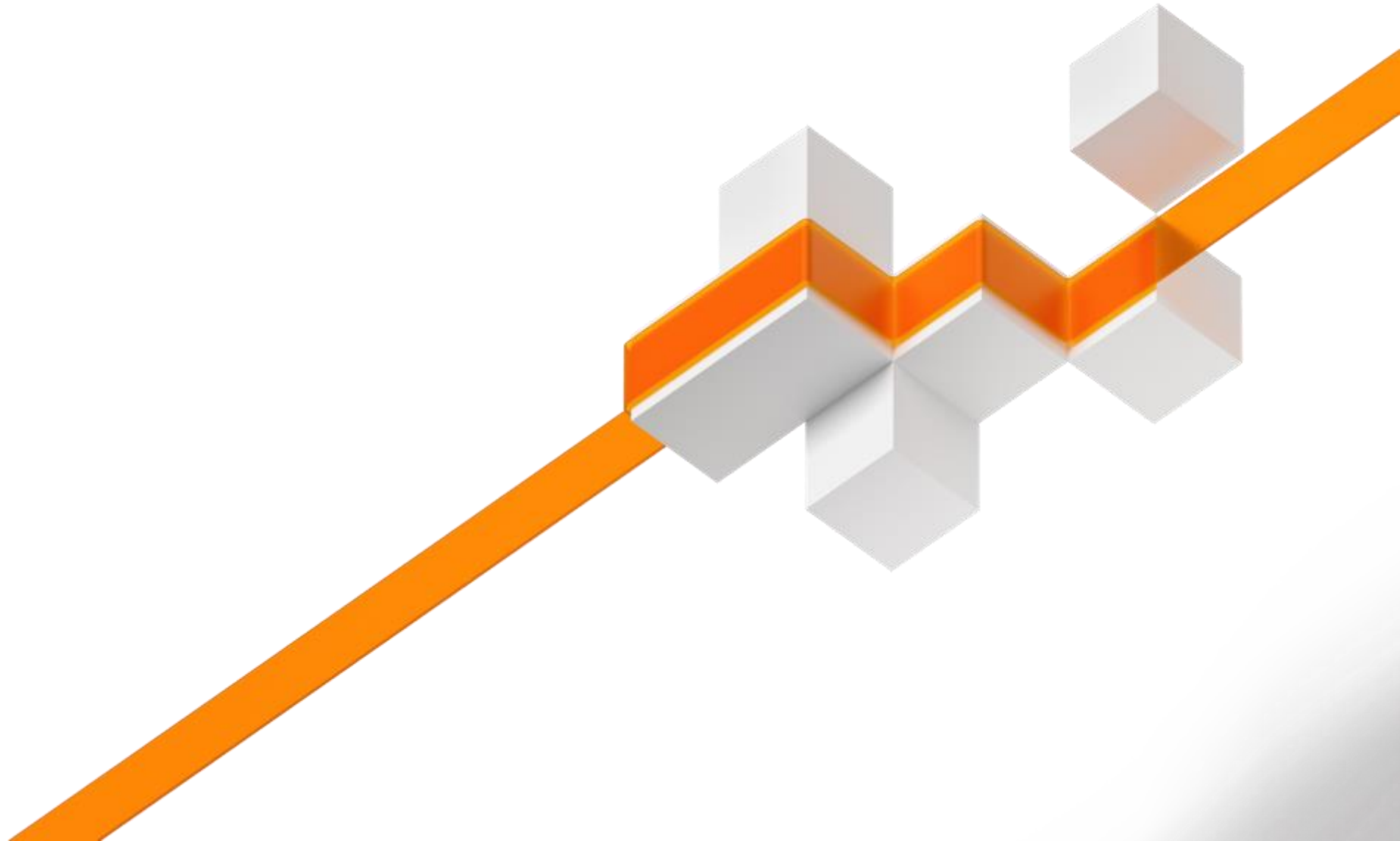


Hub and Spoke

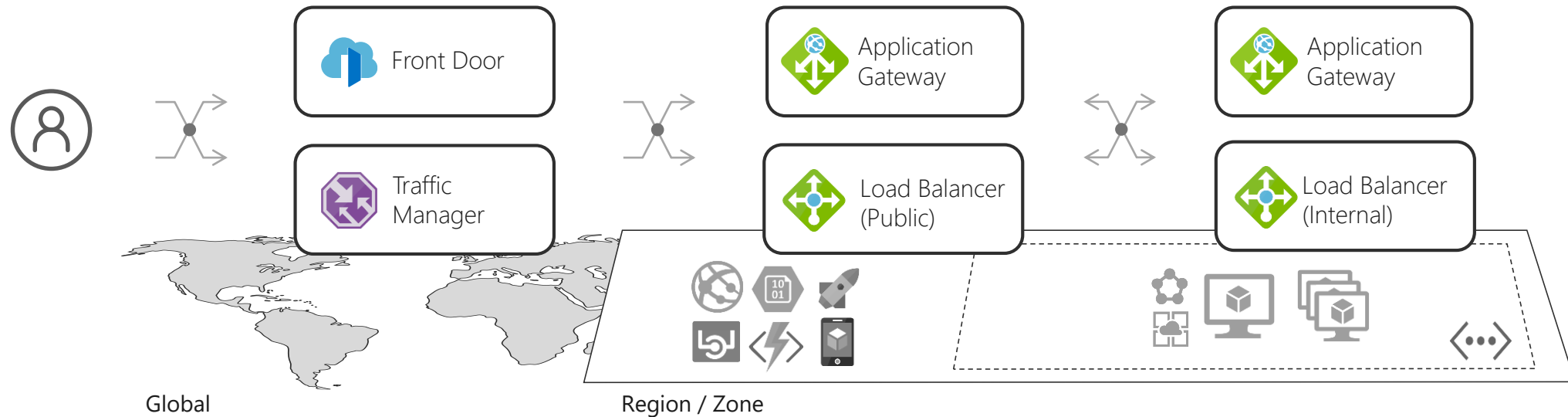
Connecting the dots



Demo!



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

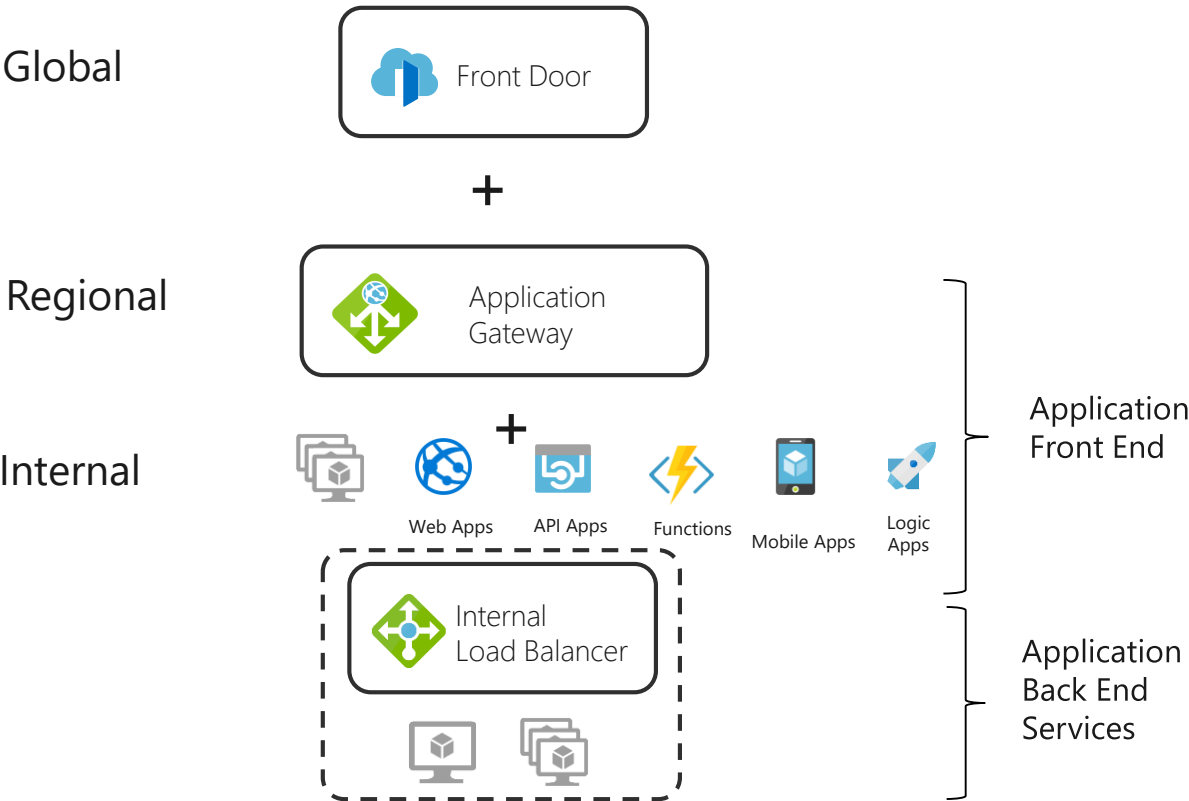
Route across and between your resources to build your regional application.

Building for global scale



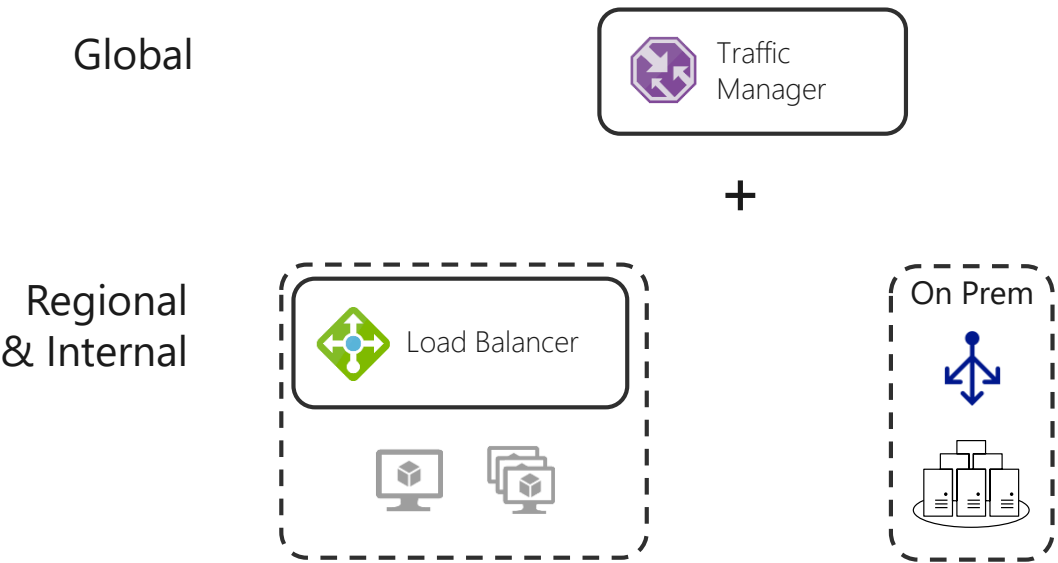
Web applications

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



Non-web applications

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



Azure Load Balancer

Cloud native network load balancer

Built-in high-availability and performance

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

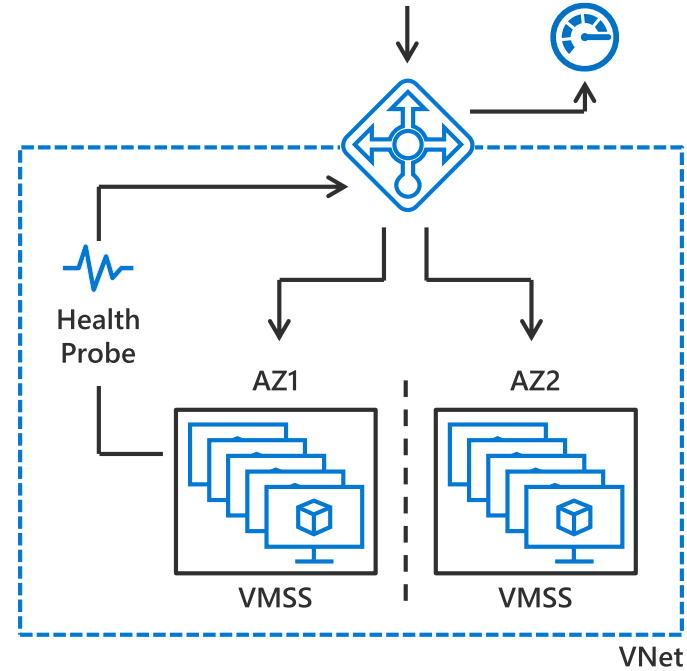
Flexible for all TCP or UDP applications

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

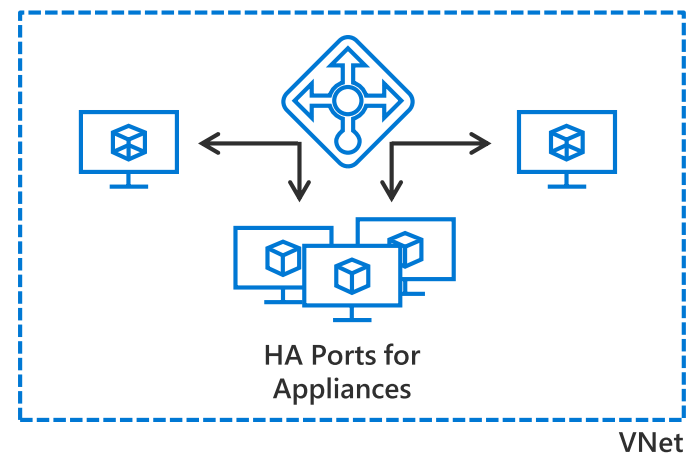
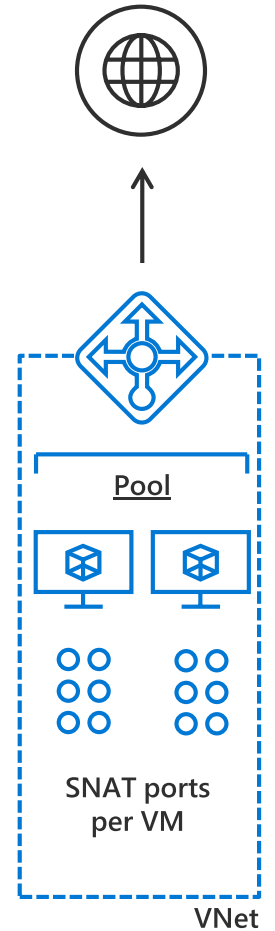
Metrics in Azure Monitor

- Multi-dimensional
- 3rd party integration

Inbound



Outbound



Application Gateway

Layer 7 load balancer for web applications

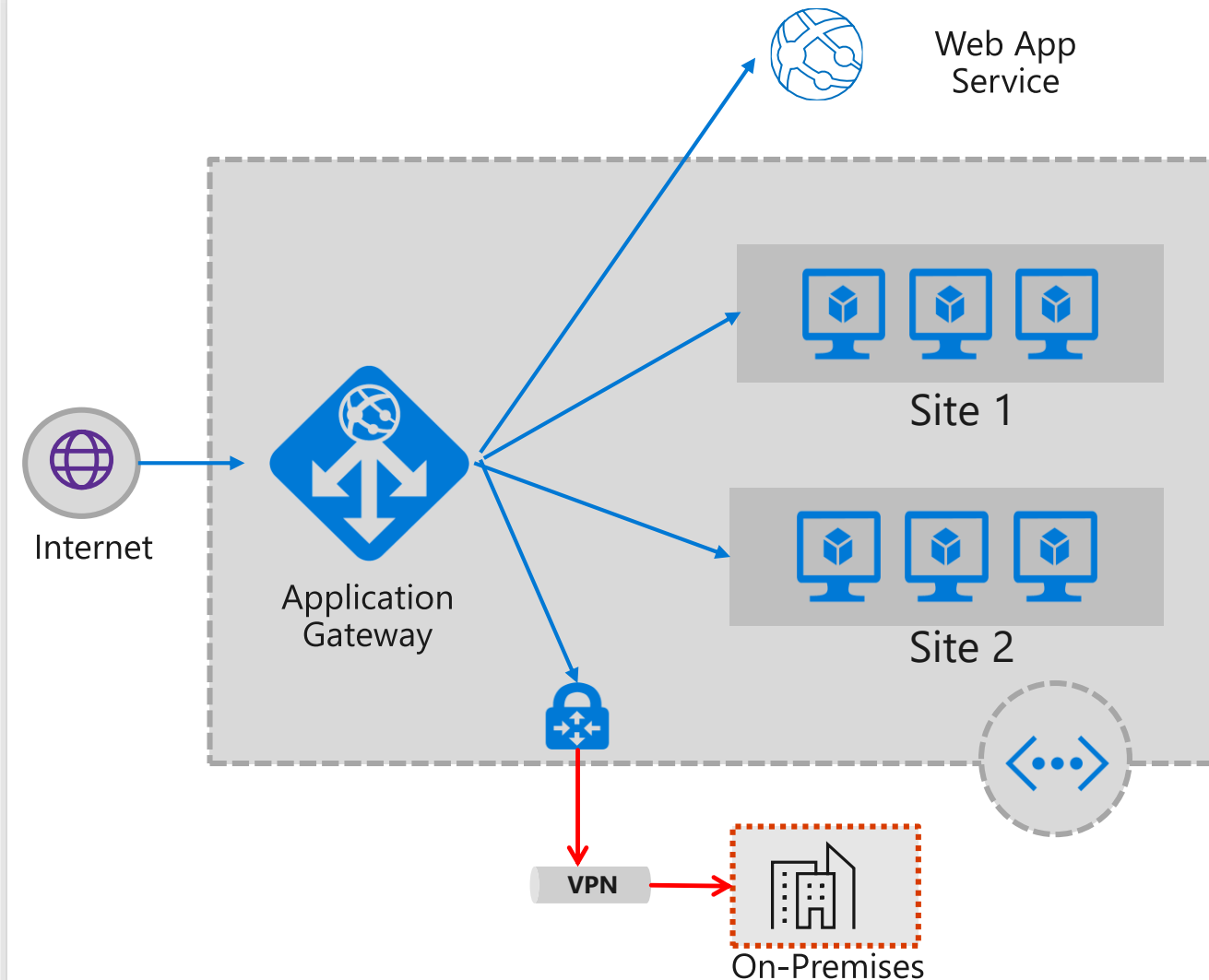
Platform managed built in high availability and scalability

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



Network Monitoring with Network Watcher

Rich set of tools to monitor all areas of applications and infrastructure

Fully integrated into Azure Monitor

Visualize



Dashboards



Network Topology

Analyze



Metrics Explorer



Traffic Analytics

Monitor & Troubleshoot



Connection Monitor



ER Monitor



VPN Troubleshoot



NSG Flow logs



Azure Monitor
Resource Health
Activity logs



Connection
Troubleshoot



Packet
Capture



Network Watcher

Respond and Integrate



Alerts



Autoscale



Functions



Event Hubs



Logic Apps



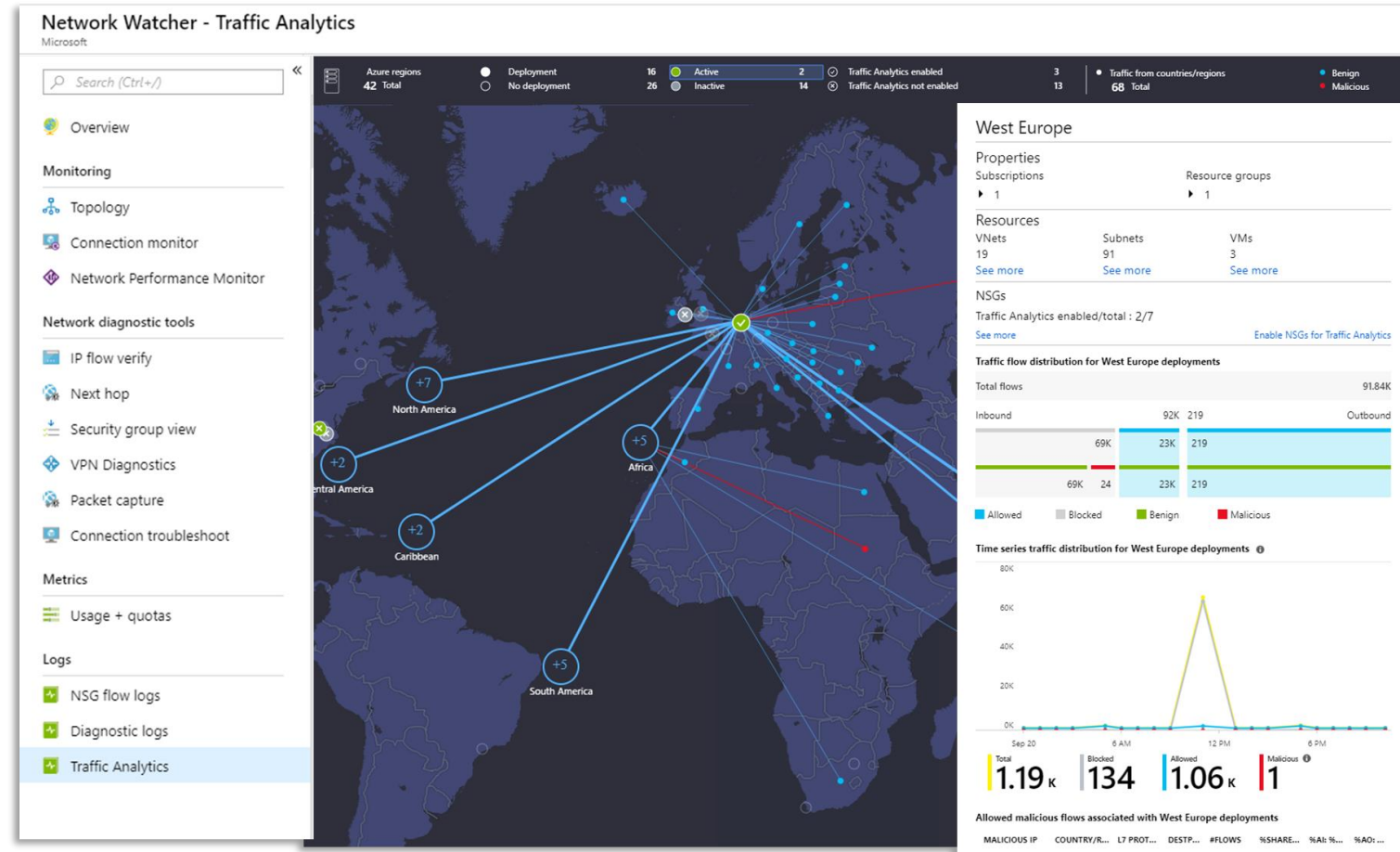
3rd Party

Traffic Analytics

Unified and Integrated Network Monitoring experience



- Monitor and troubleshoot connectivity issues
- Diagnose VPN, NSG and Routing issues
- Capture packets on your VM
- Agentless NSG Flows logs



Connection Monitor 2.0

Connectivity

Latency

Topology

Dashboard > Network Watcher - Connection monitor (Preview)

Network Watcher - Connection monitor (Preview)

Overview Create Refresh Feedback

Subscriptions: 2 of 34 selected - Don't see a subscription? [Open Directory](#) • [Subscription settings](#)

2 subscriptions 2 locations All sources All destinations Time: Current Time (9/23/2019, 11:32:30 ...)

Connection Monitor Test groups Test

Fail 2 out of 13 Warning 5 out of 13 Indeterminate 0 out of 13 Not Running 5 out of 13 Pass 1 out of 13

Search 4 selected Applied filters

Newly created Connection Monitors take 3-5 mins to get monitoring data and show up in the dashboard.

CONNECTION MONITOR	TEST CONFIGURATIONS	STATUS	LAST POLLED
▼ DemoNetworkMonitoring		⚠	9/23/2019 11:31:04 AM
▼ Connectivity_To_Outlook	HTTP_TC +1 more	⚠	9/23/2019 11:31:00 AM
CMPreviewVM(CMPreviewTest) -> outlook.office365.com	HTTP_TC	❌	9/23/2019 11:30:43 AM
WIN-8LGH868DJHC -> outlook.office365.com	HTTP_TC_networkTestConfig	✅	9/23/2019 11:31:00 AM
WIN-GTV0G9E2LCF -> outlook.office365.com	HTTP_TC_networkTestConfig	✅	9/23/2019 11:30:00 AM
WIN-8LGH868DJHC -> outlook.office365.com	HTTP_TC	✅	9/23/2019 11:31:00 AM
WIN-GTV0G9E2LCF -> outlook.office365.com	HTTP_TC	✅	9/23/2019 11:30:00 AM
CMPreviewVM(CMPreviewTest) -> outlook.office365.com	HTTP_TC_networkTestConfig	✅	9/23/2019 11:30:43 AM
▼ EastUS_To_CentralUS	HTTP_TC_ForAzureOnly_networkTestConfig +1 more	❌	9/23/2019 11:31:04 AM
CMPreviewVM(CMPreviewTest) -> CMPreviewCentralEUAf	HTTP_TC_ForAzureOnly_networkTestConfig	❌	9/23/2019 11:30:44 AM
CMPreviewVM(CMPreviewTest) -> CMPreviewCentralEUAf	HTTP_TC_ForAzureOnly	❌	9/23/2019 11:31:04 AM
▶ NetworkMonitorina		⚠	9/23/2019 11:31:04 AM

Microsoft does not take care of your network

- Azure Resources are often created with a public IP as default
- Create a secure hub to enforce centralize publishing of services
- Limit creation of public IPs with Azure policies
- Use Azure Firewall to create secure zones
- Use NSGs to Micro-segment services
- Monitor your network

AzureManagement.slack.com



Join the new Azure Management Community

<https://tinyurl.com/joinAzm>

Questions?

