

Design Network Implementation



Dan Rey
Cloud Consultant
Technical Trainer | MCT

70-535 Exam **Network** Objectives (15% - 20%)

- **Design Azure virtual networks**

- Design solutions that use Azure networking services: design for load balancing using Azure Load Balancer and Azure Traffic Manager; define DNS, DHCP, and IP strategies; determine when to use Azure Application Gateway; determine when to use multi-node application gateways, Traffic Manager and load balancers

- **Design external connectivity for Azure Virtual Networks**

- Determine when to use Azure VPN, ExpressRoute and Virtual Network Peering architecture and design; determine when to use User Defined Routes (UDRs); determine when to use VPN gateway site-to-site failover for ExpressRoute

- **Design security strategies**

- Determine when to use network virtual appliances; design a perimeter network (DMZ); determine when to use a Web Application Firewall (WAF), Network Security Group (NSG), and virtual network service tunneling

- **Design connectivity for hybrid applications**

- Design connectivity to on-premises data from Azure applications using Azure Relay Service, Azure Data Management Gateway for Data Factory, Azure On-Premises Data Gateway, Hybrid Connections, or Azure Web App's virtual private network (VPN) capability; identify constraints for connectivity with VPN; identify options for joining VMs to domains

Platform Services

Security & Management



Compute



Web and Mobile



Developer Services



Hybrid Operations



Integration



Analytics & IoT



Data



Media & CDN



Infrastructure Services

Compute



Storage



Networking



Datacenter Infrastructure **Now 50 Announced Regions** s

Design Azure Virtual Networks



Azure Virtual Network Overview

1. What Azure locations will you use to host VNets?
2. Do you need to provide communication between these Azure locations?
3. Do you need to provide communication between your Azure VNet(s) and your on-premises datacenter(s)?
4. How many Infrastructure as a Service (IaaS) VMs, cloud services roles, and web apps do you need for your solution?
5. Do you need to isolate traffic based on groups of VMs (i.e. front end web servers and back end database servers)?
6. Do you need to control traffic flow using virtual appliances?
7. Do users need different sets of permissions to different Azure resources?

A slight but worthwhile aside

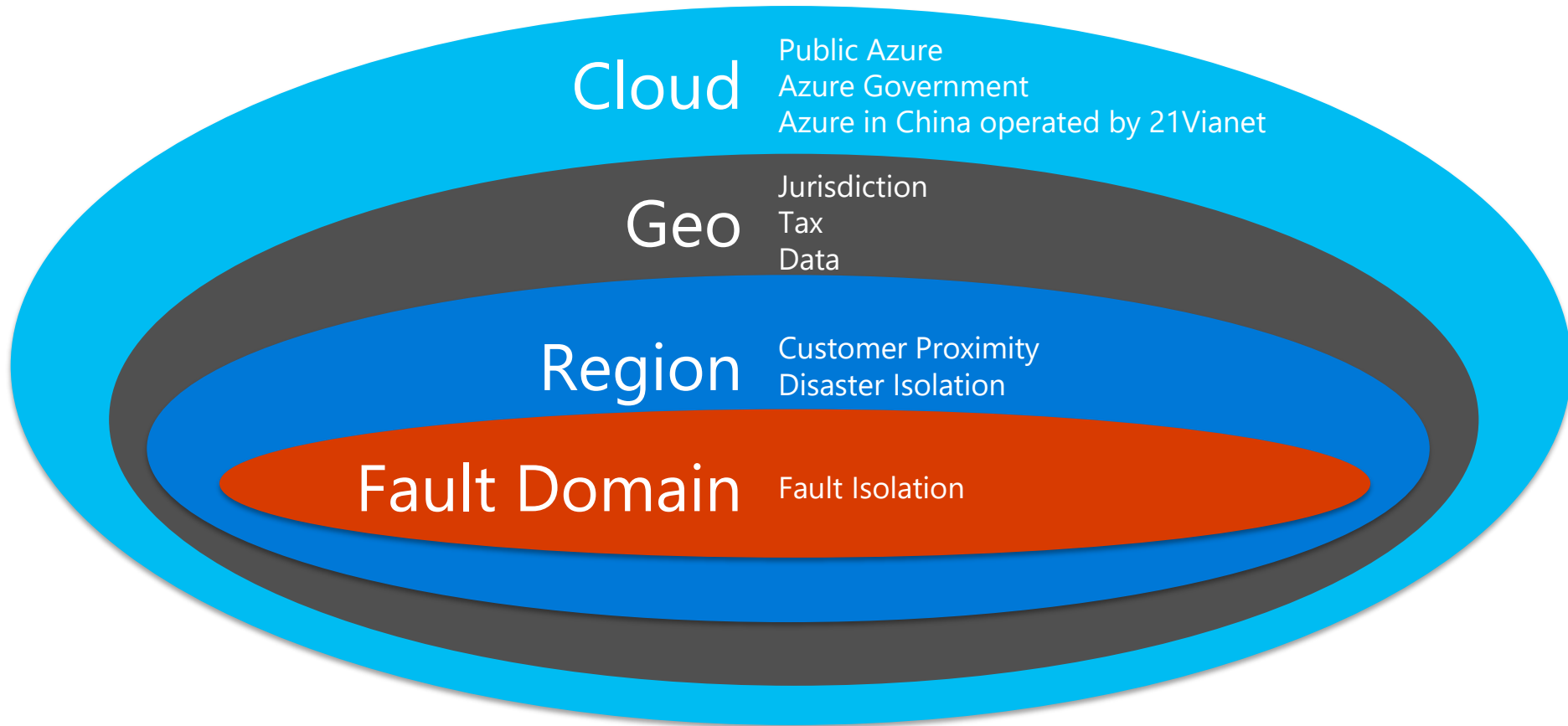


Azure Regions





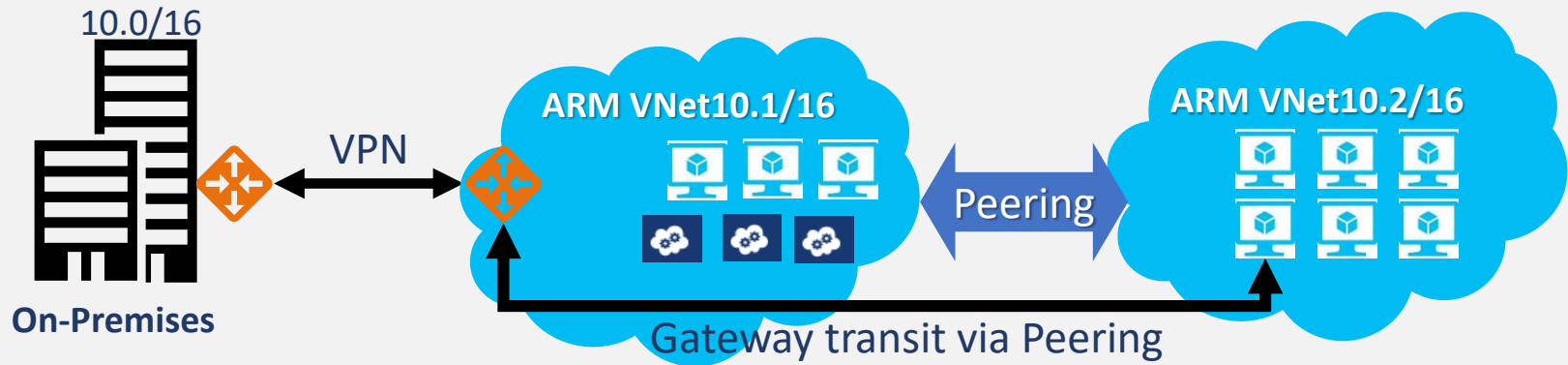
Azure Regional Hierarchy



And we're back



Azure Virtual Network Peering



- Direct and bidirectional L3 connectivity between VNet's in same region
- High throughput, low latency connectivity
- Bypass gateway, no bandwidth bottleneck
- Supports Gateway Transit (ARM-to-ARM only)
- 10/50 Vnet Peering per Virtual network
- Peer ASM and ARM VNet's
- Peer across subscriptions
- NSGs and UDRs will work across the link
- Public preview – Global Vnet Peering

Azure Network Services Overview

works at the **transport layer** (Layer 4).

It provides **network-level distribution** of traffic across instances of an application running in the same Azure data center.



Azure Load Balancer

works at the **application layer** (Layer 7) It acts as a **reverse-proxy service**, terminating the client connection and forwarding requests to back-end endpoints.



Azure Application Gateway

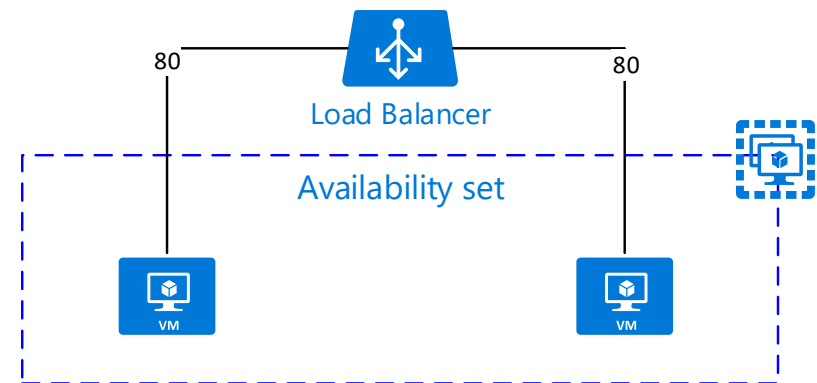
works at the **DNS level**. It uses DNS responses to direct end-user traffic to **globally distributed endpoints**. Clients then connect to those endpoints directly.



Azure Traffic Manager

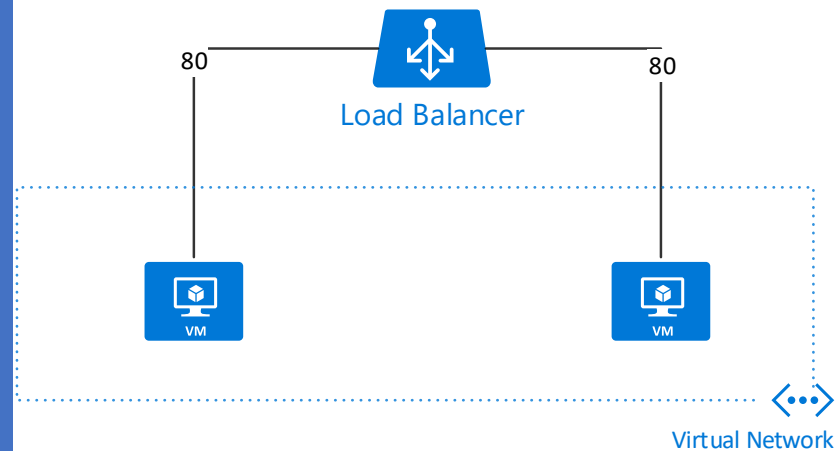
Basic Load Balancer

- Public and Private Load Balancers
- Hash-based distribution – 5-tuple Hash
 - source IP, source port, destination IP, destination port, and Protocol
- Availability Set
- Port forwarding
- Service monitoring
 - Guest agent probe
 - HTTP custom probe
 - TCP custom probe
- NAT
- Support for multiple load-balanced IP addresses for virtual machines
- 100/1000 Load balancers per subscription
- 150/250 rules per Basic Load Balancer
- 100 Backend pools with VMs on single Availability Set
- 10 Frontend IP's



Standard Load Balancer

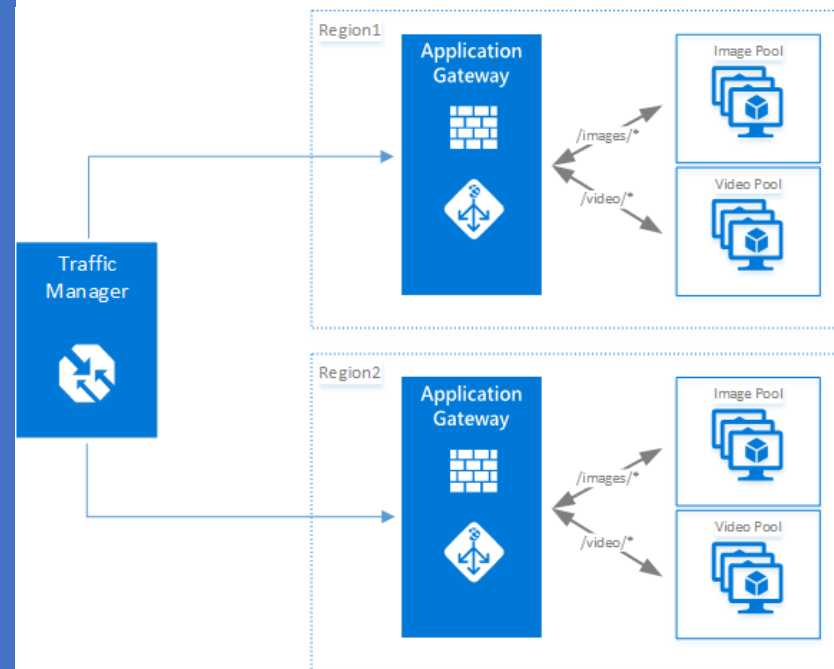
- VM need not be deployed in a Availability Set
- Cross-Zone load balancing
- Limited to region and not supported in peered networks
- NIC or Subnet level NSG is mandatory
- Migration from basic to standard SKU
- High availability using HA ports
- 100/1000 Load balancers per subscription
- 1250/1500 rules per Basic Load Balancer
- 1000 Backend pools with VMs on single VNet
- 10 Frontend IP's
- Need to signup for preview
- East US 2, Central US, North Europe, West Central US, West Europe, and Southeast Asia



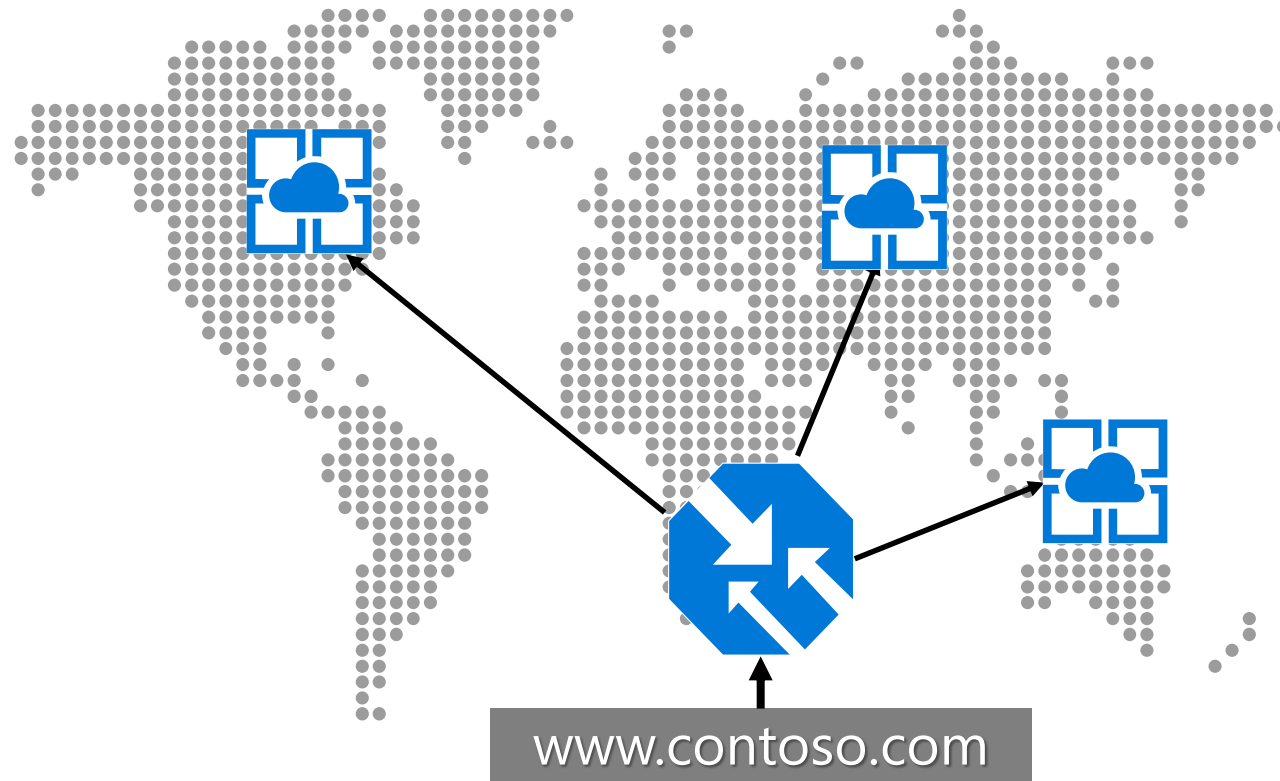
Preview

Application Gateway + WAF

- Layer 7 Load balancer (HTTP/S) with Web Application Firewall
- Ability to host multiple websites behind an Application Gateway
- Round robin distribution of incoming traffic
- cookie-based session affinity
- URL path-based routing
- End to end SSL
- HTTP to HTTPS redirect
- Protection against SQL injection, HTTP Protocol Violations
- Multi-Site Routing
- 50/100 Per Subscription
- 2 frontend IP's (Public and Private)
- 20 HTTP Listeners and 1 SSL cert and 1 site per listener
- 200 load balancing rules
- 20 backend address pools and 200 backend servers per each pool
- 10 Instances per gateway

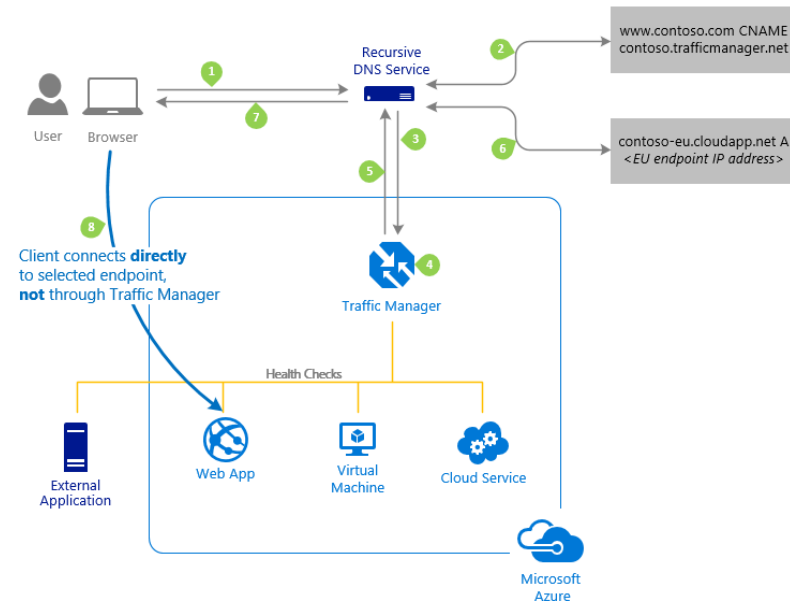


Traffic Manager



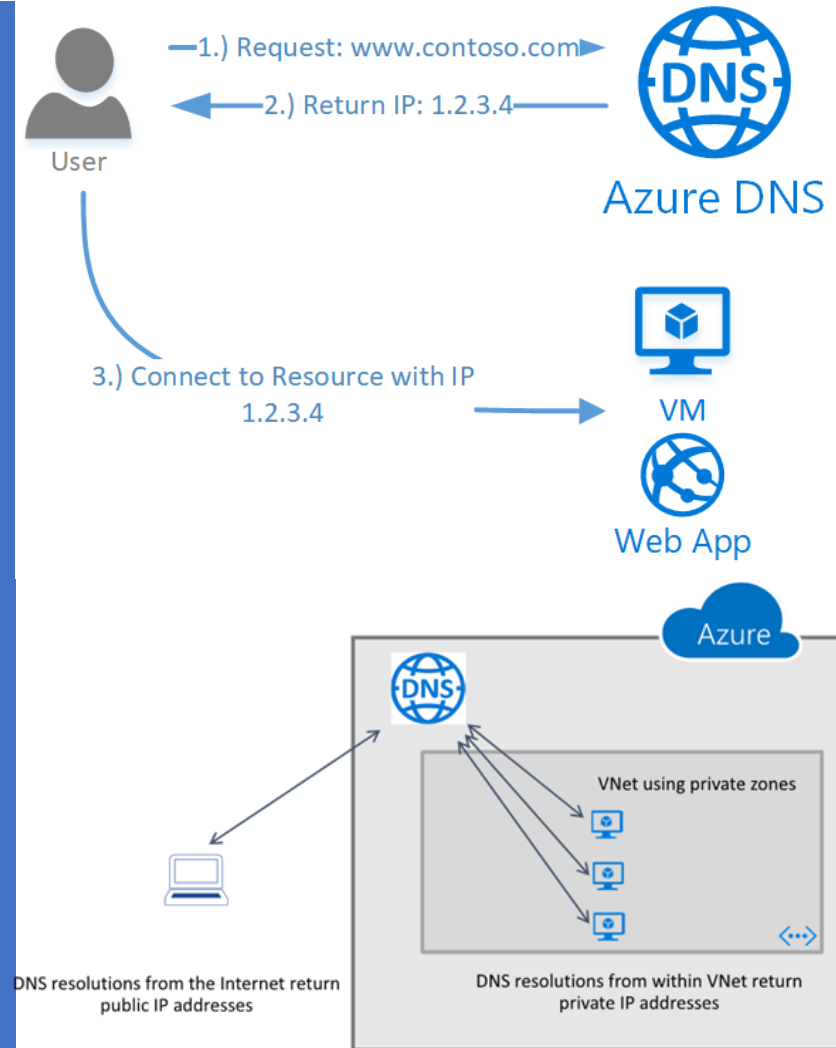
Traffic Manager

- control the distribution of user traffic for service endpoints
- Uses DNS to route traffic based on traffic routing method –
 - Priority
 - Weighted
 - Performance
 - Geographic
- Endpoint monitoring
- Benefits –
 - Improve availability of critical applications
 - Improve responsiveness for high performance applications
 - Perform service maintenance without downtime
- 100 profiles per subscription and 200 Endpoints per profile



Azure DNS









- Supports all common DNS record types
- Azure DNS for private domains – **Preview**
 - No Configuration and is Highly Available
 - DNS service to manage and resolve domain names in a virtual network
 - WINS and NetBIOS not supported
 - Removes the need of custom DNS solutions
 - Split-horizon DNS support
- Import or Export DNS zone files to and from Azure
- 99.99% SLA
- 100 DNS zones per subscription
- 5000 record sets per zone
- 20 records per record set



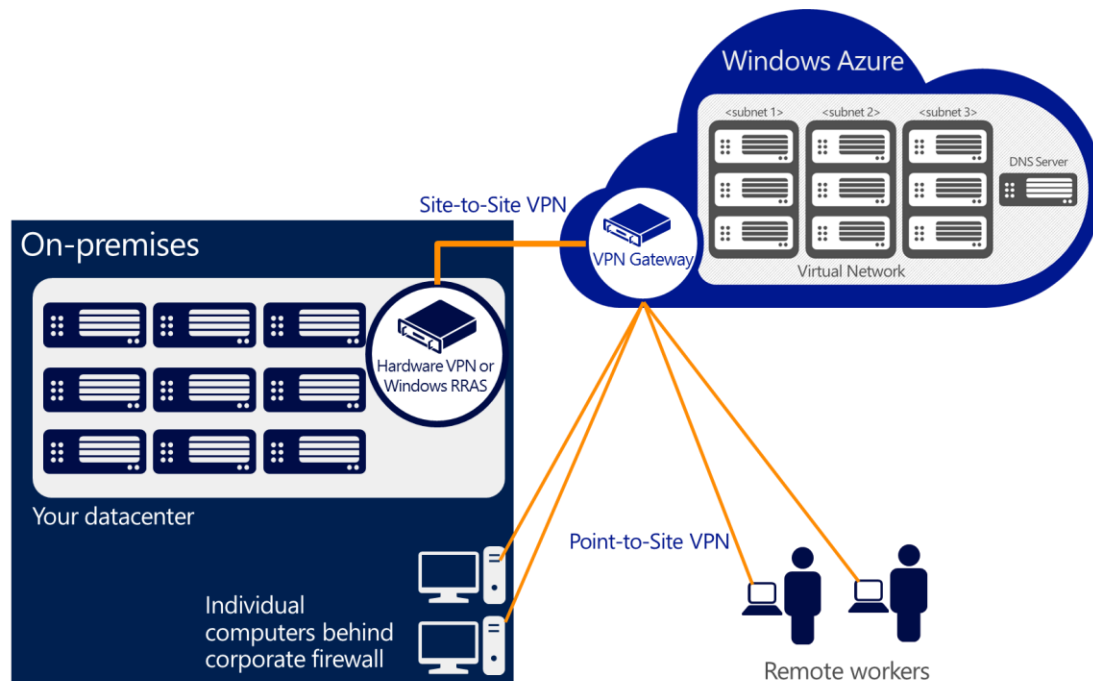
Design External Connectivity for Azure Virtual Networks



Connectivity Options and Hybrid Offerings

Cloud		Customer	Segment and workloads
	Internet Connectivity		<ul style="list-style-type: none">• Consumers• Access over public IP• DNS resolution• Connect from anywhere
	Secure point-to-site connectivity		<ul style="list-style-type: none">• Developers• POC Efforts• Small scale deployments• Connect from anywhere
	Secure site-to-site VPN connectivity		<ul style="list-style-type: none">• SMB, Enterprises• Connect to Azure compute
	ExpressRoute private connectivity		<ul style="list-style-type: none">• SMB & Enterprises• Mission critical workloads• Backup/DR, media, HPC• Connect to Microsoft services

Virtual Private Network

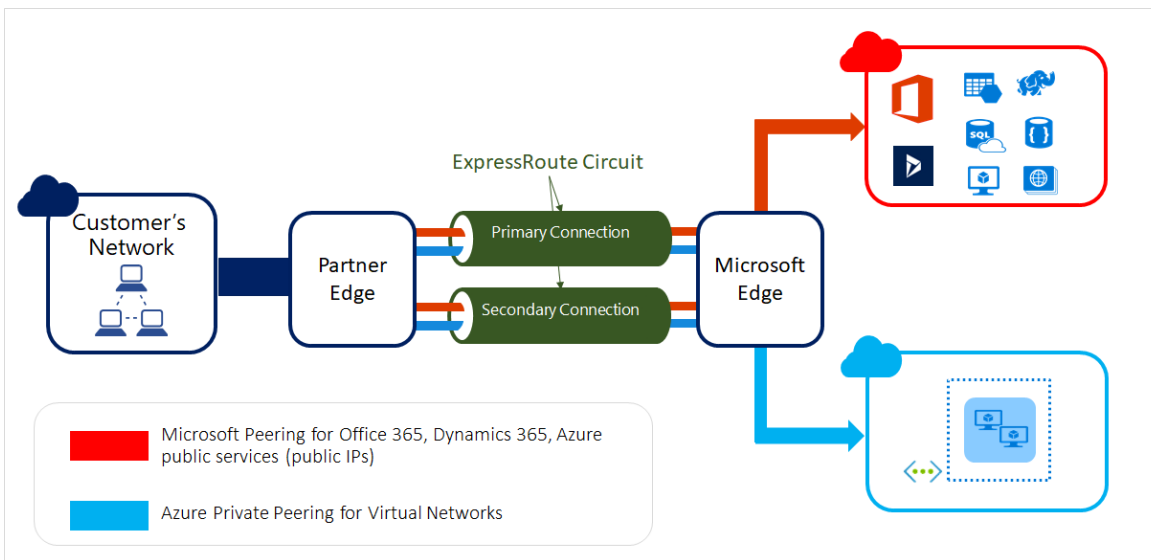


Route Based SKU	S2S/VNet-to-VNet Tunnels	P2S Connections	Aggregate Throughput Benchmark
VpnGw1	Max. 30	Max. 128	650 Mbps
VpnGw2	Max. 30	Max. 128	1 Gbps
VpnGw3	Max. 30	Max. 128	1.25 Gbps
Basic	Max. 10	Max. 128	100 Mbps

At a high level, most hybrid configurations require 5 resources:

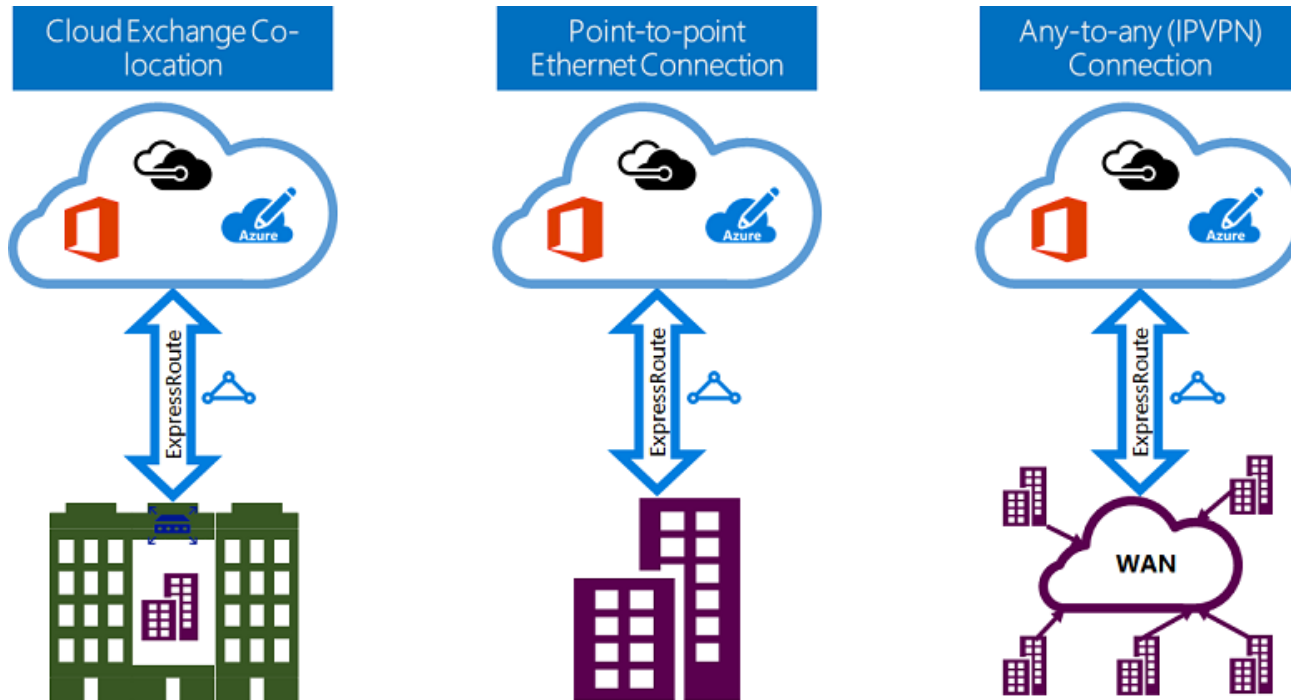
- VNET
- Gateway Subnet
- Virtual Network Gateway (Route/Policy Based)
- Local Network Gateway

Express Route

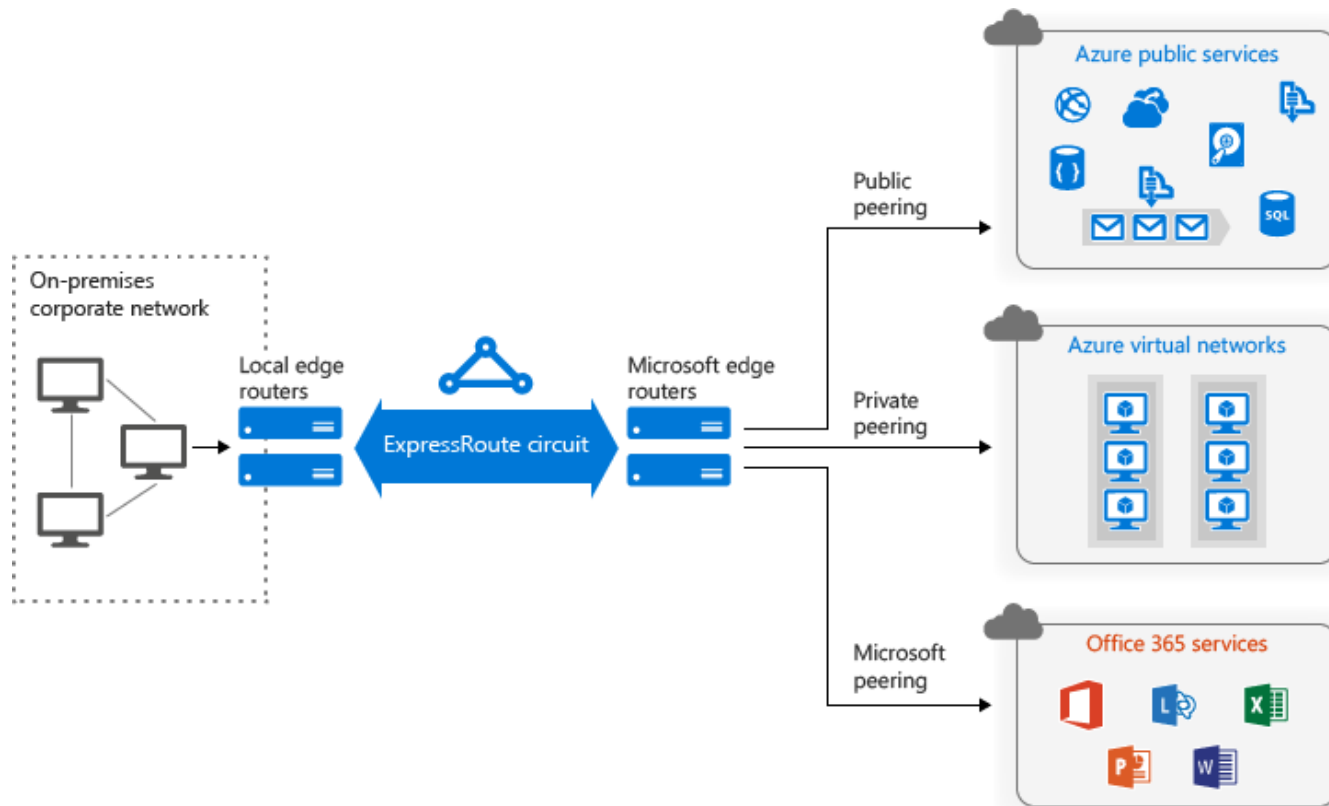


- Layer 3 connectivity between your on-premises and Azure
- Dynamic routing between your network and Microsoft by leveraging BGP

Express Route Connectivity Models



Express Route: Routing Domains (Peerings)

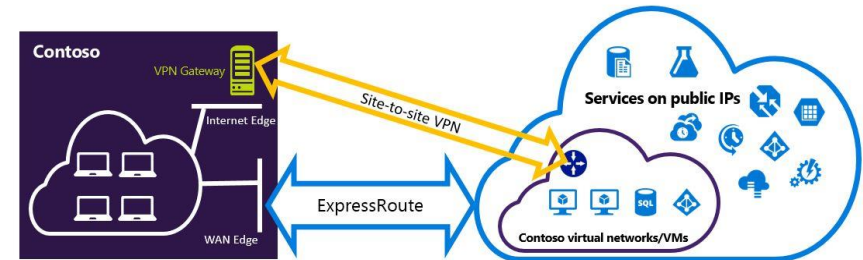
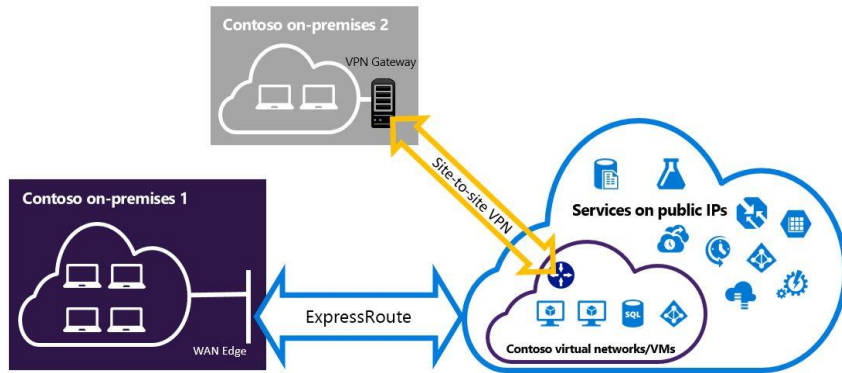


Express Route Standard vs Premium Add-on

Number of Routes	Express Route	Premium add-on
Private Peering	4,000	10,000
Public Peering	200	200
Microsoft Peering	200	200

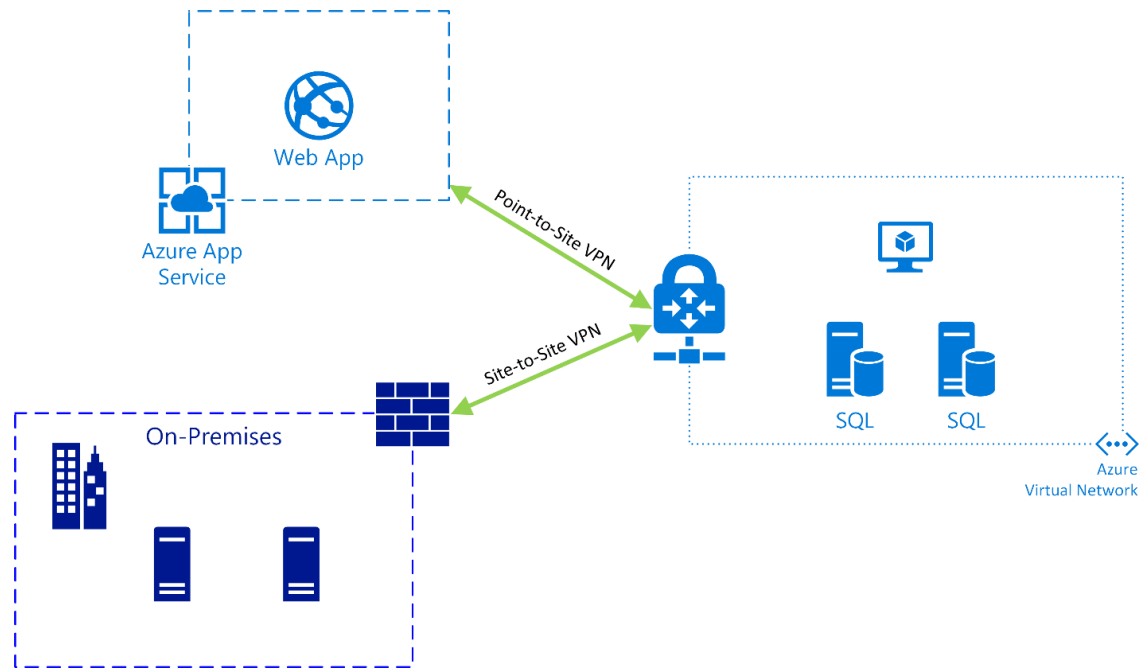
Global connectivity for services - An ExpressRoute circuit created in any region (excluding Azure China, Azure Germany, and Azure Government cloud) will have access to resources across any other region in the world.

Circuit Size	Number of VNet links for standard	Number of VNet Links with Premium add-on
50 Mbps	10	20
100 Mbps	10	25
200 Mbps	10	25
500 Mbps	10	40
1 Gbps	10	50
2 Gbps	10	60
5 Gbps	10	75
10 Gbps	10	100

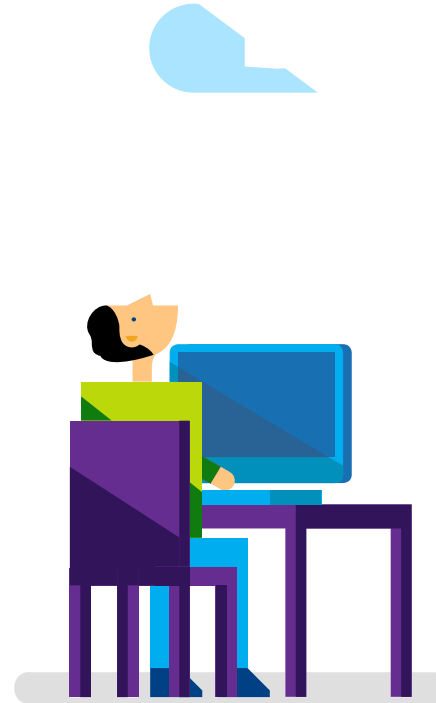


Express Route and Site-to-Site Co-Exist

Integrating Web App with Virtual Network

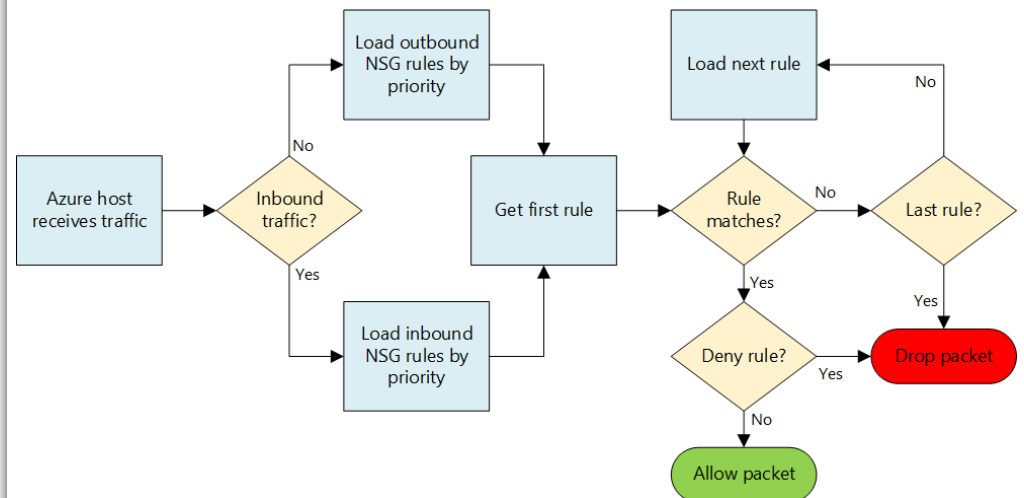


Design Security Strategies



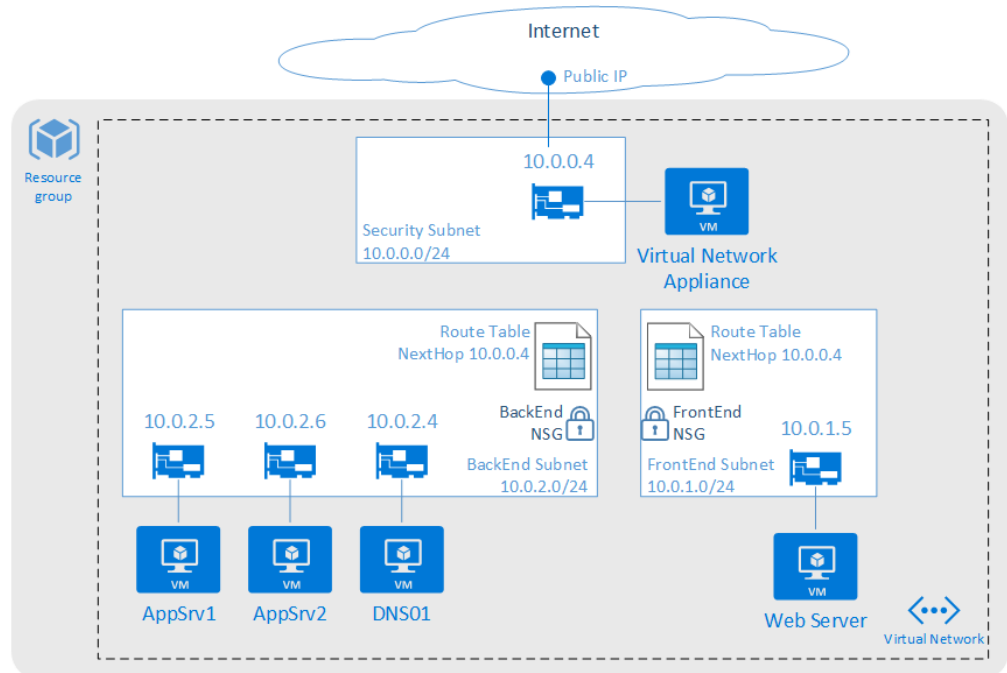
Network Security Groups

- Control inbound and outbound traffic on a NIC or subnet level
- Configure rules in NSG
 - Name
 - Source address
 - Source port
 - Protocol (TCP/UDP/ICMP)
 - Destination address
 - Destination port
 - Direction
 - Action (Allow/Deny)
- Augmented Rules
- 100/200 NSG's per subscription
- 200/400 Rules per NSG



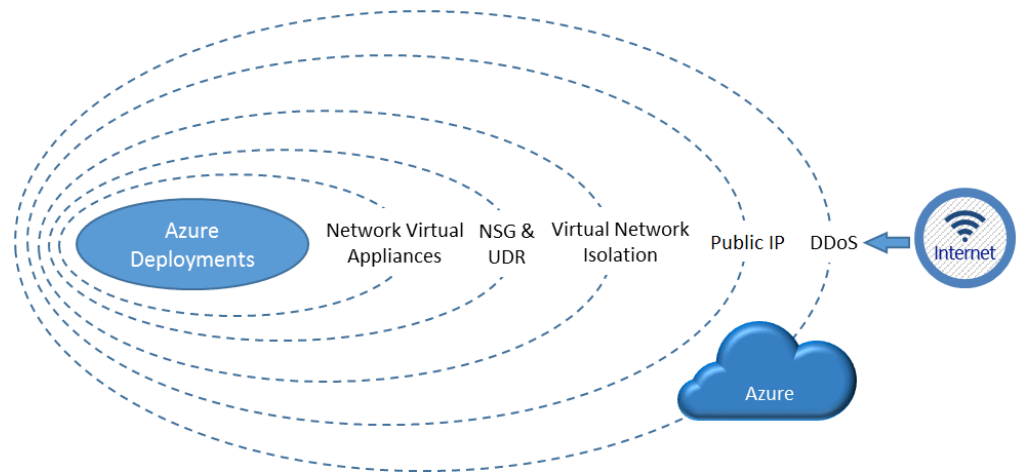
Route Tables

- User defined routes
- Routes to overwrite Azure system routes
- Associated to subnets
- Specify next hop
 - Virtual Appliance
 - Virtual Network Gateway
 - None
 - Virtual Network
 - Internet
- Configure routes in route table
 - Route Name
 - Address Prefix (Destination Address)
 - Next hop type
 - Next hop address (Virtual Appliance)
- 100/200 Route Tables per subscription
- 100/400 routes per Route Table



Azure DDOS Protection

- Two tiers of DDOS protection
 - Basic – Free with Azure
 - Standard – Preview
- Always-on monitoring and real-time mitigation
- Standard DDOS will help you protect resources in a virtual Network and also Public IP's associated to Azure VMs.
- Mitigates attacks like -
 - Volumetric attacks
 - Protocol attacks
 - Application layer attacks
- Automatic DDOS mitigation



Thank You
