

Design Network Implementation

Design Network Implementation

- **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

What is Azure Networking?

- Networking
 - Virtual Networks
 - Network Security Groups
- Hybrid:
 - Extend on-premises
 - VPN
 - Point-to-Site
 - Site-to-Site
 - ExpressRoute
- Networking Services:
 - Azure Load Balancer
 - Azure Application Gateway
 - Azure Traffic Manager
 - DNS
 - DHCP
 - IP Addresses
 - UDRs
- * **Bold Red text are key points**

Networking: Virtual Networks

- Isolated
- 50/500 Virtual Networks per Region per Subscription
- **Up to 500K Concurrent TCP connections per VM**
- Up to 1000 Subnets. Special: GatewaySubnet
- 300/10,000 NICs per region per sub
- Internet Connected by default
- Connectivity – to each other via Peering, or to on-prem via VPN, ExpressRoute
- Bound to a single region
- Use Public IP address Ranges and Private IP Address ranges
- Some IP address Ranges are not allowed:
 - 224.0.0.0/4 (Multicast)
 - 255.255.255.255/32 (Broadcast)
 - 127.0.0.0/8 (loopback)
 - 169.254.0.0/16 (link-local)
 - 168.63.129.16/32 (Internal DNS)
 - <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-public-ip-within-vnet>

Networking: Virtual Networks

VNet properties

Property	Description	Constraints
name	VNet name	String of up to 80 characters. May contain letters, numbers, underscore, periods, or hyphens. Must start with a letter or number. Must end with a letter, number, or underscore. Can contains upper or lower case letters.
location	Azure location (also referred to as region).	Must be one of the valid Azure locations.
addressSpace	Collection of address prefixes that make up the VNet in CIDR notation.	Must be an array of valid CIDR address blocks, including public IP address ranges.
subnets	Collection of subnets that make up the VNet	see the subnet properties table below.
dhcpOptions	Object that contains a single required property named dnsServers .	
dnsServers	Array of DNS servers used by the VNet. If no server is specified, Azure internal name resolution is used.	Must be an array of up to 10 DNS servers, by IP address

Subnet Properties

Property	Description	Constraints
name	Subnet name	String of up to 80 characters. May contain letters, numbers, underscore, periods, or hyphens. Must start with a letter or number. Must end with a letter, number, or underscore. Can contains upper or lower case letters.
location	Azure location (also referred to as region).	Must be one of the valid Azure locations.
addressPrefix	Single address prefix that make up the subnet in CIDR notation	Must be a single CIDR block that is part of one of the VNet's address spaces.
networkSecurityGroup	NSG applied to the subnet	
routeTable	Route table applied to the subnet	
ipConfigurations	Collection of IP configuration objects used by NICs connected to the subnet	

Networking: Network Security Groups

- 100/400 NSGs per region per sub
- Rules per NSG: 200/500
- Rules to allow/deny traffic
- Rules for inbound/outbound
- Can be associated with Subnets and/or directly to NICs attached to VMs.
- Rules are based on Protocol, Source Port Range, Destination Port Range, Source Address Prefix, Destination Address Prefix
- Default Tags for categories of IP addresses:
 - **VirtualNetwork**
 - **AzureLoadbalancer**
 - **Internet**

- **Default Rules**

- **Inbound**

- **Allow Vnet, Allow LoadBalancer, Deny All Inbound**

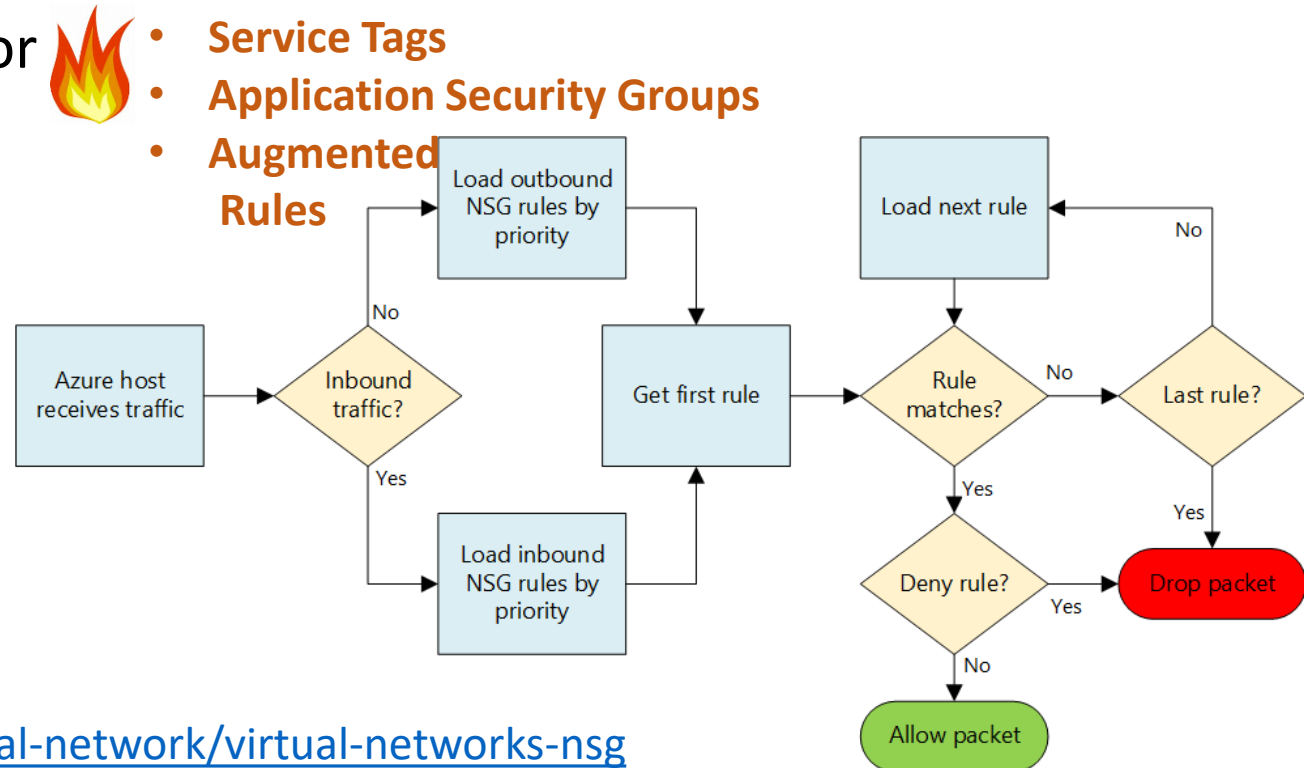
- **Outbound**

- **Allow Vnet, Allow Internet, Deny All Outbound**

- **Service Tags**

- **Application Security Groups**

- **Augmented Rules**



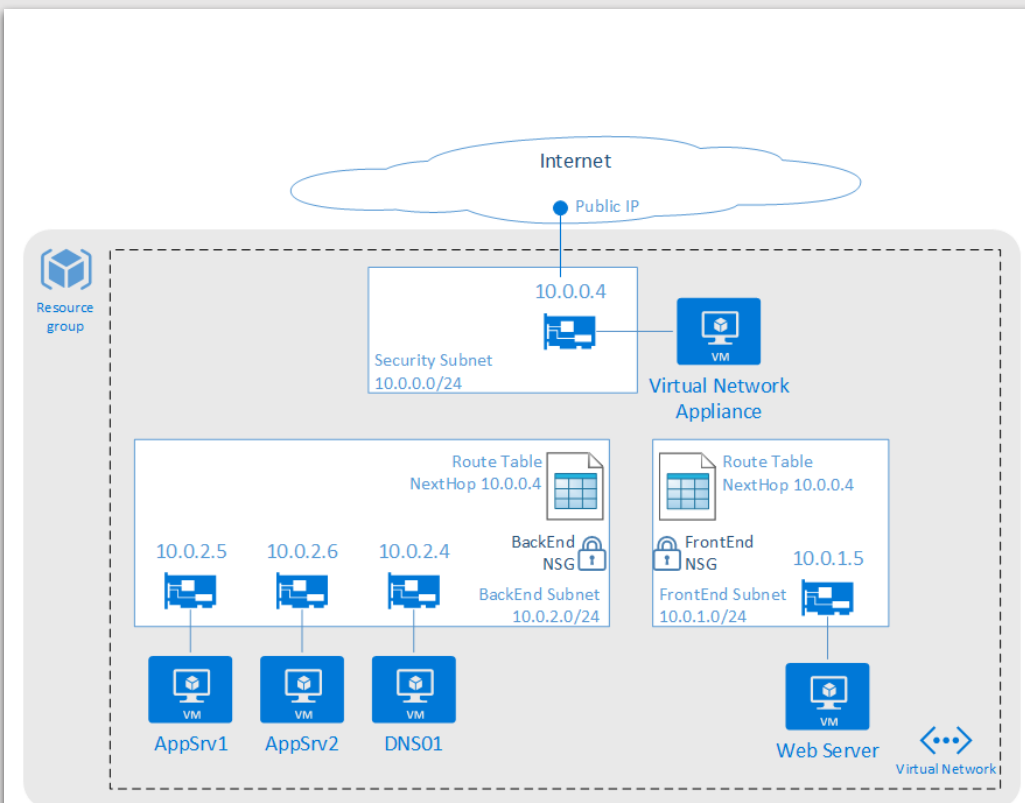
<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>

Networking: Network Security Groups

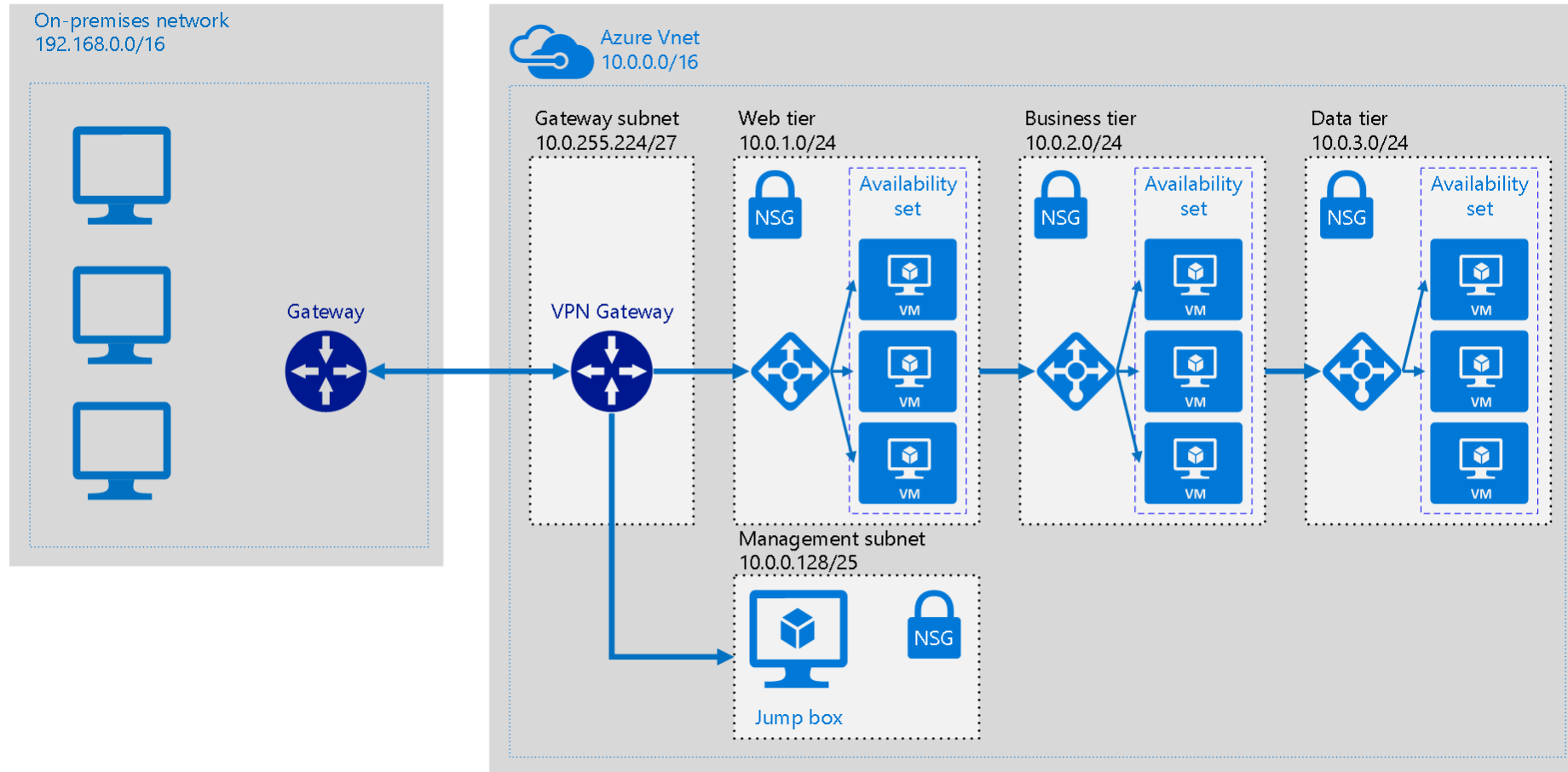
Property	Description	Constraints	Considerations
Protocol	Protocol to match for the rule.	TCP, UDP, or *	Using * as a protocol includes ICMP (East-West traffic only), as well as UDP and TCP, and may reduce the number of rules you need. At the same time, using * might be too broad an approach, so it's recommended that you use * only when necessary.
Source port range	Source port range to match for the rule.	Single port number from 1 to 65535, port range (example: 1-65635), or * (for all ports).	Source ports could be ephemeral. Unless your client program is using a specific port, use * in most cases. Try to use port ranges as much as possible to avoid the need for multiple rules. Multiple ports or port ranges cannot be grouped by a comma.
Destination port range	Destination port range to match for the rule.	Single port number from 1 to 65535, port range (example: 1-65535), or * (for all ports).	Try to use port ranges as much as possible to avoid the need for multiple rules. Multiple ports or port ranges cannot be grouped by a comma.
Source address prefix	Source address prefix or tag to match for the rule.	Single IP address (example: 10.10.10.10), IP subnet (example: 192.168.1.0/24), default tag , or * (for all addresses).	Consider using ranges, default tags, and * to reduce the number of rules.
Destination address prefix	Destination address prefix or tag to match for the rule.	Single IP address (example: 10.10.10.10), IP subnet (example: 192.168.1.0/24), default tag , or * (for all addresses).	Consider using ranges, default tags, and * to reduce the number of rules.
Direction	Direction of traffic to match for the rule.	Inbound or outbound.	Inbound and outbound rules are processed separately, based on direction.
Priority	Rules are checked in the order of priority. Once a rule applies, no more rules are tested for matching.	Number between 100 and 4096.	Consider creating rules jumping priorities by 100 for each rule to leave space for new rules you might create in the future.
Access	Type of access to apply if the rule matches.	Allow or deny.	Keep in mind that if an allow rule is not found for a packet, the packet is dropped.

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



Hybrid: Extend On Premises



Hybrid: Extend On Premises

- At a high level, most hybrid configurations require 5 resources:
 - **VNET**
 - **Gateway Subnet**
 - **Azure VNET Gateway**
 - **“Local” Gateway**
 - **Connection**
- Planning a Hybrid Networking Architecture:
 - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-plan-design>

Hybrid: VPN

- VPN
 - Types
 - Policy-Based (Static Routing)
 - Route-Based (Dynamic Routing)
 - Learn more: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/>
 - SKUs
 - Basic (99.9% SLA)
 - Standard (99.95% SLA)
 - High Performance (99.95% SLA)

	VPN Gateway throughput (1)	VPN Gateway max IPsec tunnels (2)	ExpressRoute Gateway throughput	VPN Gateway and ExpressRoute coexist
Basic SKU (3)(5)(6)	100 Mbps	10	500 Mbps (6)	No
Standard SKU (4)(5)	100 Mbps	10	1000 Mbps	Yes
High Performance SKU (4)	200 Mbps	30	2000 Mbps	Yes

Hybrid: VPN

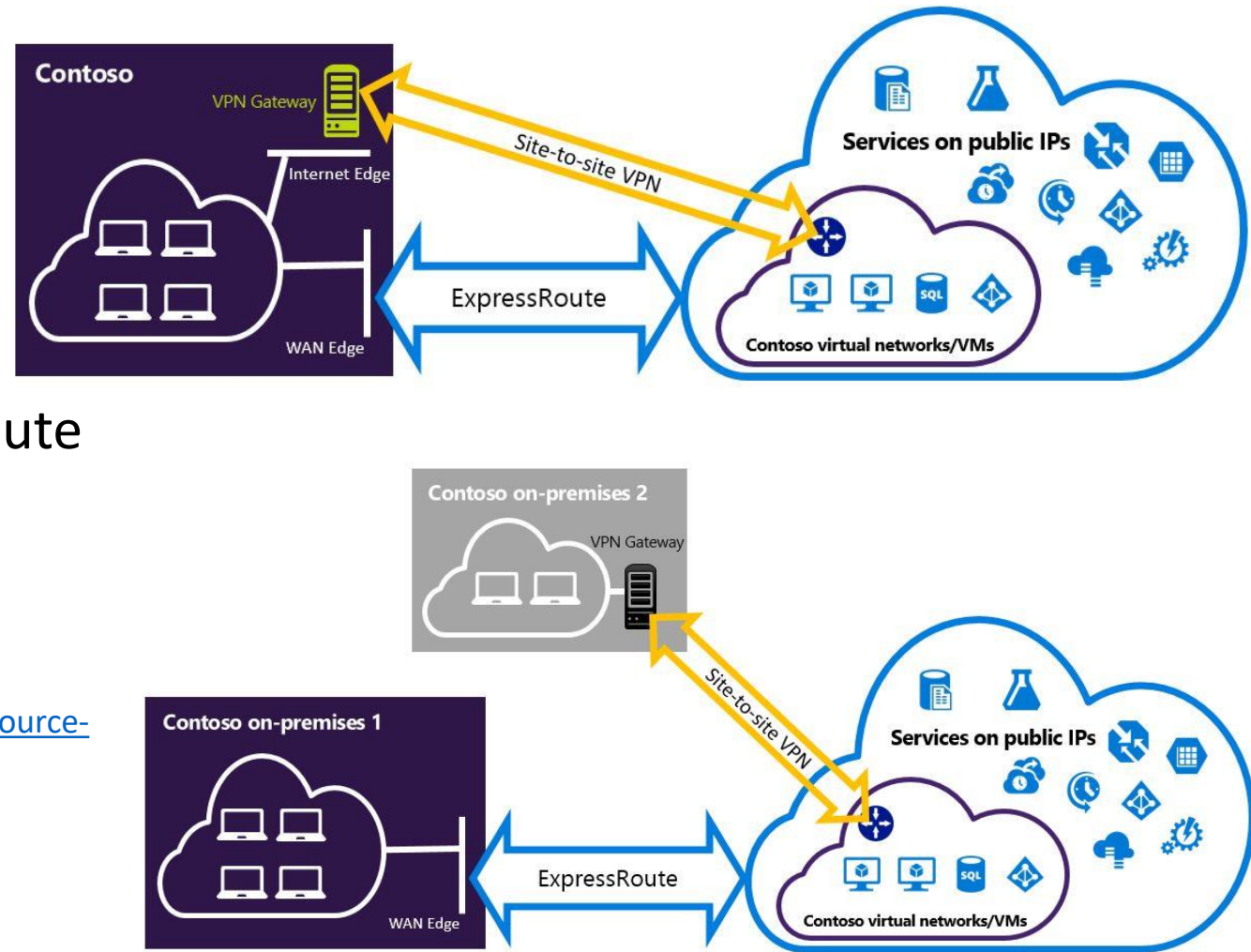
	PolicyBased Basic VPN Gateway	RouteBased Basic VPN Gateway	RouteBased Standard VPN Gateway	RouteBased High Performance VPN Gateway
Site-to-Site connectivity (S2S)	PolicyBased VPN configuration	RouteBased VPN configuration	RouteBased VPN configuration	RouteBased VPN configuration
Point-to-Site connectivity (P2S)	Not supported	Supported (Can coexist with S2S)	Supported (Can coexist with S2S)	Supported (Can coexist with S2S)
Authentication method	Pre-shared key	Pre-shared key for S2S connectivity, Certificates for P2S connectivity	Pre-shared key for S2S connectivity, Certificates for P2S connectivity	Pre-shared key for S2S connectivity, Certificates for P2S connectivity
Maximum number of S2S connections	1	10	10	30
Maximum number of P2S connections	Not supported	128	128	128
Active routing support (BGP)	Not supported	Not supported	Supported	Supported

Hybrid: VPN

- On-Premises VPN appliances
 - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-device>
- Point-to-Site, Site-to-Site, ExpressRoute
 - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices>
- ExpressRoute & Site-to-Site Co-Exist
 - <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>

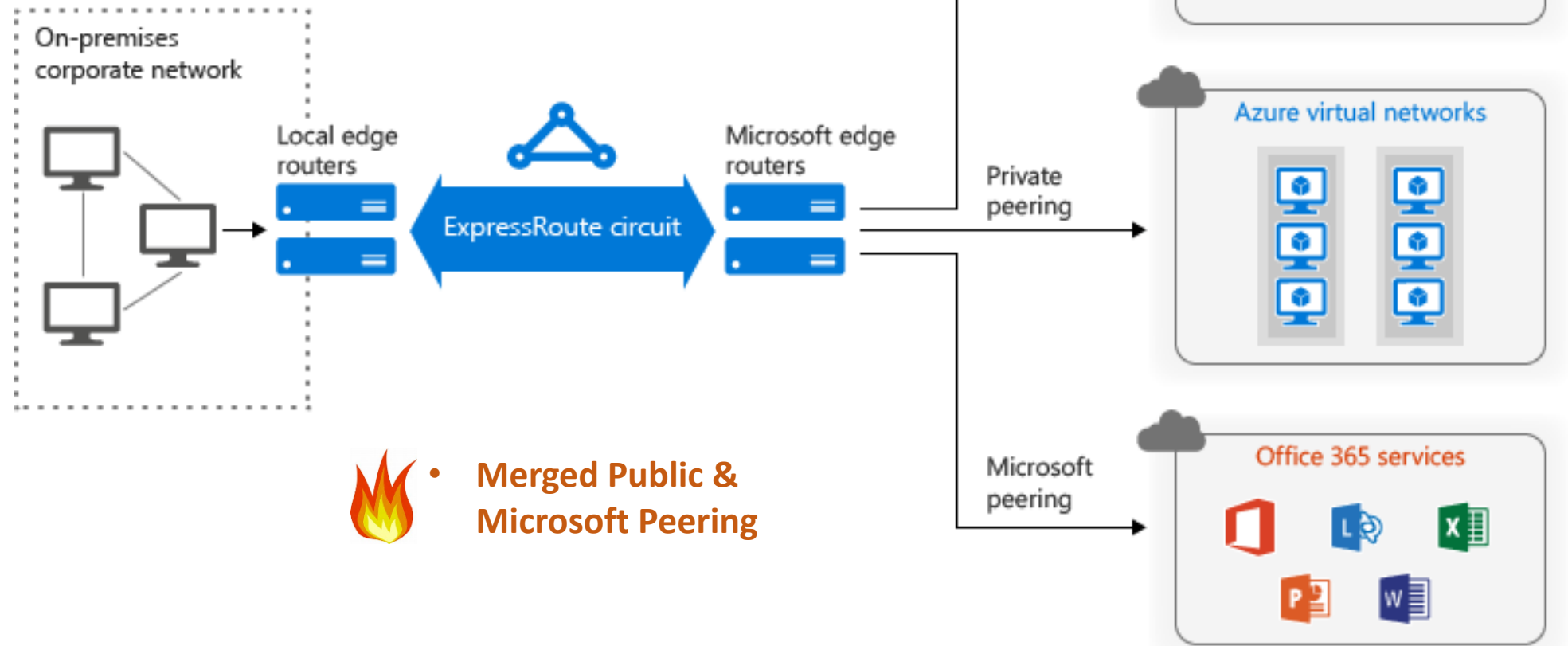


- **Point-to-Site supports Mac clients**



Hybrid: Express Route

- Express Route



Express Route Standard vs Premium Add-on

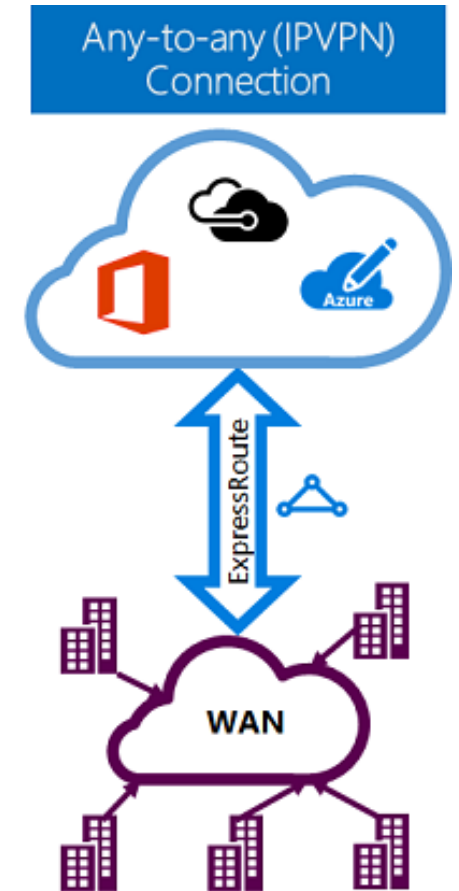
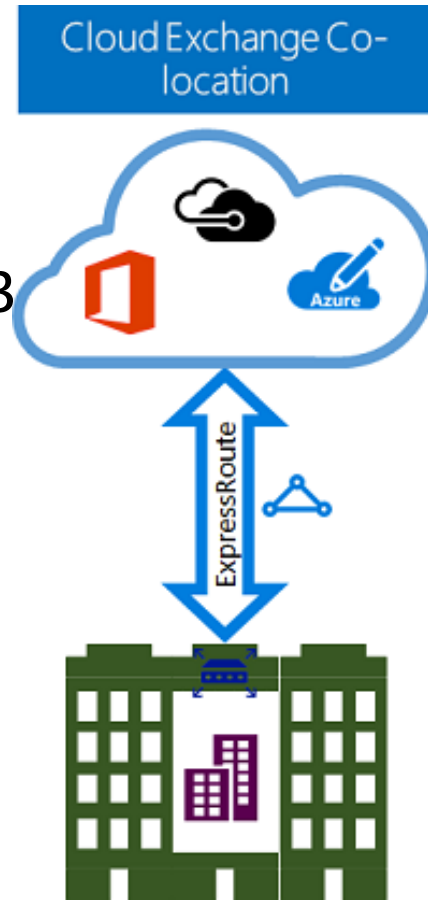
Number of Routes	Express Route	Premium add-on
Private Peering	4,000	10,000
Public Peering	200	200
Microsoft Peering	200	200

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

Hybrid: ExpressRoute

- ExpressRoute
 - Layer 2 / Layer 3











<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-connectivity-models>

Hybrid: ExpressRoute (99.95% SLA)

- 10 ER circuits per region per sub (ARM)
- Min/Max Circuit Size = 50 Mbps / 10 Gbps
- 10 VNet Links per circuit
- 2 Plans (Metered, Unlimited), Multiple Port Speeds
 - <https://azure.microsoft.com/en-us/pricing/details/expressroute/>
- ExpressRoute Premium Add-on
 - Increased route limits for public and private peering from 4,000 routes to 10,000 routes.
 - 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.
 - Without Premium Add-On, ER circuit limited to geo-political area
 - Increased number of VNet links per ExpressRoute circuit from 10 to a larger limit (depending on the bandwidth of the circuit). **20 - 100**
- ExpressRoute videos
 - <https://channel9.msdn.com/Shows/Azure-Friday/Azure-Hybrid-Networking-101>
 - <https://channel9.msdn.com/Shows/Azure-Friday/Azure-Hybrid-Networking-201>

Hybrid Network Design Considerations

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

You want to let your mobile workers connect to a Network in Azure so they can access an internal only system. What VPN solution should you deploy?

- 1) Vnet to Vnet
- 2) Point to Site
- 3) Site to Site
- 4) ExpressRoute

You want to let your mobile workers connect to a Network in Azure so they can access an internal only system. What VPN solution should you deploy?

- 1) Vnet to Vnet
- 2) Point to Site**
- 3) Site to Site
- 4) ExpressRoute

Network Services

Network Services: Load Balancer

- **Hash-based distribution**
 - 5 tuple and 2 or 3 tuple
- **Port forwarding (e.g. Port 80 to Port 81)**
- Automatic Reconfiguration
- Service Monitoring
 - Guest probe
 - HTTP custom probe
 - TCP custom probe
- **NAT Capability**
- Source NAT (share same VIP)
- 100 per subscription
- 150 rules per Load Balancer



- **Supports 1000 VMs**
- **Availability Zones**
- **HA Ports**



- 5-tuple hash
- Source IP
 - Source Port
 - Destination IP
 - Destination Port
 - Protocol



Private IP, port



VM

Private IP, port



VM

Private IP, port



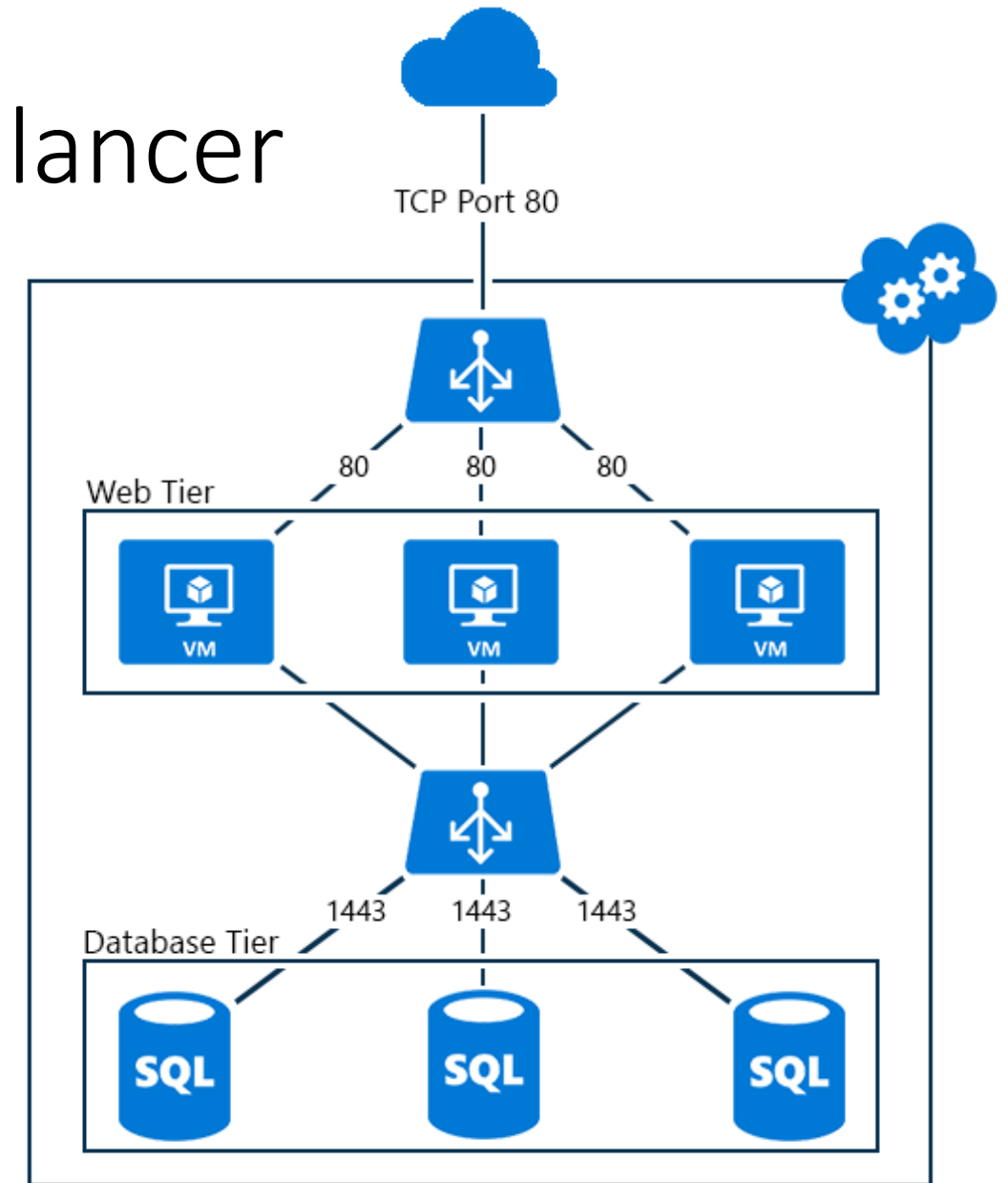
VM

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

Network Services: Load Balancer

- Public / Internet Facing Load Balancer
- Internal Load Balancer
- Outbound traffic & Source NAT

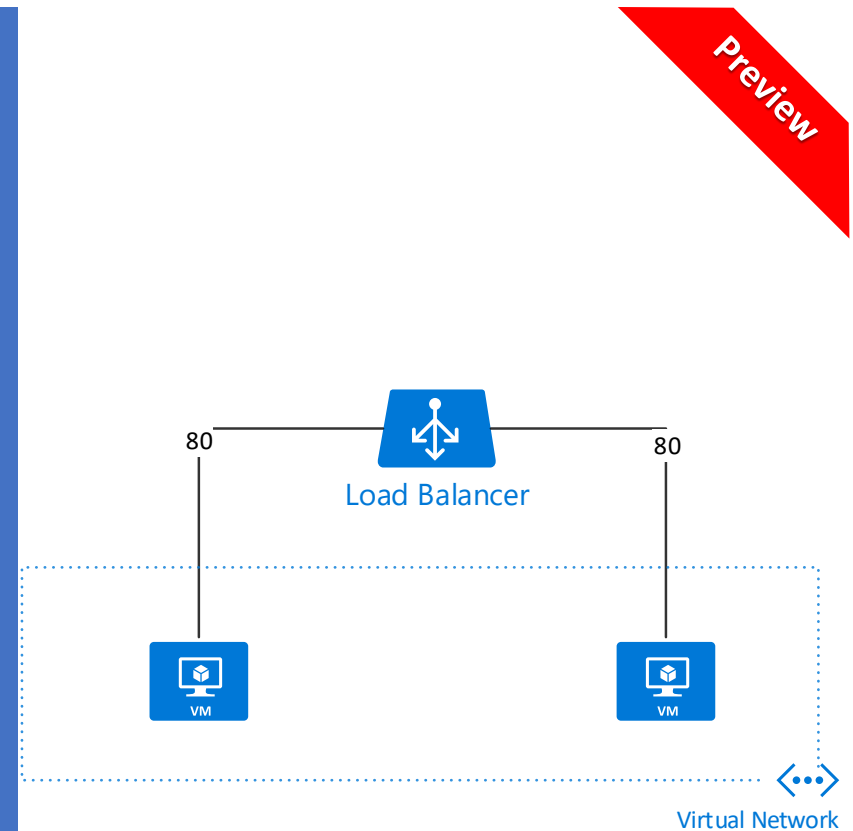
Scenario	Method	Note
Standalone VM (no load balancer, no Instance Level Public IP address)	Default SNAT	Azure associates a public IP address for SNAT
Load-balanced VM (no Instance Level Public IP address on VM)	SNAT using the load balancer	Azure uses a public IP address of the Load Balancer for SNAT
VM with Instance Level Public IP address (with or without load balancer)	SNAT is not used	Azure uses the public IP assigned to the VM



<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections>

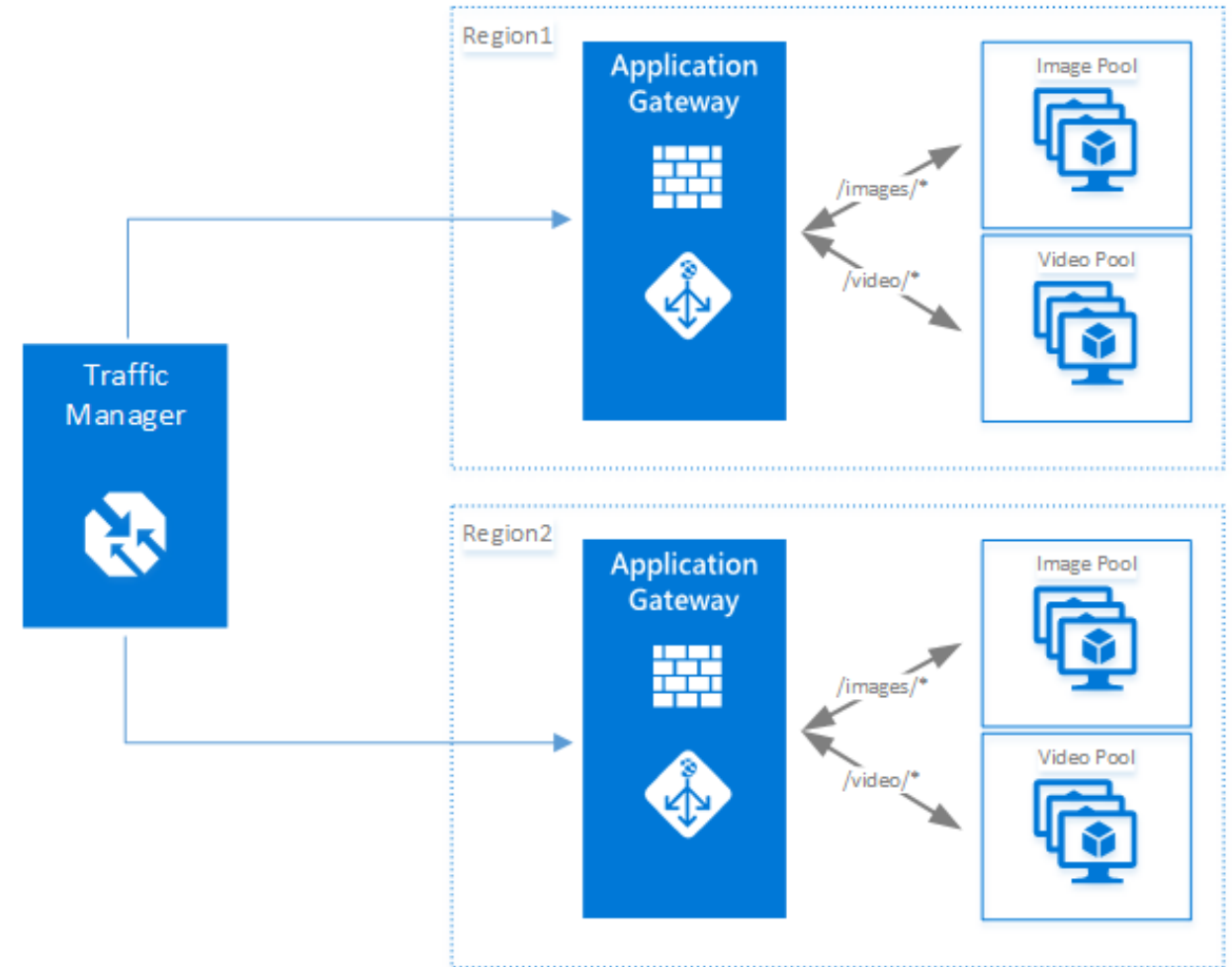
Standard Load Balancer

- 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



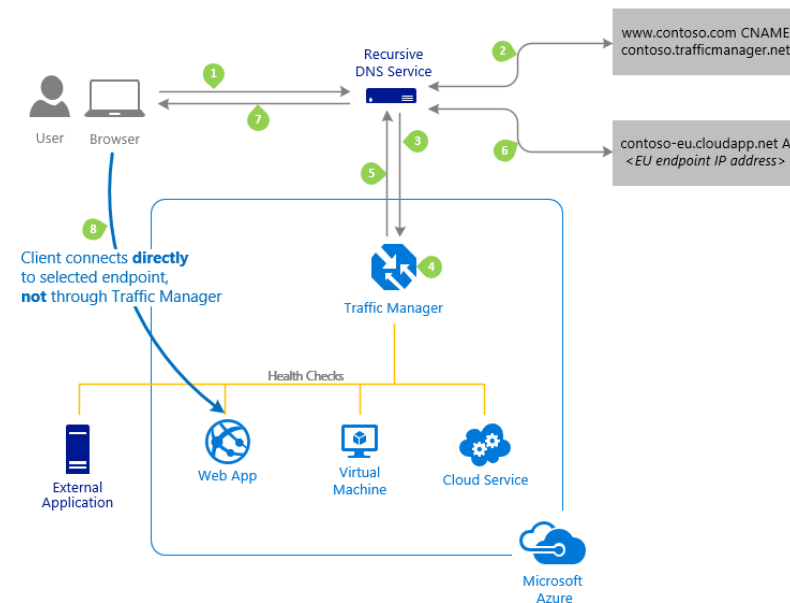
Network Services: Application Gateway

- **Layer 7 Load balancer, 99.95% SLA**
 - HTTP(S) Load balancing
 - Cookie based session affinity
- **Web Application Firewall built-in**
- **SSL Offload**
- **End-to-End SSL**
- **URL based content routing**
- **Multi-site routing**
- Websockets
- **3 sizes: Small, Medium, Large**
 - Up to 10 instances per gateway.
- 50 App Gateways per Subscription
- 20 Backend Pools per App Gateway



Traffic Manager

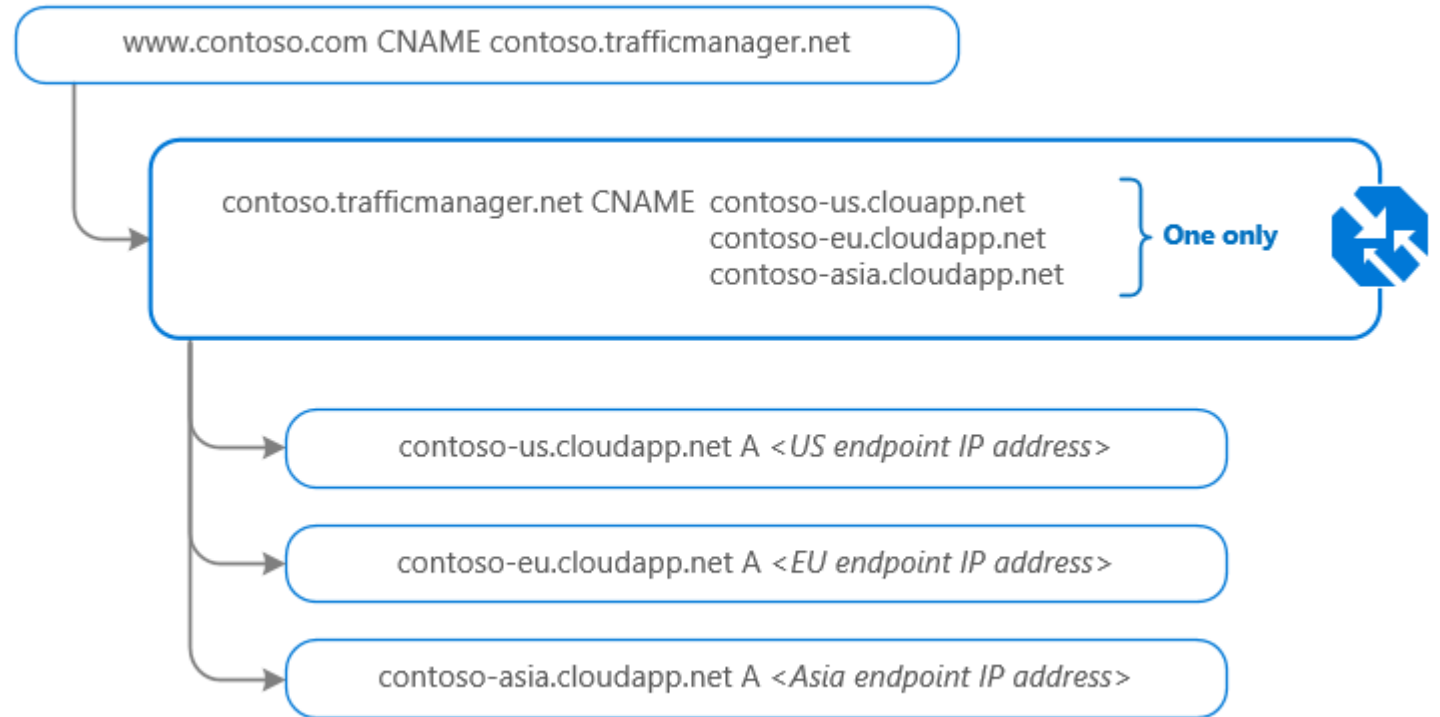
- control the distribution of user traffic for service endpoints
- Uses DNS to route traffic based on traffic routing method –
 - Priority
 - Weighted
 - Performance
 - Geographic
- Endpoint monitoring
- Benefits –
 - Improve availability of critical applications
 - Improve responsiveness for high performance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



Network Services: Traffic Manager

- **Endpoint Types**

- **Azure**
- **External**
- **Nested**
- **Web Apps**



<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-endpoint-types>

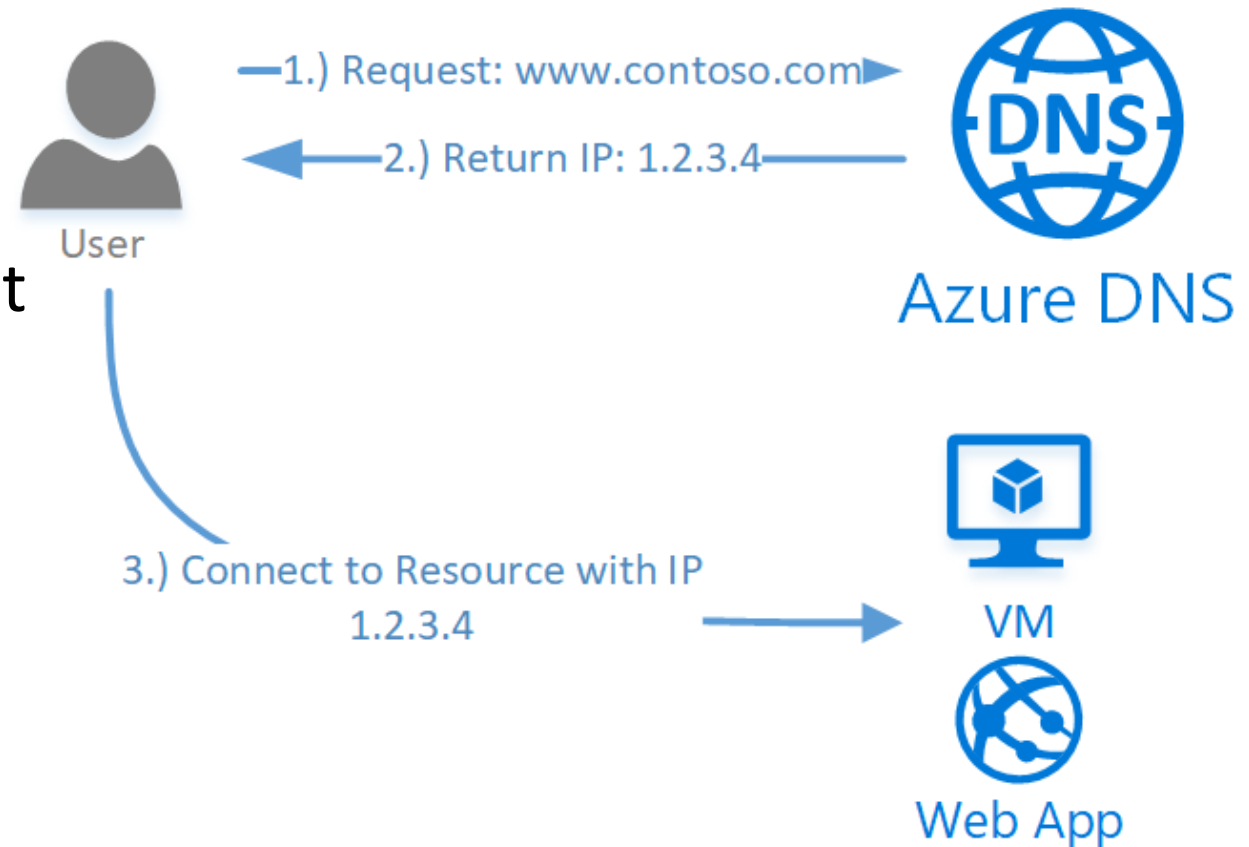
Network Services

- Load Balancer vs Application Gateway vs Traffic Manager

Service	Azure Load Balancer	Application Gateway	Traffic Manager
Technology	Transport level (Layer 4)	Application level (Layer 7)	DNS level
Application protocols supported	Any	HTTP, HTTPS, and WebSockets	Any (An HTTP endpoint is required for endpoint monitoring)
Endpoints	Azure VMs and Cloud Services role instances	Any Azure internal IP address, public internet IP address, Azure VM, or Azure Cloud Service	Azure VMs, Cloud Services, Azure Web Apps, and external endpoints
Vnet support	Can be used for both Internet facing and internal (Vnet) applications	Can be used for both Internet facing and internal (Vnet) applications	Only supports Internet-facing applications
Endpoint Monitoring	Supported via probes	Supported via probes	Supported via HTTP/HTTPS GET

Network Services: Azure DNS

- Azure Service for managing **Public DNS** (99.99% SLA)
- Integrates with Azure Management Services
- Controlled with Role Based Access Control
- 100 DNS Zones per subscription
- 5000 Record sets per zone
- 20 Records per record set



<https://docs.microsoft.com/en-us/azure/dns/dns-overview>

Networking Services: Private DNS

- **Use Azure Provided, OR**
- **Bring Your Own?**



• **Azure DNS Private Zones for cross VNET name resolution**

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances>

Scenario	Solution	Suffix
Name resolution between role instances or VMs located in the same cloud service or virtual network	Azure-provided name resolution	hostname or FQDN
Name resolution between role instances or VMs located in different virtual networks	Customer-managed DNS servers forwarding queries between vnets for resolution by Azure (DNS proxy). see Name resolution using your own DNS server	FQDN only
Resolution of on-premises computer and service names from role instances or VMs in Azure	Customer-managed DNS servers (e.g. on-premises domain controller, local read-only domain controller or a DNS secondary synced using zone transfers). See Name resolution using your own DNS server	FQDN only
Resolution of Azure hostnames from on-premises computers	Forward queries to a customer-managed DNS proxy server in the corresponding vnet, the proxy server forwards queries to Azure for resolution. See Name resolution using your own DNS server	FQDN only
Reverse DNS for internal IPs	Name resolution using your own DNS server	n/a
Name resolution between VMs or role instances located in different cloud services, not in a virtual network	Not applicable. Connectivity between VMs and role instances in different cloud services is not supported outside a virtual network.	n/a

Networking Services: Private DNS

- Azure Provided
 - No configuration, Highly Available
 - Intra VNET name resolution doesn't require FQDN
 - DNS suffix cannot be modified
 - WINS and NetBIOS not supported
 - DNS queries are throttled
- Your Own DNS Server
 - Forwarded DNS Requests are sent to reserved IP 168.63.129.16
 - Specify DNS Server per Virtual Network or NIC
 - 20/100 DNS Servers per Virtual Network

Networking Services: DHCP

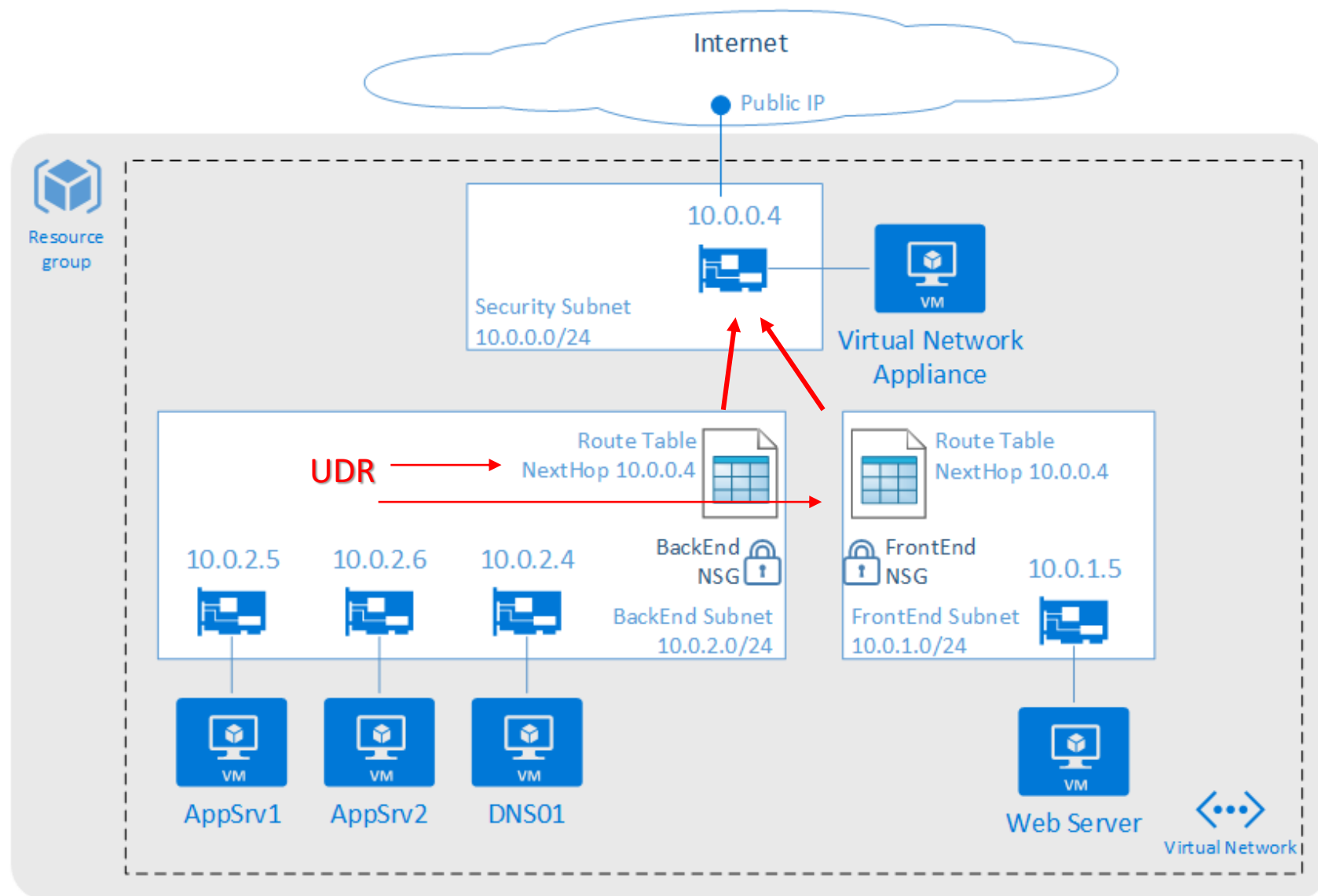
- Private IP address allocations:
 - **Dynamic (default)**
 - **Static – survives stop/start**
 - Use Static for
 - VMs that act as domain controllers or DNS servers.
 - Resources that require firewall rules using IP addresses.
 - Resources accessed by other apps/resources through an IP address.
 - Can be associated with
 - VM, **Load Balancer**, **App Gateway**
- <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-ip-addresses-overview-arm>

Networking Services: IP Addresses

- Public and Private
 - 4096 Private IP addresses per vnet
 - **60 Dynamic Public IPs**
 - **20 Static Public IPs**
- Public IP addresses can be dynamic or static.
 - **Dynamic IP address is not allocated until associated resource is created/started.**
 - **Dynamic IP Released when stop/delete resource.**
 - **Static IP address allocated immediately. Released only when it is deleted.**
- Use with
 - Virtual machines (VM)
 - Internet-facing load balancers
 - VPN gateways
 - Application gateway
- Azure Datacenter IP Ranges: <https://www.microsoft.com/en-us/download/details.aspx?id=41653>

Networking Services: User Defined Routes

- System Routes allow VMs to communicate with each other inside a VNET
 - Out of the box, 3 rules:
 - Local Vnet Rule: Intra and Inter Subnet communication
 - Internet Rule: VMs to Internet
 - On-Prem Rule: VNET to on-prem via VPN
 - VNET to VNET via a Gateway or Peering also supported
- User Defined Routes (UDR) to control the routing of packets
 - **Force Tunneling to the Internet via on-prem network**
 - **Use Virtual Appliances**
- Route selection order: User Defined Route, BGP Route (with ER), System Route
- **IP forwarding** allows a VM like a Virtual Appliance to receive traffic addressed to other destinations
- 100/200 User defined Routes per region per subscription



I am updating an app to a new release. I want to minimize downtime as much as possible and slowly introduce the release into production. Which Traffic Manager routing method should I use?

- 1) Weighted
- 2) Priority
- 3) Performance
- 4) Geographic

I am updating an app to a new release. I want to minimize downtime as much as possible and slowly introduce the release into production. Which Traffic Manager routing method should I use?

- 1) **Weighted**
- 2) Priority
- 3) Performance
- 4) Geographic

You've got an Azure Vnet in Europe and one in North America. What is the most cost effective way to connect these vnets so they can communicate securely?

- 1) Vnet Peering
- 2) Vnet-to-Vnet Connection
- 3) ExpressRoute
- 4) Connect through on-prem with VPNs

You've got an Azure Vnet in Europe and one in North America. What is the most cost effective way to connect these vnets so they can communicate securely?

- 1) Vnet Peering
- 2) Vnet-to-Vnet Connection**
- 3) ExpressRoute
- 4) Connect through on-prem with VPNs

I have 25 IIS websites that I want to host in Azure. Each has a separate domain. Some require https and some require cookie based session affinity. At a minimum, what will I need?

- 1) 2 Public IP Addresses
- 2) 25 Application Gateways
- 3) 25 Application Gateway Instances
- 4) 2 Application Gateways
- 5) 25 Public IP Addresses

I have 25 IIS websites that I want to host in Azure. Each has a separate domain. Some require https and some require cookie based session affinity. At a minimum, what will I need?

- 1) 2 Public IP Addresses
- 2) 25 Application Gateways
- 3) 25 Application Gateway Instances
- 4) 2 Application Gateways**
- 5) 25 Public IP Addresses

Clients outside of Azure access my VM by IP address. I've maxed out my static Public IP addresses for the subscription and I occasionally need to turn the VM off. What is the most cost effective alternative?

- 1) Private Static IP address and a Dynamic Public IP address
- 2) Application Gateway with Dynamic Public IP address
- 3) VPN with a Dynamic Public IP address
- 4) Load Balancer with Dynamic Public IP address
- 5) Never turn off the VM

Clients outside of Azure access my VM by IP address. I've maxed out my static Public IP addresses for the subscription and I occasionally need to turn the VM off. What is the most cost effective alternative?

- 1) Private Static IP address and a Dynamic Public IP address
- 2) Application Gateway with Dynamic Public IP address
- 3) VPN with a Dynamic Public IP address
- 4) Load Balancer with Dynamic Public IP address**
- 5) Never turn off the VM