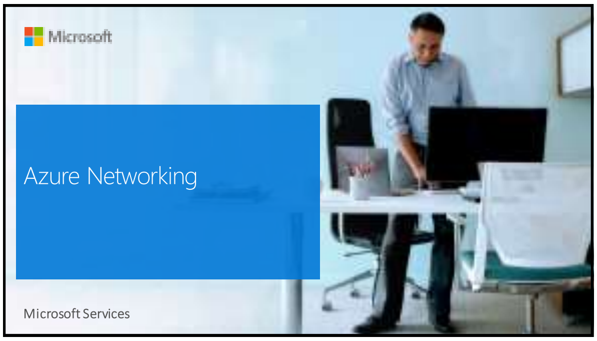


Microsoft

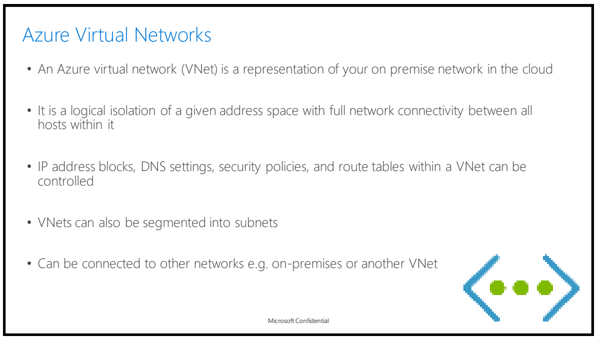
Azure Networking

Microsoft Services

Agenda

- Azure Virtual Networks
- Azure Connectivity
- Azure Networking Services

Microsoft Confidential

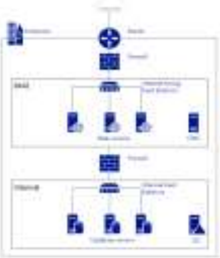


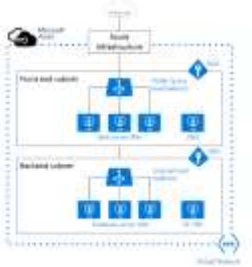
Azure Virtual Networks

- An Azure virtual network (VNet) is a representation of your on premise network in the cloud
- It is a logical isolation of a given address space with full network connectivity between all hosts within it
- IP address blocks, DNS settings, security policies, and route tables within a VNet can be controlled
- VNets can also be segmented into subnets
- Can be connected to other networks e.g. on-premises or another VNet

Microsoft Confidential

Azure Virtual Networks

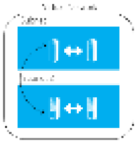




Microsoft Confi

Virtual Network Name Resolution

- An Internal DNS suffix *.internal.cloudapp.net is provided to each VM using DHCP
- This enables hostname resolution as the hostname records are in the internal.cloudapp.net zone on Azure internal DNS servers
- An Internal DNS suffix is not supplied to VMs when using your own DNS
- Instead we provide a non-functioning placeholder reddog.microsoft.com
- Internal DNS name resolution resolves DNS queries only for hosts that are within the same VNet



Microsoft Confidential

Virtual Network Service Endpoints

- Virtual Network service endpoints extend your virtual network to other Azure services such as storage, over a direct connection
- Endpoints allow you to secure your critical Azure resources to only your virtual networks
- Traffic from your VNet to an Azure service always remains on the Microsoft Azure backbone network
- Service endpoints available are:
  - Azure Active Directory
  - Azure CosmosDB
  - Azure ContainerRegistry
  - Azure EventHub
  - Azure Key Vault
  - Azure ServiceBus
  - Azure SQL
  - Azure Storage
  - Azure Web Services

Microsoft Confidential

Virtual Network Service Endpoints Benefits

- Improved security for your Azure service resources by fully removing public Internet access to resources, and only allowing traffic from your virtual network
- Optimal routing for Azure service traffic from your virtual network by keeping traffic on the Azure backbone and not going over the Internet
- Simple to set up with less management overhead, you no longer need reserved public IP addresses in your virtual network to secure access to Azure resources through an IP firewall
- Can be applied to new or existing virtual networks

Add service endpoints

Service

Microsoft.Storage

* Subnets

0 selected

Microsoft Confidential

Virtual Network Features

- Bring your own IPv4 address space to be used in a VNet
  - Both RFC 1918 and Public IP address ranges are supported
  - Public IP address ranges are not directly accessible from the Internet
  - Overlapping ranges are not supported
- Use on-premises or Azure internal DNS servers for name resolution
  - Allows you to add your on-premises DNS servers IP addresses for name resolution in the VNet
  - Allows VMs running in Microsoft Azure to be joined to your on-premises Active Directory
  - Azure internal DNS is used for name resolution within a VNet if you do not configure your own DNS servers
- Acts as a DHCP server by dynamically assigning IP addresses to VM's
- Supports IP address reservation for connected devices

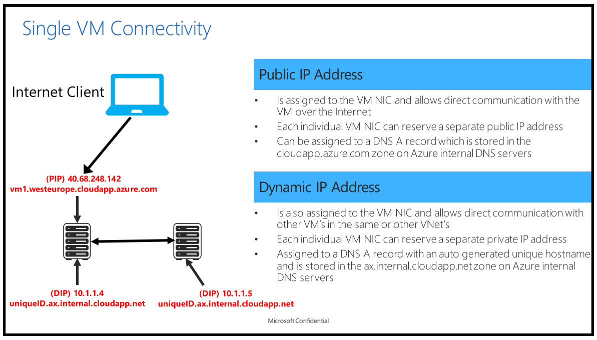
Microsoft Confidential

Demo: Deploying a Virtual Network & Enable Service Endpoints

Microsoft

Azure Connectivity

Microsoft Services



Single VM Connectivity

Internet Client

(PIP) 40.68.248.142
vm1.westeurope.cloudapp.azure.com

(DIP) 10.1.1.4
uniqueID.ax.internal.cloudapp.net

(DIP) 10.1.1.5
uniqueID.ax.internal.cloudapp.net

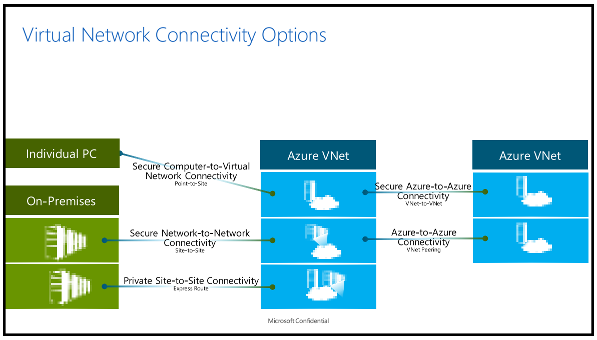
Public IP Address

- Is assigned to the VM NIC and allows direct communication with the VM over the Internet
- Each individual VM NIC can reserve a separate public IP address
- Can be assigned to a DNS A record which is stored in the cloudapp.azure.com zone on Azure internal DNS servers

Dynamic IP Address

- Is also assigned to the VM NIC and allows direct communication with other VM's in the same or other VNet's
- Each individual VM NIC can reserve a separate private IP address
- Assigned to a DNS A record with an auto generated unique hostname and is stored in the ax.internal.cloudapp.net zone on Azure internal DNS servers

Microsoft Confidential



Virtual Network Connectivity Options

Individual PC

On-Premises

Azure VNet

Azure VNet

Secure Computer-to-Virtual Network Connectivity
Point-to-Site

Secure Network-to-Network Connectivity
Site-to-Site

Private Site-to-Site Connectivity
Express Route

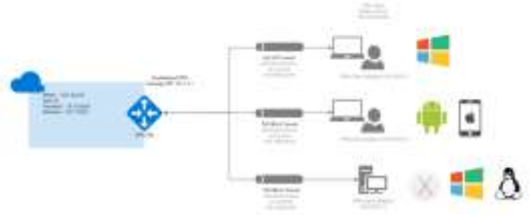
Secure Azure-to-Azure Connectivity
VNet-to-VNet

Azure-to-Azure Connectivity
VNet Peering

Microsoft Confidential

Point-to-Site Connectivity

- Extend your Azure virtual network securely to a single or multiple computers using a SSTP or IKEv2 tunnel

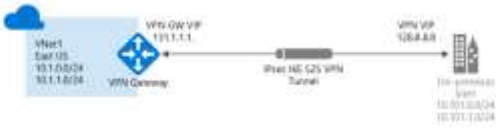


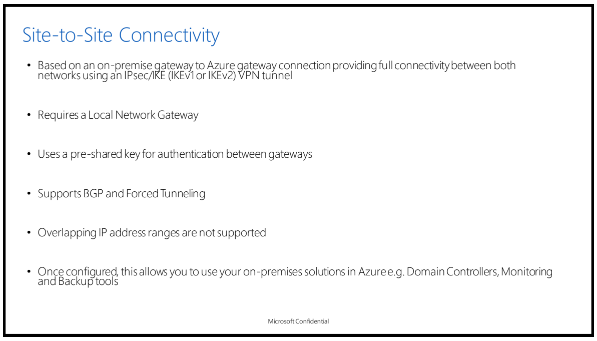
Point-to-Site Connectivity

- Based on a VPN client connection to an Azure virtual network gateway
- Uses Azure or customer provided certificates or RADIUS authentication to authenticate VPN clients
- Supports SSTP and IKEv2 VPN tunnels over the Internet
- Supports Windows 7, Mac OS X version 10.11 and above and Linux with strongSwan (IKEv2)
- Supports up to 128 VPN client connections

Site-to-Site Connectivity

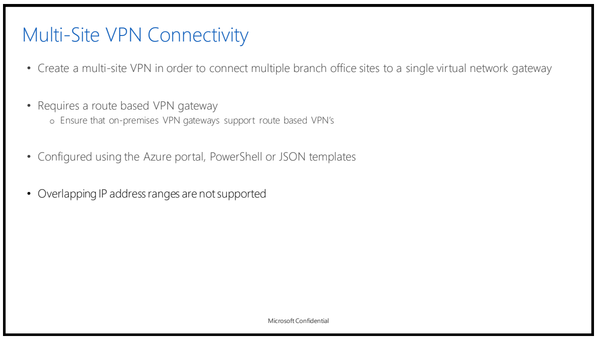
- Extend your on-premises network securely to the cloud using an IPSec/IKEv2 VPN tunnel over the Internet





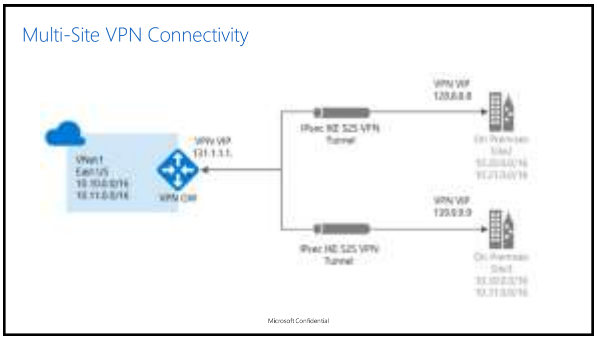
Site-to-Site Connectivity

- Based on an on-premise gateway to Azure gateway connection providing full connectivity between both networks using an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel
- Requires a Local Network Gateway
- Uses a pre-shared key for authentication between gateways
- Supports BGP and Forced Tunneling
- Overlapping IP address ranges are not supported
- Once configured, this allows you to use your on-premises solutions in Azure e.g. Domain Controllers, Monitoring and Backup tools



Multi-Site VPN Connectivity

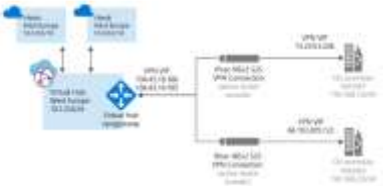
- Create a multi-site VPN in order to connect multiple branch office sites to a single virtual network gateway
- Requires a route based VPN gateway
  - Ensure that on-premises VPN gateways support route based VPN's
- Configured using the Azure portal, PowerShell or JSON templates
- Overlapping IP address ranges are not supported



Multi-Site VPN Connectivity

Azure Virtual WAN

- Azure Virtual WAN provides large-scale site-to-site connectivity and is built for throughput, scalability, and ease of use
- Extend your on-premises network securely to an Azure regional hub network using an IPSec/IKEv1 or IKEv2 VPN tunnel over the Internet

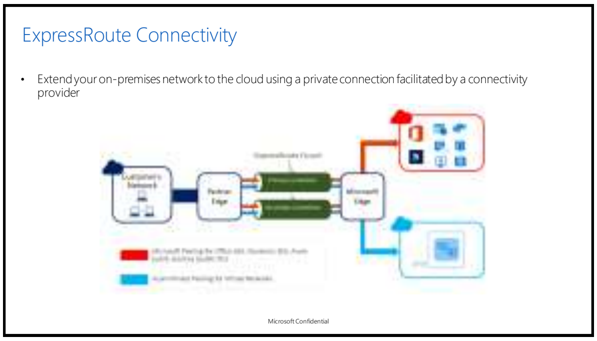


Azure Virtual WAN Components

- virtualWAN - The virtualWAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources
- Site – A site represents your on-premises VPN device and its settings
- Hub - A hub is a Microsoft-managed virtual network that contains various service endpoints to enable connectivity from your on-premises network
- Hub virtual network connection - The Hub virtual network connection resource is used to connect the hub seamlessly to your virtual network
- Hub route table – A hub route table is a routing table that can be applied to the virtual hub route table

Azure Virtual WAN concepts

- One virtual hub per Azure region
- Each virtual hub supports up to 1000 connections with 2 Gbps throughput, 20Gbps is available in the West Central region
- Each connection consists of two tunnels that are in an active-active configuration
- Tunnels terminate in an Azure Virtual Hub vpngateway
- Global VNet peering is not supported
- Supports BGP and NVA's

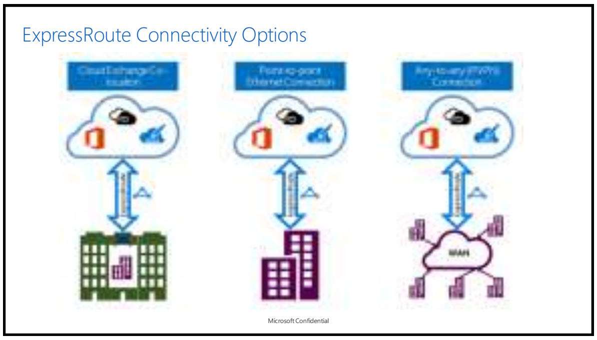


ExpressRoute Connectivity

- Extend your on-premises network to the cloud using a private connection facilitated by a connectivity provider

ExpressRoute Circuit
Customer's Network
Partner Edge
Primary Connection
Secondary Connection
Microsoft Edge
Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)
Azure Private Peering for Virtual Networks

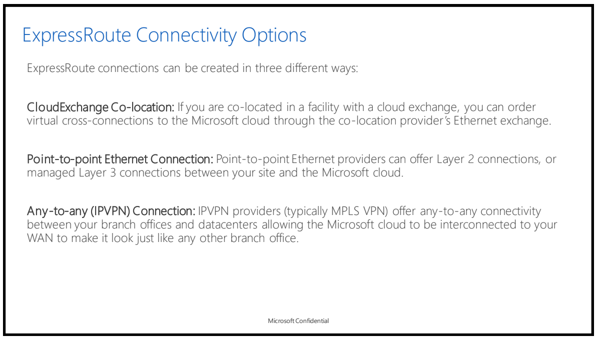
Microsoft Confidential



ExpressRoute Connectivity Options

Cloud Exchange Co-location
Point-to-point Ethernet Connection
Any-to-any (IPVPN) Connection
WAN

Microsoft Confidential



ExpressRoute Connectivity Options

ExpressRoute connections can be created in three different ways:

CloudExchange Co-location: If you are co-located in a facility with a cloud exchange, you can order virtual cross-connections to the Microsoft cloud through the co-location provider's Ethernet exchange.

Point-to-point Ethernet Connection: Point-to-point Ethernet providers can offer Layer 2 connections, or managed Layer 3 connections between your site and the Microsoft cloud.

Any-to-any (IPVPN) Connection: IPVPN providers (typically MPLS VPN) offer any-to-any connectivity between your branch offices and datacenters allowing the Microsoft cloud to be interconnected to your WAN to make it look just like any other branch office.

Microsoft Confidential

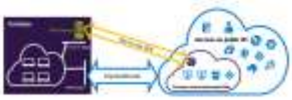
ExpressRoute Connectivity

- Offers redundant connections for high availability
- Supports Private and Microsoft peering:
  - Private peering facilitates RFC 1918 connectivity between on-premises and your Azure virtual network
  - Microsoft peering facilitates connectivity between on-premises and Microsoft services such as Office 365, Dynamics 365, Azure Public services (Public IP's) e.g. Azure storage, Azure Web Apps
- Predictable performance and high throughput, supports 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps and 10 Gbps connections
- More secure over a private connection as opposed to the Internet
- No data encryption included by default, this must be implemented by the provider or customer
- A single ExpressRoute connection can be shared across subscriptions
- Can coexist with a Site-to-Site connection

Microsoft Confidential

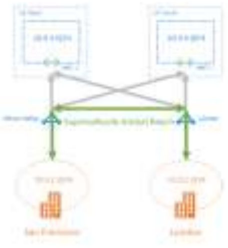
ExpressRoute & Site-to-Site coexistence

- Coexistence requires two gateways, one for ExpressRoute and the other for a Site-to-Site connection
- Configure a Site-to-Site VPN connection as a secure failover path for ExpressRoute
- Use Site-to-Site VPNs to connect to sites that are not connected through ExpressRoute

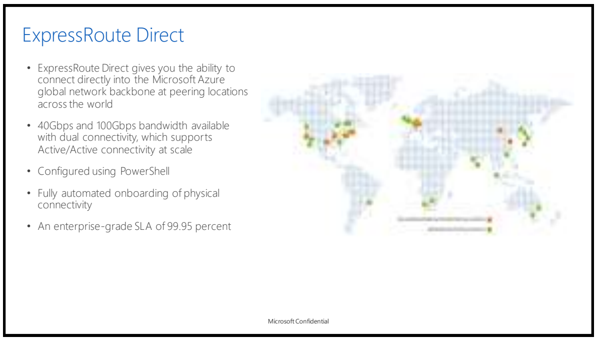


ExpressRoute Global Reach

- ExpressRoute Global Reach is an Azure service that connects two or more on-premises networks by linking their existing ExpressRoute circuits through Microsoft's global network
- Provides connectivity between on-premises networks that do not have WAN connectivity between them
- Requires the ExpressRoute Standard SKU for circuits that are in the same region, else the ExpressRoute Premium SKU is required for circuits between regions
- Configured using PowerShell
- Maximum of 10 connected circuits for ExpressRoute Standard or 100 connected circuits for ExpressRoute Premium (linked Virtual Networks are also included in the count)



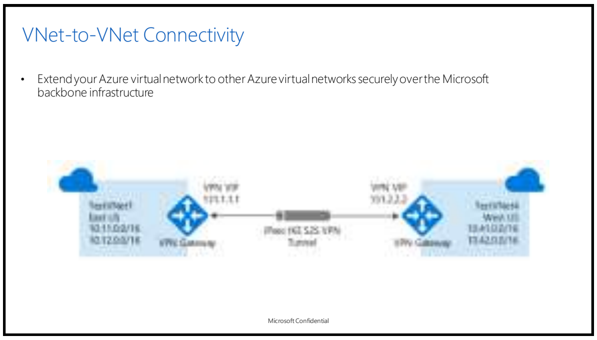
Microsoft Confidential



ExpressRoute Direct

- ExpressRoute Direct gives you the ability to connect directly into the Microsoft Azure global network backbone at peering locations across the world
- 40Gbps and 100Gbps bandwidth available with dual connectivity, which supports Active/Active connectivity at scale
- Configured using PowerShell
- Fully automated onboarding of physical connectivity
- An enterprise-grade SLA of 99.95 percent

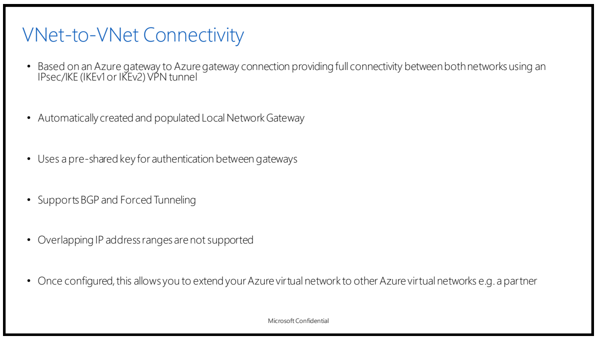
Microsoft Confidential



VNet-to-VNet Connectivity

- Extend your Azure virtual network to other Azure virtual networks securely over the Microsoft backbone infrastructure

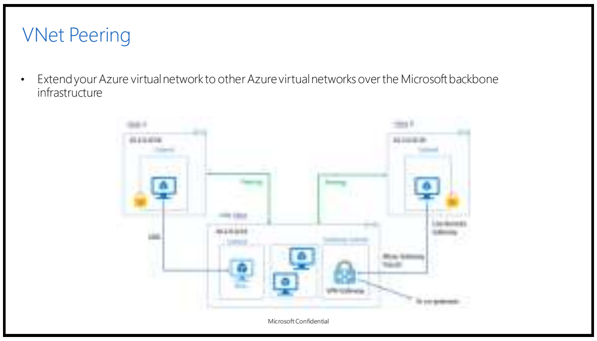
Microsoft Confidential



VNet-to-VNet Connectivity

- Based on an Azure gateway to Azure gateway connection providing full connectivity between both networks using an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel
- Automatically created and populated Local Network Gateway
- Uses a pre-shared key for authentication between gateways
- Supports BGP and Forced Tunneling
- Overlapping IP address ranges are not supported
- Once configured, this allows you to extend your Azure virtual network to other Azure virtual networks e.g. a partner

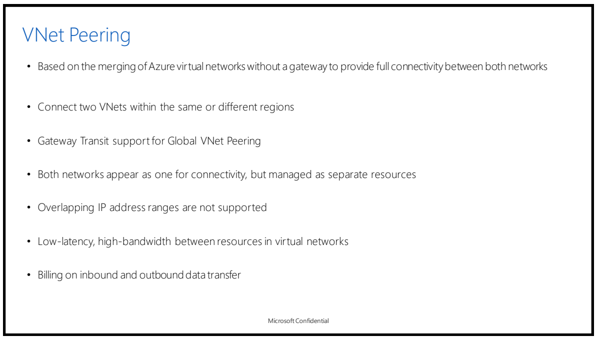
Microsoft Confidential



VNet Peering

- Extend your Azure virtual network to other Azure virtual networks over the Microsoft backbone infrastructure

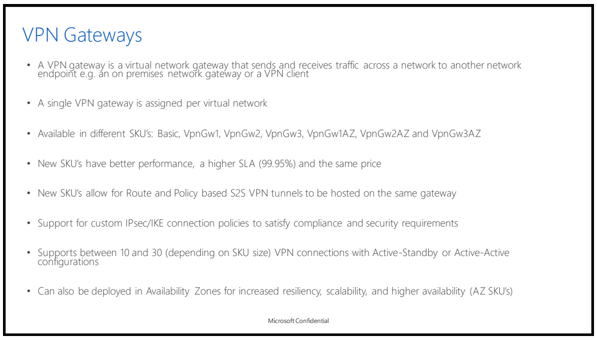
Microsoft Confidential



VNet Peering

- Based on the merging of Azure virtual networks without a gateway to provide full connectivity between both networks
- Connect two VNets within the same or different regions
- Gateway Transit support for Global VNet Peering
- Both networks appear as one for connectivity, but managed as separate resources
- Overlapping IP address ranges are not supported
- Low-latency, high-bandwidth between resources in virtual networks
- Billing on inbound and outbound data transfer

Microsoft Confidential



VPN Gateways

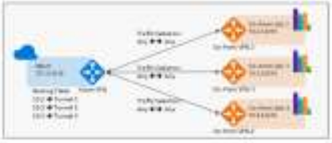
- A VPN gateway is a virtual network gateway that sends and receives traffic across a network to another network endpoint e.g. an on premises network gateway or a VPN client
- A single VPN gateway is assigned per virtual network
- Available in different SKU's: Basic, VpnGw1, VpnGw2, VpnGw3, VpnGw1AZ, VpnGw2AZ and VpnGw3AZ
- New SKU's have better performance, a higher SLA (99.95%) and the same price
- New SKU's allow for Route and Policy based S2S VPN tunnels to be hosted on the same gateway
- Support for custom IPsec/IKE connection policies to satisfy compliance and security requirements
- Supports between 10 and 30 (depending on SKU size) VPN connections with Active-Standby or Active-Active configurations
- Can also be deployed in Availability Zones for increased resiliency, scalability, and higher availability (AZ SKU's)

Microsoft Confidential

VPN Gateway Types

Route-Based VPN Gateway

- Route-based VPN devices use any-to-any (wildcard) traffic selectors, and let their routing tables direct traffic to the relevant IPsec tunnels
- Built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface)
- Supports BGP, Forced Tunneling and multi-site VPN tunnels

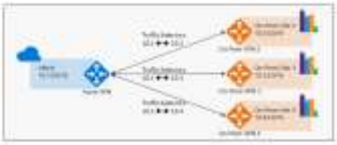


Microsoft Confidential

VPN Gateway Types

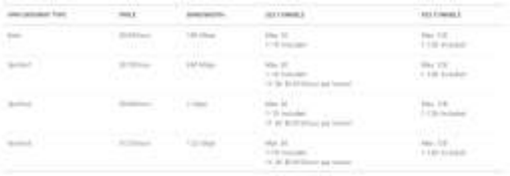
Policy-Based VPN Gateway

- Policy-based VPN devices use combinations of both networks prefixes to define how traffic is encrypted/decrypted through IPsec tunnels
- Built on firewall devices that perform packet filtering. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine
- Does not support BGP, Forced Tunneling and multi-site VPN tunnels

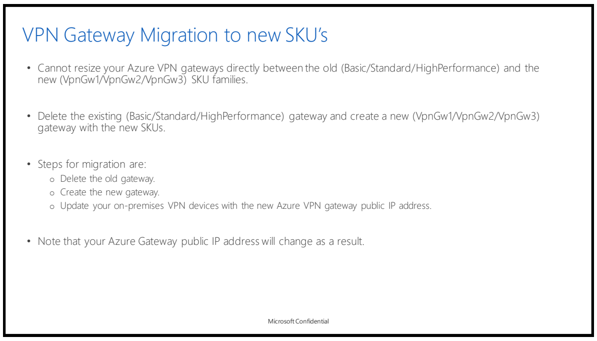


Microsoft Confidential

VPN Gateways



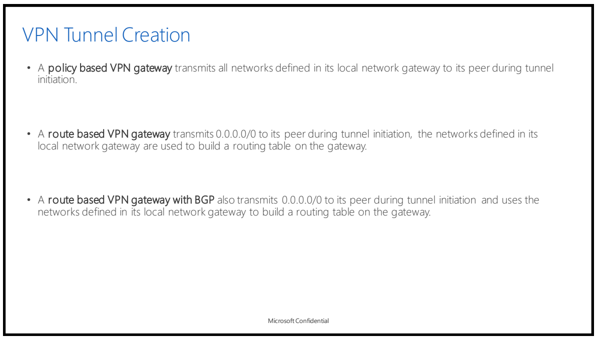
VPN GATEWAY TYPE	PRICE	BANDWIDTH	S2S TUNNELS	P2S TUNNELS
Basic	$0.04/hour	100 Mbps	Max. 10 1-10: Included	Max. 128 1-128: Included
VpnGw1	$0.19/hour	650 Mbps	Max. 30 1-10: Included 11-30: $0.015/hour per tunnel	Max. 128 1-128: Included
VpnGw2	$0.49/hour	1 Gbps	Max. 30 1-10: Included 11-30: $0.015/hour per tunnel	Max. 128 1-128: Included
VpnGw3	$1.25/hour	1.25 Gbps	Max. 30 1-10: Included 11-30: $0.015/hour per tunnel	Max. 128 1-128: Included



VPN Gateway Migration to new SKU's

- Cannot resize your Azure VPN gateways directly between the old (Basic/Standard/HighPerformance) and the new (VpnGw1/VpnGw2/VpnGw3) SKU families.
- Delete the existing (Basic/Standard/HighPerformance) gateway and create a new (VpnGw1/VpnGw2/VpnGw3) gateway with the new SKUs.
- Steps for migration are:
  - Delete the old gateway.
  - Create the new gateway.
  - Update your on-premises VPN devices with the new Azure VPN gateway public IP address.
- Note that your Azure Gateway public IP address will change as a result.

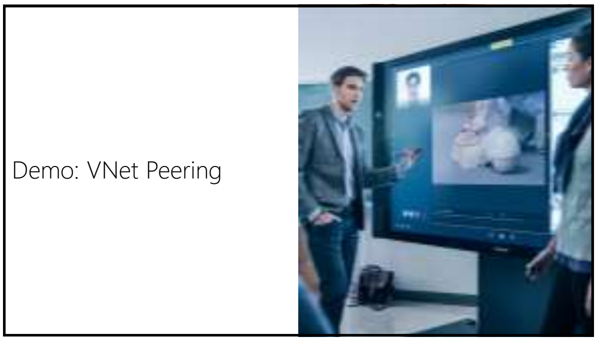
Microsoft Confidential



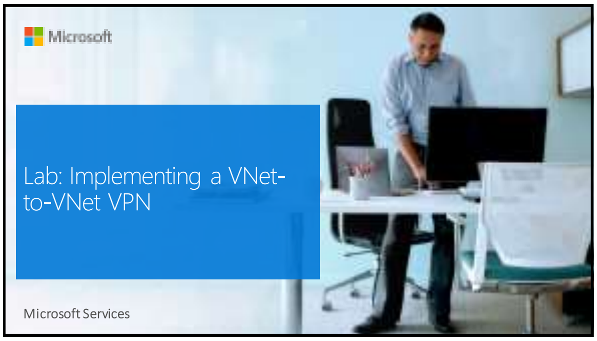
VPN Tunnel Creation

- A **policy based VPN gateway** transmits all networks defined in its local network gateway to its peer during tunnel initiation.
- A **route based VPN gateway** transmits 0.0.0.0/0 to its peer during tunnel initiation, the networks defined in its local network gateway are used to build a routing table on the gateway.
- A **route based VPN gateway with BGP** also transmits 0.0.0.0/0 to its peer during tunnel initiation and uses the networks defined in its local network gateway to build a routing table on the gateway.

Microsoft Confidential



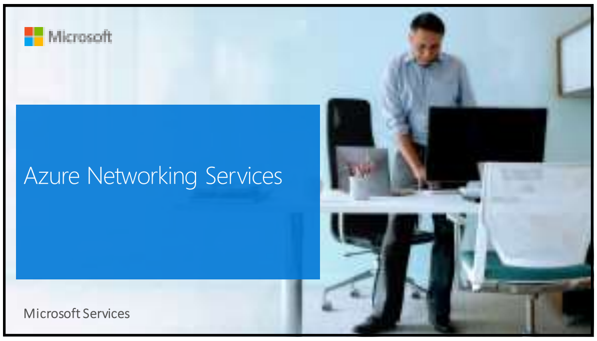
Demo: VNet Peering



Microsoft

Lab: Implementing a VNet-to-VNet VPN

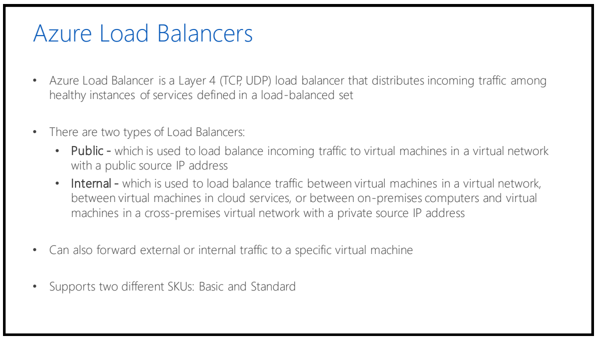
Microsoft Services



Microsoft

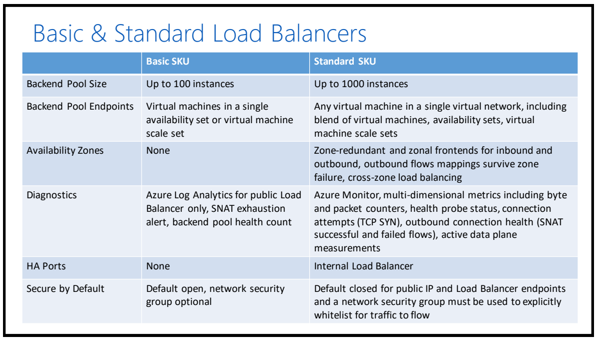
Azure Networking Services

Microsoft Services



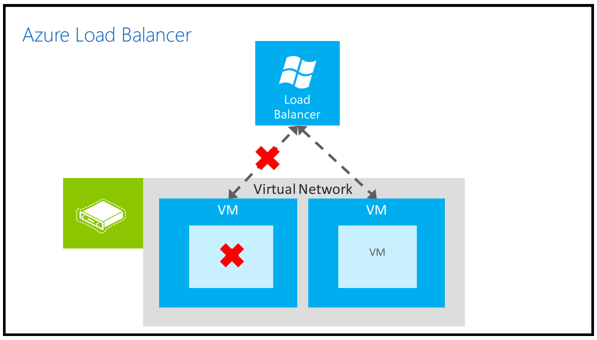
Azure Load Balancers

- Azure Load Balancer is a Layer 4 (TCP, UDP) load balancer that distributes incoming traffic among healthy instances of services defined in a load-balanced set
- There are two types of Load Balancers:
  - **Public** - which is used to load balance incoming traffic to virtual machines in a virtual network with a public source IP address
  - **Internal** - which is used to load balance traffic between virtual machines in a virtual network, between virtual machines in cloud services, or between on-premises computers and virtual machines in a cross-premises virtual network with a private source IP address
- Can also forward external or internal traffic to a specific virtual machine
- Supports two different SKUs: Basic and Standard

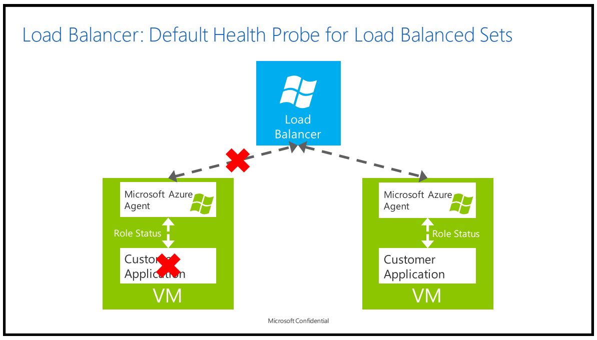


Basic & Standard Load Balancers

	Basic SKU	Standard SKU
Backend Pool Size	Up to 100 instances	Up to 1000 instances
Backend Pool Endpoints	Virtual machines in a single availability set or virtual machine scale set	Any virtual machine in a single virtual network, including blend of virtual machines, availability sets, virtual machine scale sets
Availability Zones	None	Zone-redundant and zonal frontends for inbound and outbound, outbound flows mappings survive zone failure, cross-zone load balancing
Diagnostics	Azure Log Analytics for public Load Balancer only, SNAT exhaustion alert, backend pool health count	Azure Monitor, multi-dimensional metrics including byte and packet counters, health probe status, connection attempts (TCP SYN), outbound connection health (SNAT successful and failed flows), active data plane measurements
HA Ports	None	Internal Load Balancer
Secure by Default	Default open, network security group optional	Default closed for public IP and Load Balancer endpoints and a network security group must be used to explicitly whitelist for traffic to flow

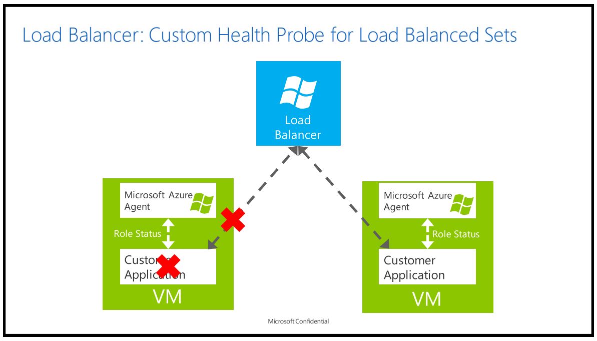


Azure Load Balancer



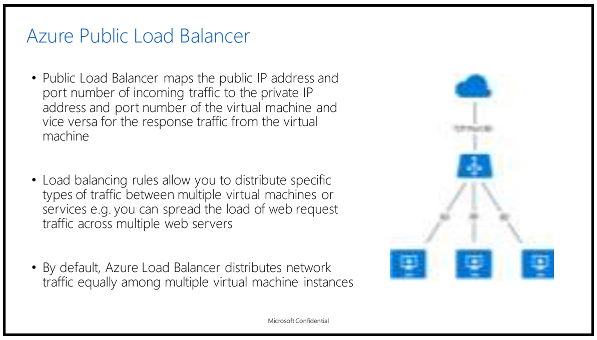
Load Balancer: Default Health Probe for Load Balanced Sets

Microsoft Confidential



Load Balancer: Custom Health Probe for Load Balanced Sets

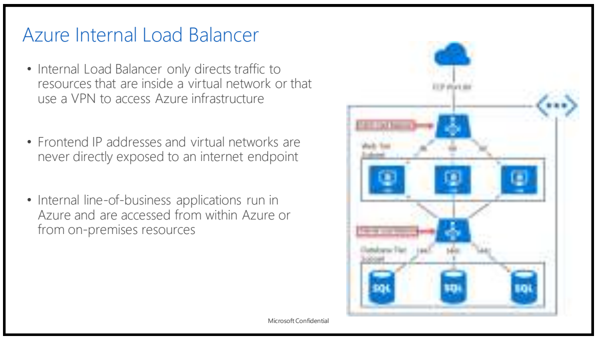
Microsoft Confidential



Azure Public Load Balancer

- Public Load Balancer maps the public IP address and port number of incoming traffic to the private IP address and port number of the virtual machine and vice versa for the response traffic from the virtual machine
- Load balancing rules allow you to distribute specific types of traffic between multiple virtual machines or services e.g. you can spread the load of web request traffic across multiple web servers
- By default, Azure Load Balancer distributes network traffic equally among multiple virtual machine instances

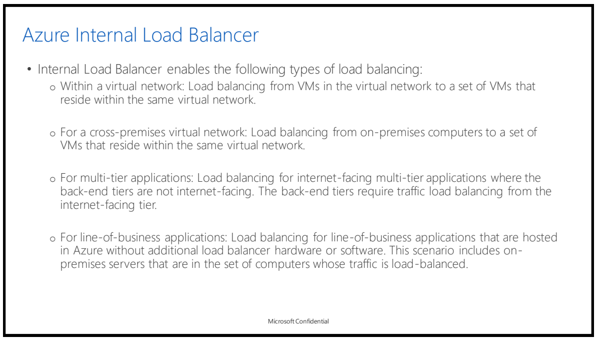
Microsoft Confidential



Azure Internal Load Balancer

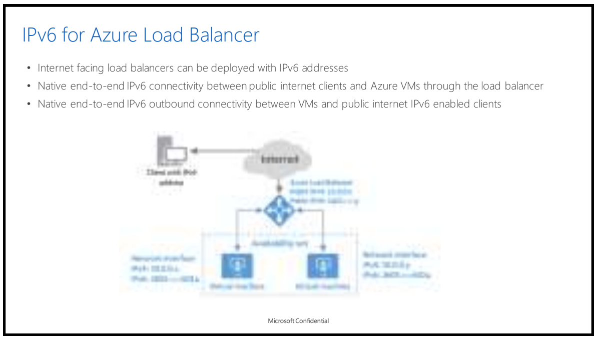
- Internal Load Balancer only directs traffic to resources that are inside a virtual network or that use a VPN to access Azure infrastructure
- Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint
- Internal line-of-business applications run in Azure and are accessed from within Azure or from on-premises resources

Microsoft Confidential



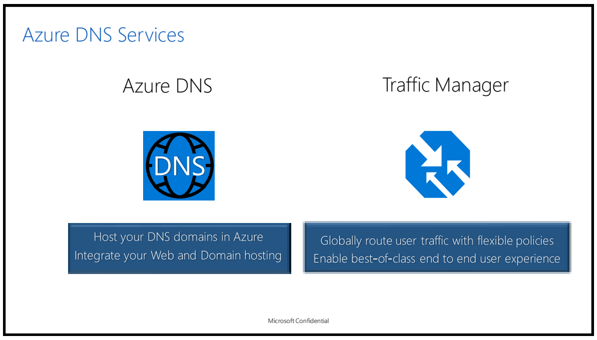
Azure Internal Load Balancer

- Internal Load Balancer enables the following types of load balancing:
  - Within a virtual network: Load balancing from VMs in the virtual network to a set of VMs that reside within the same virtual network.
  - For a cross-premises virtual network: Load balancing from on-premises computers to a set of VMs that reside within the same virtual network.
  - For multi-tier applications: Load balancing for internet-facing multi-tier applications where the back-end tiers are not internet-facing. The back-end tiers require traffic load balancing from the internet-facing tier.
  - For line-of-business applications: Load balancing for line-of-business applications that are hosted in Azure without additional load balancer hardware or software. This scenario includes on-premises servers that are in the set of computers whose traffic is load-balanced.



IPv6 for Azure Load Balancer

- Internet facing load balancers can be deployed with IPv6 addresses
- Native end-to-end IPv6 connectivity between public internet clients and Azure VMs through the load balancer
- Native end-to-end IPv6 outbound connectivity between VMs and public internet IPv6 enabled clients



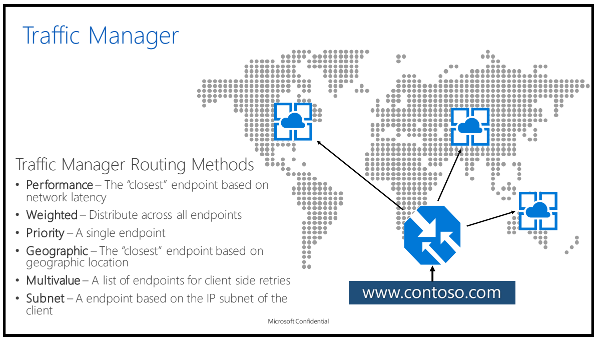
Azure DNS Services

Azure DNS

Host your DNS domains in Azure
Integrate your Web and Domain hosting

Traffic Manager

Globally route user traffic with flexible policies
Enable best-of-class end to end user experience



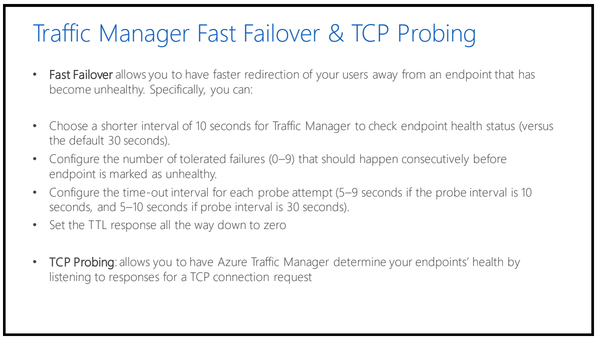
Traffic Manager

Traffic Manager Routing Methods

- **Performance** – The "closest" endpoint based on network latency
- **Weighted** – Distribute across all endpoints
- **Priority** – A single endpoint
- **Geographic** – The "closest" endpoint based on geographic location
- **Multivalue** – A list of endpoints for client side retries
- **Subnet** – A endpoint based on the IP subnet of the client

www.contoso.com

Microsoft Confidential

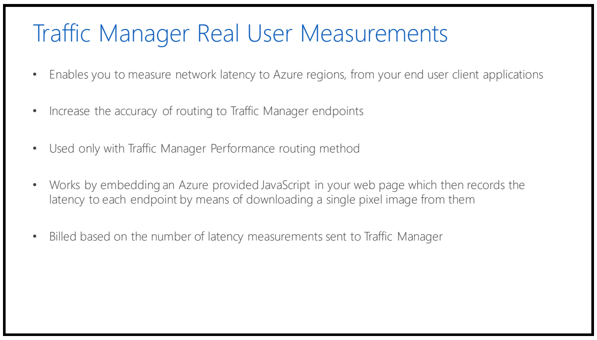


Traffic Manager Fast Failover & TCP Probing

- **Fast Failover** allows you to have faster redirection of your users away from an endpoint that has become unhealthy. Specifically, you can:

- Choose a shorter interval of 10 seconds for Traffic Manager to check endpoint health status (versus the default 30 seconds).
- Configure the number of tolerated failures (0–9) that should happen consecutively before endpoint is marked as unhealthy.
- Configure the time-out interval for each probe attempt (5–9 seconds if the probe interval is 10 seconds, and 5–10 seconds if probe interval is 30 seconds).
- Set the TTL response all the way down to zero

- **TCP Probing**: allows you to have Azure Traffic Manager determine your endpoints' health by listening to responses for a TCP connection request



Traffic Manager Real User Measurements

- Enables you to measure network latency to Azure regions, from your end user client applications
- Increase the accuracy of routing to Traffic Manager endpoints
- Used only with Traffic Manager Performance routing method
- Works by embedding an Azure provided JavaScript in your web page which then records the latency to each endpoint by means of downloading a single pixel image from them
- Billed based on the number of latency measurements sent to Traffic Manager

Traffic Manager Traffic View

- Traffic View provides Traffic Manager with a view of your user bases and their traffic pattern
- Using Traffic View you are able to:
  - Understand where your user bases are located (up to a local DNS resolver level granularity).
  - View the volume of traffic (observed as DNS queries handled by Azure Traffic Manager) originating from these regions.
  - Get insights into what is the representative latency experienced by these users.
  - Deep dive into the specific traffic patterns from each of these user bases to Azure regions where you have endpoints.
- Billed based on the number of data points used to create the insights presented

Azure Front Door Service

- Azure Front Door service is a HTTP, HTTPS and HTTP/2 load balancing and TCP optimization service
- Offers various load-balancing capabilities for your applications using the HTTP, HTTPS and HTTP/2 protocols
- Provides Dynamic Site Acceleration using Split TCP to optimize latency and round-trip time from the Front Door service to the backend application server
- Global load balancing with near real-time failover
- Highly available and scalable service, fully managed by Azure

User
Azure Front Door Service

Microsoft Confidential

Azure Front Door Routing Methods

- Latency: Requests are sent to the lowest latency backends acceptable within a sensitivity range i.e. the "closest" set of backends with respect to network latency
- Priority: All requests use a primary service backend, and provide backups in case the primary or the backup backends are unavailable
- Weighted: Requests are distributed across a set of backends, either evenly or according to weight coefficients
- Session Affinity: All subsequent requests from a user are sent to the same backend as long as the user session is still active and the backend instance still reports healthy based on health probes

Microsoft Confidential

Azure Load Balancing Services Comparison - Regional

- Azure Application Gateway offers various regional Layer 7 load-balancing capabilities for your applications e.g. SSL offloading to the application gateway, and is located in an Azure datacenter.

- Azure Load Balancer provides high-performance, low-latency regional Layer 4 load-balancing services for all UDP and TCP protocols and is located in an Azure datacenter.

Microsoft Confidential

Azure Load Balancing Services Comparison - Global

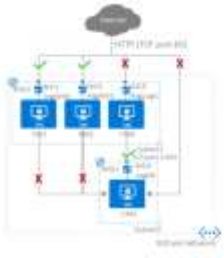
- Azure Front Door Service offers various global layer 7 load-balancing capabilities for your applications and provides Dynamic Site Acceleration (DSA) with near real-time failover. It supports the HTTP, HTTPS and HTTP/2 application protocols and is located in all POPs (Point of Presence)
  - o User connects to the Azure Front Door service POP and is then routed to the backend server via Microsofts global network

- Azure Traffic Manager provides global DNS load balancing, it looks at incoming DNS requests and responds with the DNS name of a healthy endpoint, in accordance with the routing policy the customer has selected e.g. Performance, Priority, Weighted etc. It supports any application protocol and is located in all POPs (Point of Presence)
  - o User connects directly to the backend server via the Internet

Microsoft Confidential

Network Security Groups (NSG)

- Define access control rules for inbound/outbound traffic to a VM/NIC or group of VMs in a subnet
- NSG rules can be changed at any time and apply to all instances
- NSG can be associated with:
  - A single ASM VM in a VNet or the NIC of an ARM VM
  - A subnet in a VNet
  - A VM/NIC and a Subnet together for added security
- Rules are processed in order of priority
- Rules are based on 5-tuple (source/dest IP/port, protocol)



Network Security Groups

- Two different ACL groups, one for individual VM/NIC, one for Subnet
- Rules are applied to inbound traffic for subnet followed by rules for the VM/NIC
- Outbound rules are applied for VM first and then followed by subnet rules

Example PowerShell:

```
New-AzureRMNetworkSecurityGroup -Name "MyVNetSG" -Location
uswest -Label "Security group for my Vnet in West US"

Get-AzureRMNetworkSecurityGroup -Name "MyVNetSG" | Set-
AzureRmNetworkSecurityRuleConfig -Name WEB -Type Inbound -
Priority 100 -Action Allow -SourceAddressPrefix 'INTERNET'  -
SourcePortRange '*' -DestinationAddressPrefix '*' -
DestinationPortRange '*' -Protocol TCP
```

Network Security Group Inbound Rules

- Inbound security rules are required to direct Internet or other virtual networks inbound network traffic to a VM
- In the Azure Management Portal, endpoints are automatically created for:
  - Remote Desktop
- Each inbound security rule has a source and destination port range:
  - Source port range: used by the Azure to listen for incoming traffic to the VM
  - Destination port range: used by the VM to listen for incoming traffic to an application or service running on the VM
- ACLs on an endpoint can restrict traffic based upon source IP address range
  - Inbound or outbound security rules can allow or deny traffic from specific IPs and known IP address ranges
  - Rules are evaluated based on priority number. The lower the number, the higher the priority
  - Inbound and Outbound Security rules are part of a Network Security group

Microsoft Confidential

Multi-NIC Support

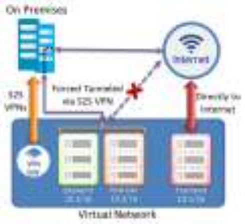
- Using multiple NICs on your VM allows you to manage network traffic better (max ~ 8)
- Isolate traffic between front-end NICs and backend NICs
- Cannot add or remove NICs once VM is created
- Can have multiple NICs on any VM except for Basic SKU
- VMs must be in an Azure Virtual Network
- Additional NICs cannot be used in a load balanced set
- On-premises VM's with multiple NIC's migrated to Azure won't work – VM must be built in Azure

Multiple IPs Per NIC

- Up to 250 private and public IP addresses can be assigned to each NIC
- Private IP addresses support Network Security Groups (NSGs) and User Defined Routes (UDRs)
- Through multiple IPs per NIC, load balancing can be configured across both primary and secondary NICs
- Allows NVAs to enforce different security policies based on the NICs and also provide bandwidth isolation among different traffic types
- Configured using the Azure portal, PowerShell, Azure CLI or ARM templates

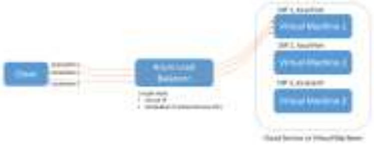
Forced Tunneling

- Force all traffic from a subnet to a VNet gateway
- Allows scenario for inspection and auditing of traffic
- Can create a routing table to create a default route, then associate routing table to VNet subnets



Source IP Affinity

- Azure Load Balancer – new distribution mode = Source IP Affinity
- Load balance traffic based on 2 or 3 tuple modes



Scenarios

- Configure load balancer distribution to an endpoint on a VM via PowerShell/Service Management API
- Configure load balancer distribution for your Load-Balanced Endpoint Sets via PowerShell/Service Management API.
- Configure load balancer distribution for your Web/Worker roles via the Service model (.csdef file)

User Defined Routing

- By default, Azure provides a route table based on your virtual network settings
- Need for custom routing may include
  - Use of a virtual appliance in your Azure environment, ex. Firewall
  - Implementing a virtual NAT appliance to control traffic between your Azure virtual network and the Internet
  - BGP Route – if you are using ExpressRoute, you can enable BGP to propagate routes from your on-premises network to Azure

Ex. - All traffic directed to the mid-tier and backed subnets initiated from the front end subnet goes through a virtual firewall appliance

Azure Application Gateway

- Azure Application Gateway is a web traffic (OSI layer 7 – HTTP and HTTPS) load balancer that enables you to manage traffic to your web applications
- Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port
- With Application Gateway you can be even more specific e.g. you can route traffic based on the incoming URL, so if /images is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images or if /video is in the URL, that traffic is routed to another pool optimized for videos

Azure Application Gateway

- The following features are included with Azure Application Gateway:
- Secure Sockets Layer (SSL) termination
  - Application gateway supports SSL termination at the gateway, after which traffic typically flows unencrypted to the backend servers
- Connection draining
  - Connection draining helps you achieve graceful removal of backend pool members during planned service updates
- Custom error pages
  - Application Gateway allows you to create custom error pages instead of displaying default error pages. You can use your own branding and layout using a custom error page

Azure Application Gateway

- Web Application Firewall
  - Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities. WAF is based on rules from the OWASP (Open Web Application Security Project) core rule sets 3.0 or 2.2.9
- URL-based routing
  - URL Path Based Routing allows you to route traffic to back-end server pools based on URL Paths of the request. One of the scenarios is to route requests for different content types to different pool
- Multiple-site hosting
  - Multiple-site hosting enables you to configure more than one web site on the same Application Gateway instance. This feature allows you to configure a more efficient topology for your deployments by adding up to 100 web sites to one application gateway

Azure Application Gateway

- Redirection
  - A common scenario for many web applications is to support automatic HTTP to HTTPS redirection to ensure all communication between an application and its users occurs over an encrypted path
- Session Affinity
  - The cookie-based session affinity feature is useful when you want to keep a user session on the same server. By using gateway-managed cookies, the Application Gateway can direct subsequent traffic from a user session to the same server for processing
- Websocket and HTTP/2 traffic
  - Application Gateway provides native support for the WebSocket and HTTP/2 protocols. There's no user-configurable setting to selectively enable or disable WebSocket support

Azure Application Gateway

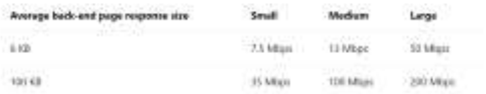
- Rewrite HTTP headers
  - HTTP headers allow a client and server to pass additional information with a request or response, by rewriting these headers, you can accomplish important tasks, such as adding security-related header fields like HSTS/ X-XSS-Protection, removing response header fields that might reveal sensitive information, and removing port information from X-Forwarded-For headers
  - Available only in the new SKU Standard_v2

How Azure Application Gateway works

- The client resolves the Application Gateways IP address using DNS, the frontend IP address of the Application Gateway is returned to the client
- The client sends a request for access to the resource at the resolved IP address
- The Application Gateway accepts incoming traffic on one or more listeners, a listener is a logical entity that checks for connection requests
- If Web Application Firewall (WAF) is enabled, the Application Gateway checks the request headers and the body (if present) against the WAF rules to determine whether the request is a valid request
- If the request is found to be valid, the request routing rule associated with the listener is evaluated to determine the backend pool to which the request is to be routed
- If the backend pool contains more than one server, the Application Gateway uses the round robin algorithm to route the requests between the healthy servers
- After a backend server has been determined, the Application Gateway opens a new TCP session with the backend server based on the configuration in the HTTP settings

Sizing

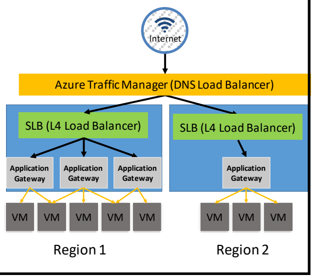
- Application Gateway is currently offered in three sizes: **Small**, **Medium**, and **Large**. Small instance sizes are intended for development and testing scenarios
- The following table shows an average performance throughput for each Application Gateway instance with SSL offload enabled:



Average back-end page response size	Small	Medium	Large
6 KB	7.5 Mbps	13 Mbps	50 Mbps
100 KB	35 Mbps	100 Mbps	200 Mbps

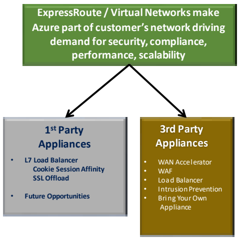
Application Gateway – LB Hierarchy

Azure Service	What	Example
Traffic Manager	Cross-region redirection & availability	http://news.com ➔ apac.news.com ➔ emea.news.com ➔ us.news.com
SLB	In-region scalability & availability	emea.news.com ➔ AppGw1 ➔ AppGw2 ➔ AppGw2
Application Gateway	URL/content-based routing & load balancing	news.com/topnews news.com/sports news.com/images
VMs	Web Servers	



Network Appliances

- Overview
  - VMs that perform specific network functions
  - Focus: Security (Firewall, IDS , IPS), Router/VPN, ADC (Application Delivery Controller), WAN Optimization
  - Typically Linux or FreeBSD-based platforms
  - 1st and 3rd Party Appliances
- Scenarios
  - IT Policy & Compliance – Consistency between on premises & Azure
  - Supplement/complement Azure capabilities
- Azure Marketplace
  - Available through Azure Certified Program to ensure quality and simplify deployment
  - You can also bring your own appliance and license



ExpressRoute / Virtual Networks make Azure part of customer's network driving demand for security, compliance, performance, scalability

1st Party Appliances

- L7 Load Balancer
  Cookie Session Affinity
  SSL Offload
- Future Opportunities

3rd Party Appliances

- WAN Accelerator
- WAF
- Load Balancer
- Intrusion Prevention
- Bring Your Own Appliance

Azure DDoS Protection

- DDoS Protection is a feature that monitors live network traffic and constantly compares it to thresholds that are defined in a DDoS Policy
- When the traffic threshold is exceeded, DDoS mitigation is automatically initiated
- During mitigation, traffic sent to the protected resource is redirected by the DDoS protection service and several checks are performed, such as:
  - Ensure packets conform to internet specifications and are not malformed
  - Interact with the client to determine if the traffic is potentially a spoofed packet (e.g: SYN Auth or SYN Cookie or by dropping a packet for the source to retransmit it)
  - Rate-limit packets, if no other enforcement method can be performed

Microsoft Confidential

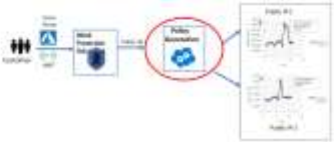
Azure DDoS Protection Tiers

- There are two DDoS Protection tiers:
  - Basic: Automatically enabled as part of the Azure platform, at no additional charge and uses a static global DDoS policy for virtual networks
  - Protection is provided for IPv4 and IPv6 Azure public IP addresses
  - Standard: Enabled at an additional cost were dynamic DDoS policies are tuned through dedicated traffic monitoring and machine learning algorithms
  - Policies are applied to public IP addresses associated to resources deployed in virtual networks, such as Azure Load Balancer, Azure Application Gateway, and Azure Service Fabric instances
  - Layer 3 to layer 7 protection covering over 60 different attack types
  - Protection is provided for IPv4 Azure public IP addresses

Microsoft Confidential

Azure DDoS Protection Testing

- Use BreakingPoint Cloud to build an interface where you can generate traffic against DDoS Protection-enabled public IP addresses for simulations
- Simulation allows you to:
  - Validate how Microsoft Azure DDoS Protection Standard protects your Azure resources from DDoS attacks
  - Optimize your incident response process while under DDoS attack
  - Document DDoS compliance
  - Train your network security teams



Microsoft Confidential

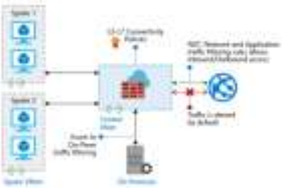
Azure DDoS Protection Metrics

- Diagnostic information can be collected using:
  - **Archival to a storage account:** Data is written to an Azure Storage account
  - **Streaming to an event hub:** Allows a log receiver to pick up logs using an Azure Event Hub. Event hubs enable integration with Splunk or other SIEM systems
  - **Sending to Log Analytics:** Writes logs to the Azure OMS Log Analytics service
- Telemetry for an attack is provided through Azure Monitor in real time

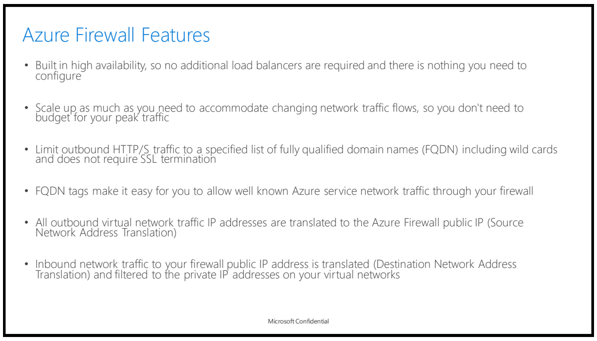
Microsoft Confidential

Azure Firewall

- Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources
- It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability
- Centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks
- Uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network
- Fully integrated with Azure Monitor for logging and analytics

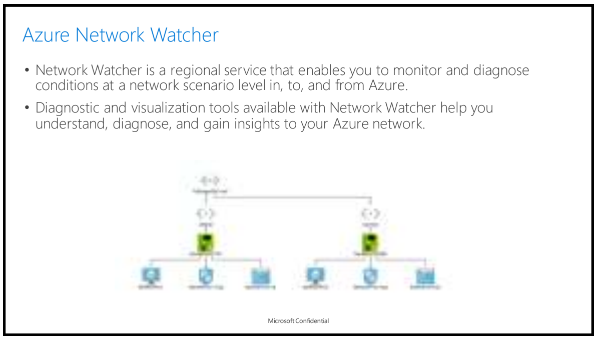


Microsoft Confidential



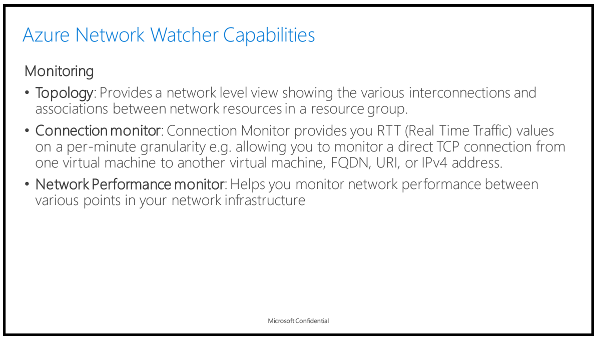
Azure Firewall Features

- Built in high availability, so no additional load balancers are required and there is nothing you need to configure
- Scale up as much as you need to accommodate changing network traffic flows, so you don't need to budget for your peak traffic
- Limit outbound HTTP/S traffic to a specified list of fully qualified domain names (FQDN) including wild cards and does not require SSL termination
- FQDN tags make it easy for you to allow well known Azure service network traffic through your firewall
- All outbound virtual network traffic IP addresses are translated to the Azure Firewall public IP (Source Network Address Translation)
- Inbound network traffic to your firewall public IP address is translated (Destination Network Address Translation) and filtered to the private IP addresses on your virtual networks



Azure Network Watcher

- Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure.
- Diagnostic and visualization tools available with Network Watcher help you understand, diagnose, and gain insights to your Azure network.



Azure Network Watcher Capabilities

Monitoring

- Topology: Provides a network level view showing the various interconnections and associations between network resources in a resource group.
- Connection monitor: Connection Monitor provides you RTT (Real Time Traffic) values on a per-minute granularity e.g. allowing you to monitor a direct TCP connection from one virtual machine to another virtual machine, FQDN, URI, or IPv4 address.
- Network Performance monitor: Helps you monitor network performance between various points in your network infrastructure

Azure Network Watcher Capabilities

Network Diagnostic tools

- IP flow verify: IP flow verify checks if a packet is allowed or denied to or from a virtual machine
- Next hop: Determines the next hop for packets being routed in the Azure Network Fabric.
- Effective security rules: Allows you to view the effective security rules and their associated network security groups that have been applied to a network interface
- VPN troubleshoot: Allows you to diagnose any issues with your Gateway and Connections and within minutes have enough information to make an informed decision to rectify the issue
- Packet capture: Captures packet data in and out of a virtual machine.
- Connection troubleshoot: Troubleshoots connectivity issues between two networks.

Microsoft Confidential

Azure Network Watcher Capabilities

Logs

- NSG flow logs: Captures logs related to traffic that is allowed or denied by the security rules in the group
- Diagnostic logs: Allows you to enable diagnostic logging for Azure networking resources such as network security groups, public IP addresses, load balancers, virtual network gateways, and application gateways
- Traffic Analytics: Provides rich visualizations of data written to NSG flow logs

Microsoft Confidential

Demo: Azure DDoS Protection & Azure Network Watcher

Microsoft