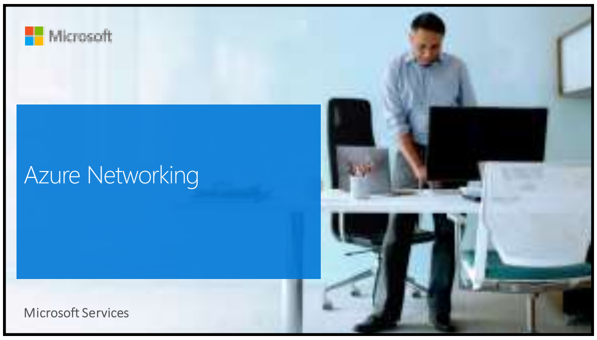
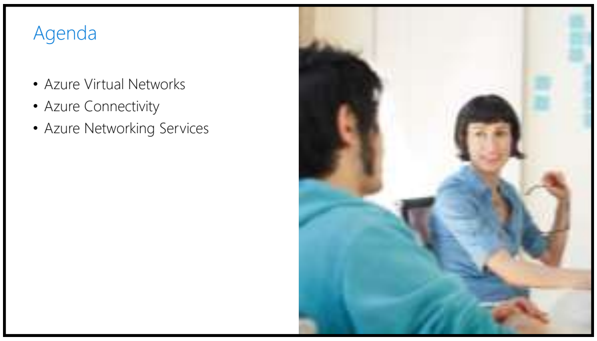


Microsoft

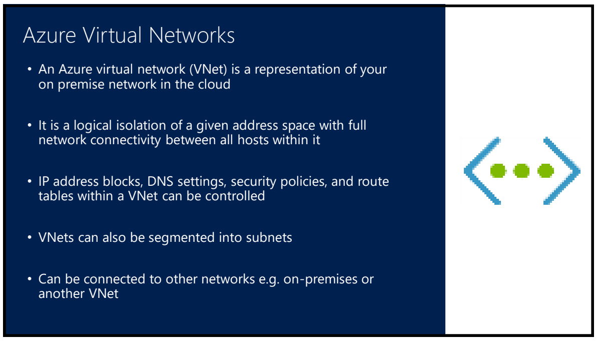
Azure Networking

Microsoft Services



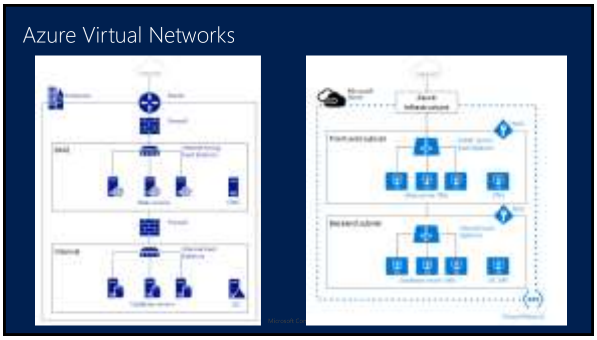
Agenda

- Azure Virtual Networks
- Azure Connectivity
- Azure Networking Services

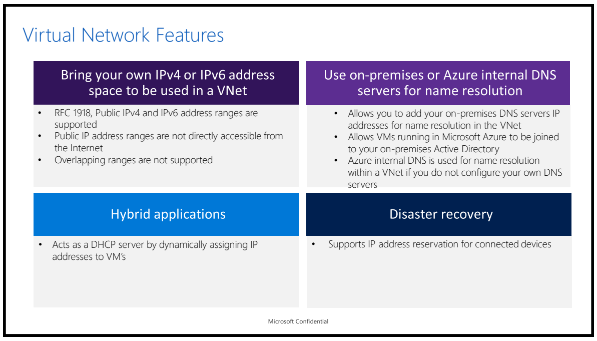


Azure Virtual Networks

- 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



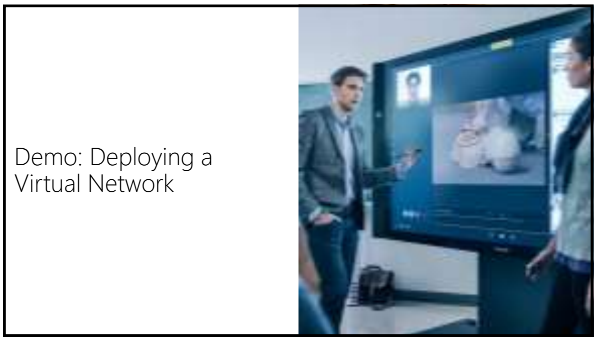
Azure Virtual Networks



Virtual Network Features

Bring your own IPv4 or IPv6 address space to be used in a VNet	Use on-premises or Azure internal DNS servers for name resolution
• RFC 1918, Public IPv4 and IPv6 address ranges are supported • Public IP address ranges are not directly accessible from the Internet • Overlapping ranges are not supported	• 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
Hybrid applications	**Disaster recovery**
• Acts as a DHCP server by dynamically assigning IP addresses to VM's	• Supports IP address reservation for connected devices

Microsoft Confidential

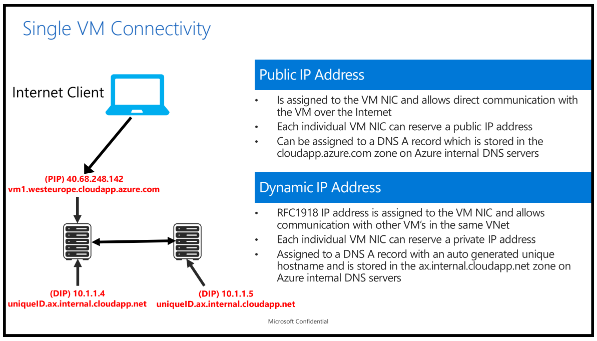


Demo: Deploying a Virtual Network

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

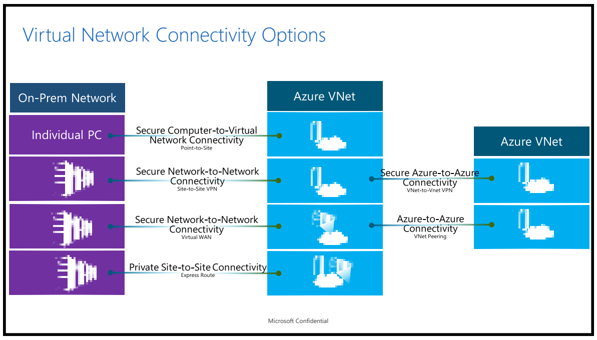
Public IP Address

- Is assigned to the VM NIC and allows direct communication with the VM over the Internet
- Each individual VM NIC can reserve a 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

- RFC1918 IP address is assigned to the VM NIC and allows communication with other VM's in the same VNet
- Each individual VM NIC can reserve a 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

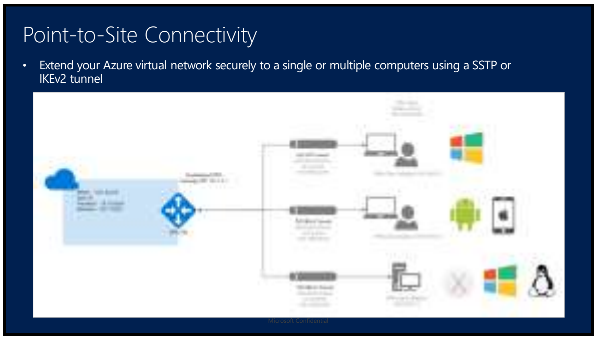
Microsoft Confidential



Virtual Network Connectivity Options

On-Prem Network
Azure VNet
Azure VNet
Individual PC
Secure Computer-to-Virtual Network Connectivity
Point-to-Site
Secure Network-to-Network Connectivity
Site-to-Site VPN
Secure Azure-to-Azure Connectivity
VNet-to-Vnet VPN
Secure Network-to-Network Connectivity
Virtual WAN
Azure-to-Azure Connectivity
VNet Peering
Private Site-to-Site Connectivity
Express Route

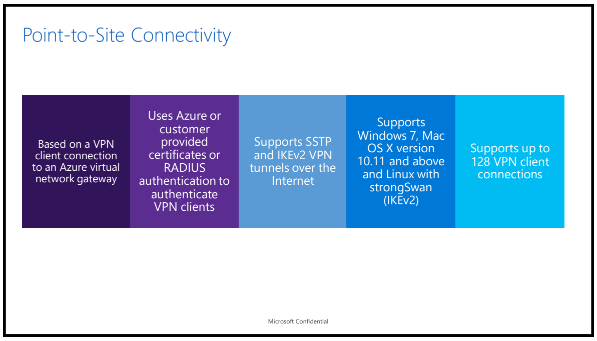
Microsoft Confidential



Point-to-Site Connectivity

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

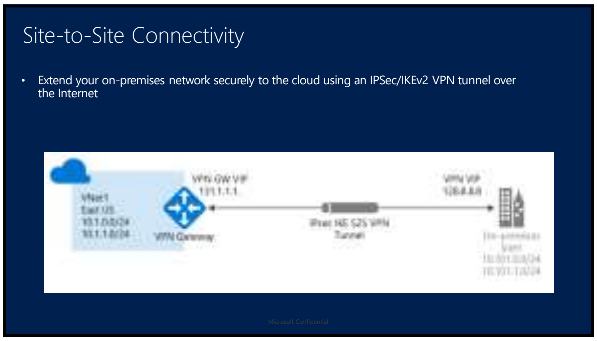
Microsoft Confidential



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

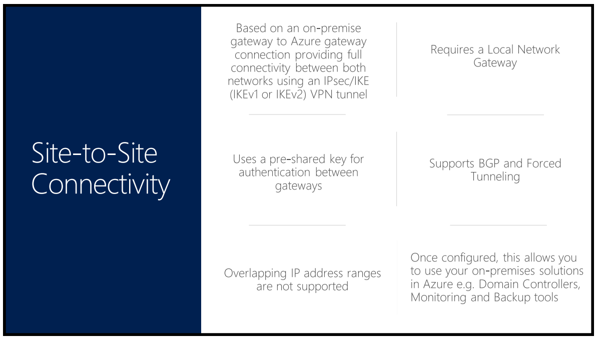
Microsoft Confidential



Site-to-Site Connectivity

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

Microsoft Confidential



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

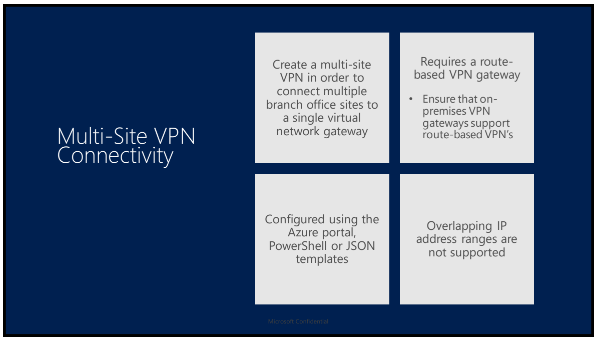
Requires a Local Network Gateway

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

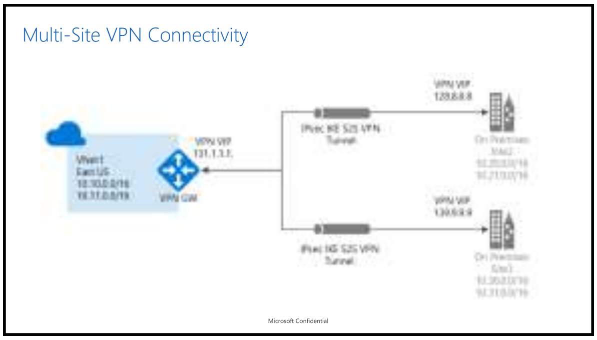
Requires a route-based VPN gateway

- Ensure that on-premises VPN gateways support route-based VPN's

Configured using the Azure portal, PowerShell or JSON templates

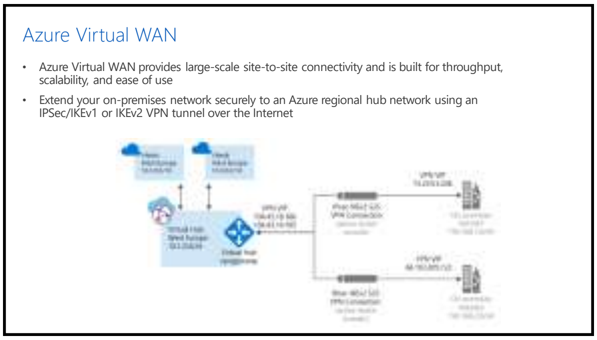
Overlapping IP address ranges are not supported

Microsoft Confidential



Multi-Site VPN Connectivity

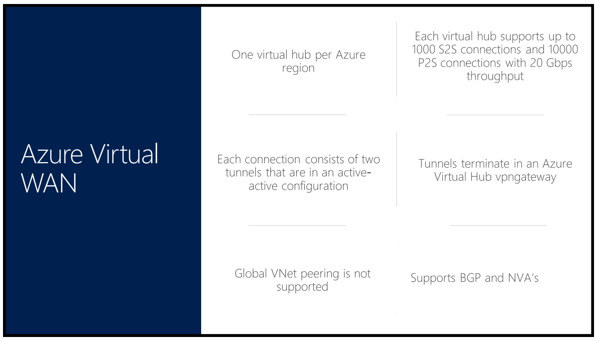
Microsoft Confidential



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

Virtual Hub
Virtual hub vpngateway
VPN site
VPN site
VPN site
VPN Connection
VPN Connection



Azure Virtual WAN

One virtual hub per Azure region

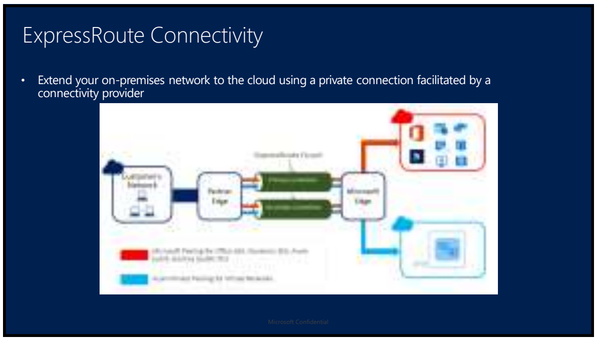
Each virtual hub supports up to 1000 S2S connections and 10000 P2S connections with 20 Gbps throughput

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

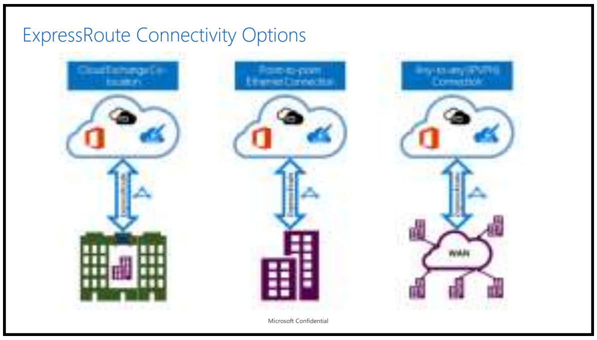
Supports BGP and NVA's



ExpressRoute Connectivity

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

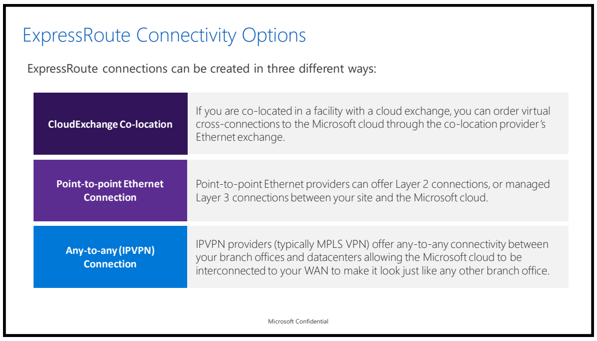
ExpressRoute Circuit
Customer's Network
Partner Edge
Microsoft Edge



ExpressRoute Connectivity Options

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

Microsoft Confidential

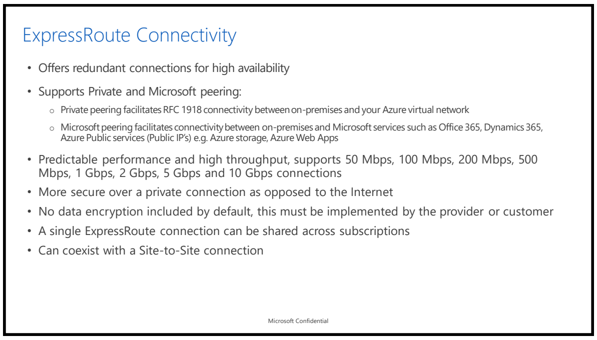


ExpressRoute Connectivity Options

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



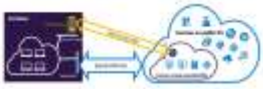
ExpressRoute Connectivity

- 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

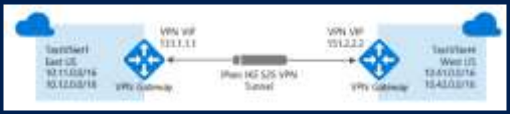
ExpressRoute & Site-to-Site coexistence

- 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



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

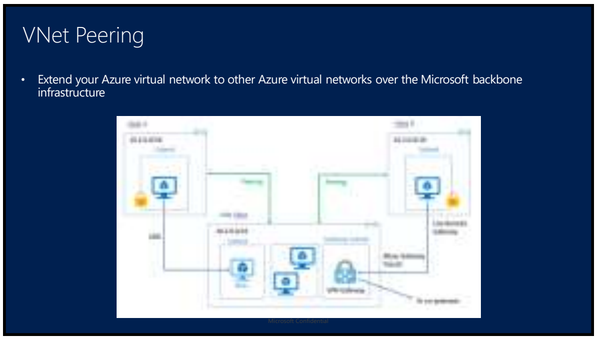
Automatically created and populated Local Network Gateway

Uses a pre-shared key for authentication between gateways

Supports BGP and Forced Tunneling

Overlapping IP address ranges are not supported

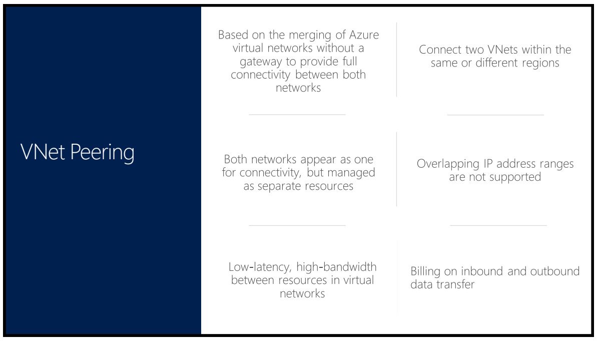
Once configured, this allows you to extend your Azure virtual network to other Azure virtual networks e.g. a partner



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

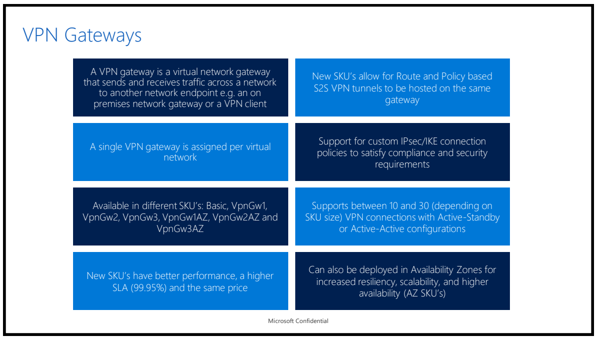
Connect two VNets within the same or different regions

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



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

New SKU's allow for Route and Policy based S2S VPN tunnels to be hosted on the same gateway

A single VPN gateway is assigned per virtual network

Support for custom IPsec/IKE connection policies to satisfy compliance and security requirements

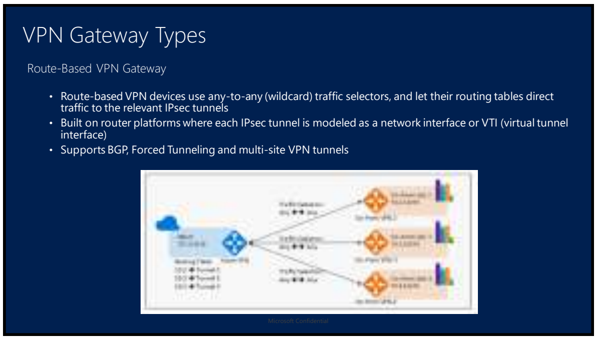
Available in different SKU's: Basic, VpnGw1, VpnGw2, VpnGw3, VpnGw1AZ, VpnGw2AZ and VpnGw3AZ

Supports between 10 and 30 (depending on SKU size) VPN connections with Active-Standby or Active-Active configurations

New SKU's have better performance, a higher SLA (99.95%) and the same price

Can also be deployed in Availability Zones for increased resiliency, scalability, and higher availability (AZ SKU's)

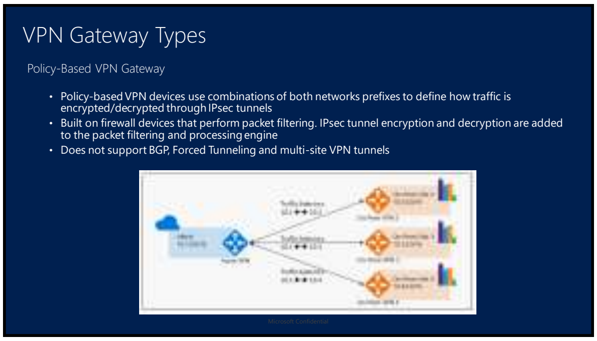
Microsoft Confidential



VPN Gateway Types

Route-Based VPN Gateway

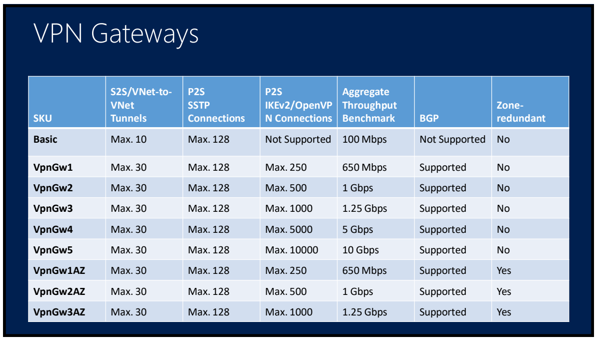
- Route-based VPN devices use any-to-any (wildcard) traffic selectors, and let their routing tables direct traffic to the relevant IPsec tunnels
- Built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface)
- Supports BGP, Forced Tunneling and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



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



VPN Gateways

SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP	Zone-redundant
Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported	No
VpnGw1	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	No
VpnGw2	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	No
VpnGw3	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	No
VpnGw4	Max. 30	Max. 128	Max. 5000	5 Gbps	Supported	No
VpnGw5	Max. 30	Max. 128	Max. 10000	10 Gbps	Supported	No
VpnGw1AZ	Max. 30	Max. 128	Max. 250	650 Mbps	Supported	Yes
VpnGw2AZ	Max. 30	Max. 128	Max. 500	1 Gbps	Supported	Yes
VpnGw3AZ	Max. 30	Max. 128	Max. 1000	1.25 Gbps	Supported	Yes

Virtual Network Service Endpoints

- Virtual network service endpoints extend your virtual network to Azure public facing services over a direct public connection
- Allows you to isolate internal network traffic to your critical Azure resources to only your virtual networks
- Traffic from your VNet to an Azure public service goes via the Internet but always remains on the Microsoft Azure backbone network
- Service endpoints available are:

Azure Storage
Azure SQL Database
Azure SQL Data Warehouse
Azure Database for PostgreSQL server
Azure Database for MySQL server
Azure Database for MariaDB
Azure Cosmos DB
Azure Key Vault
Azure Service Bus
Azure Event Hubs
Azure Data Lake Store Gen 1
Azure App Service

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

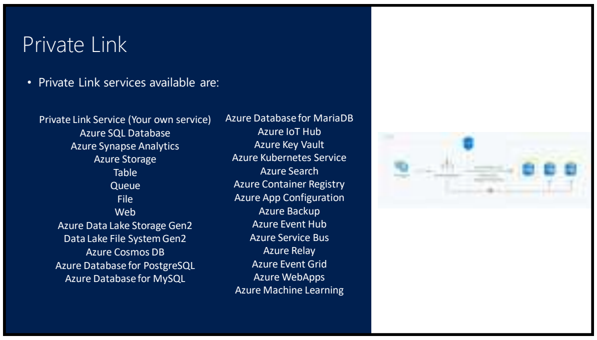
Service endpoint policies
0 selected

Subnets *
0 selected

[illegible]

Private Link

- Azure Private Link is similar to virtual network service endpoints in that it extends your virtual network to Azure public facing services but over a direct private connection
- Private Link also allows you to configure a specific resource that you would like to connect to e.g. only the blob service in a storage account as opposed to the entire storage account
- Traffic from your VNet to an Azure public service goes via the local area network

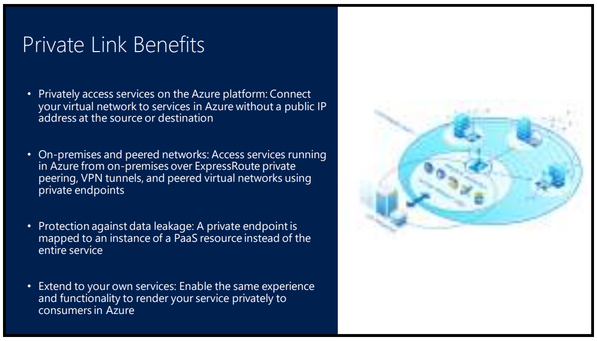


Private Link

- Private Link services available are:

Private Link Service (Your own service)
Azure SQL Database
Azure Synapse Analytics
Azure Storage
Table
Queue
File
Web
Azure Data Lake Storage Gen2
Data Lake File System Gen2
Azure Cosmos DB
Azure Database for PostgreSQL
Azure Database for MySQL

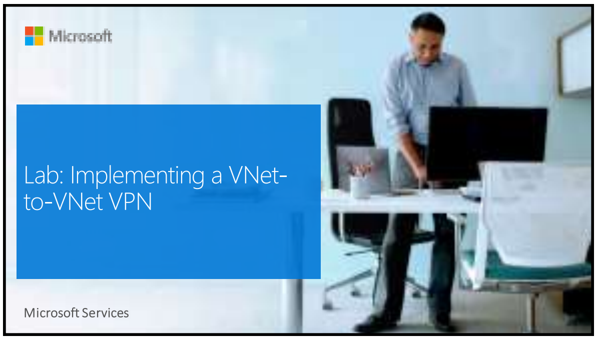
Azure Database for MariaDB
Azure IoT Hub
Azure Key Vault
Azure Kubernetes Service
Azure Search
Azure Container Registry
Azure App Configuration
Azure Backup
Azure Event Hub
Azure Service Bus
Azure Relay
Azure Event Grid
Azure WebApps
Azure Machine Learning



Private Link Benefits

- Privately access services on the Azure platform: Connect your virtual network to services in Azure without a public IP address at the source or destination
- On-premises and peered networks: Access services running in Azure from on-premises over ExpressRoute private peering, VPN tunnels, and peered virtual networks using private endpoints
- Protection against data leakage: A private endpoint is mapped to an instance of a PaaS resource instead of the entire service
- Extend to your own services: Enable the same experience and functionality to render your service privately to consumers in Azure

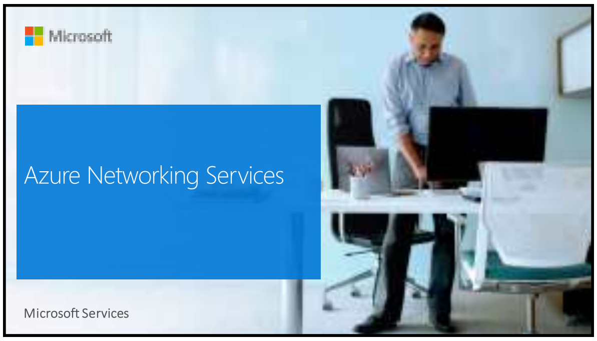
Demo: VNet Peering & Service Endpoints



Microsoft

Lab: Implementing a VNet-to-VNet VPN

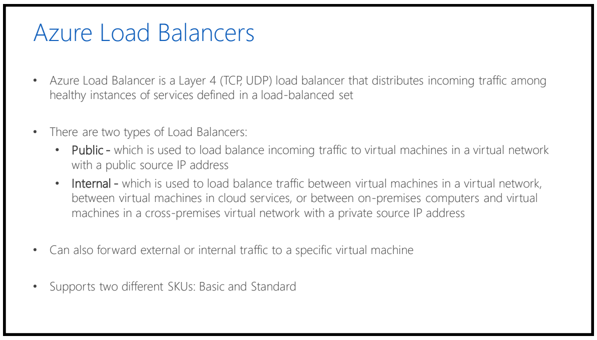
Microsoft Services



Microsoft

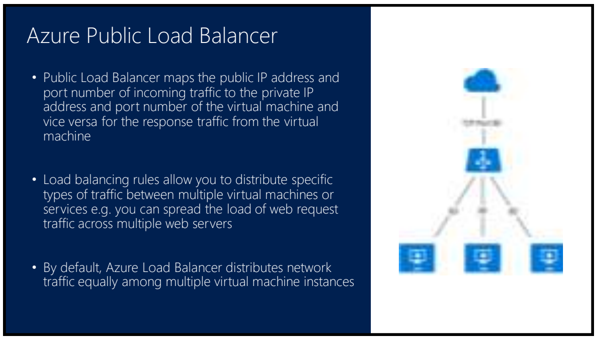
Azure Networking Services

Microsoft Services



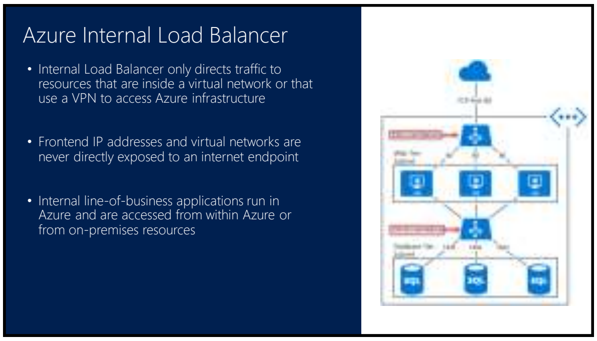
Azure Load Balancers

- 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



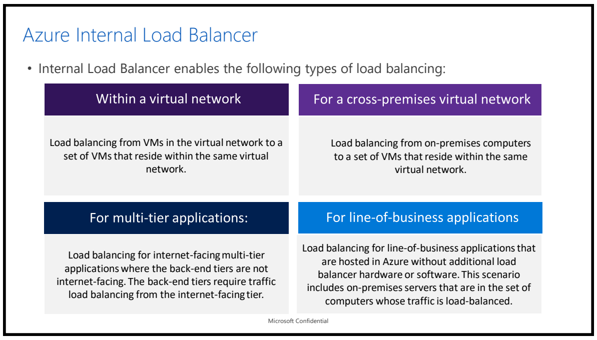
Azure Public Load Balancer

- 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



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

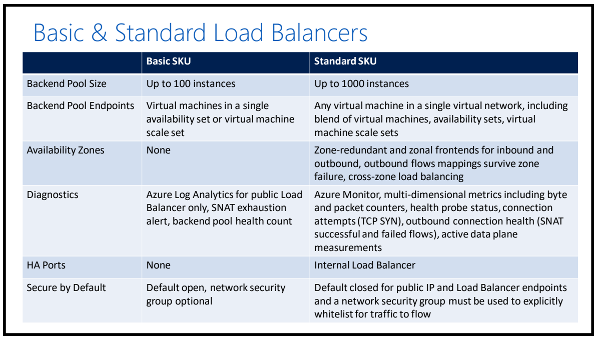


Azure Internal Load Balancer

- Internal Load Balancer enables the following types of load balancing:

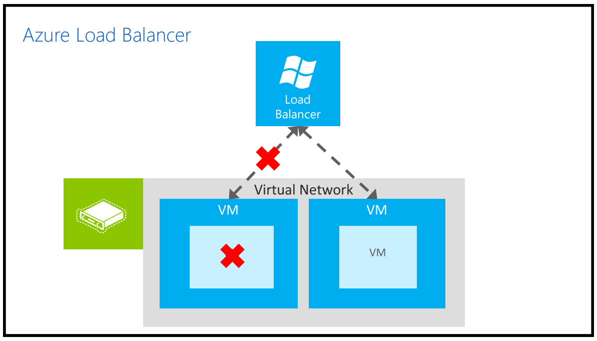
Within a virtual network	For a cross-premises virtual network
Load balancing from VMs in the virtual network to a set of VMs that reside within the same virtual network.	Load balancing from on-premises computers to a set of VMs that reside within the same virtual network.
For multi-tier applications:	**For line-of-business 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.	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.

Microsoft Confidential

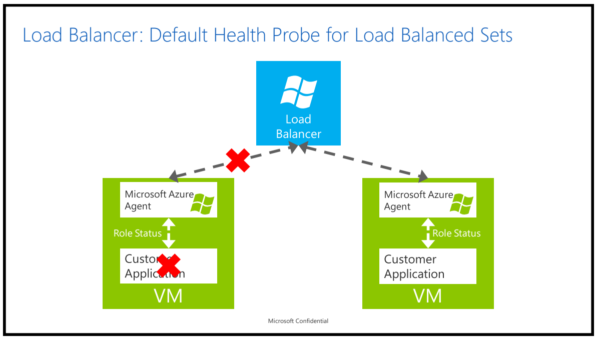


Basic & Standard Load Balancers

	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

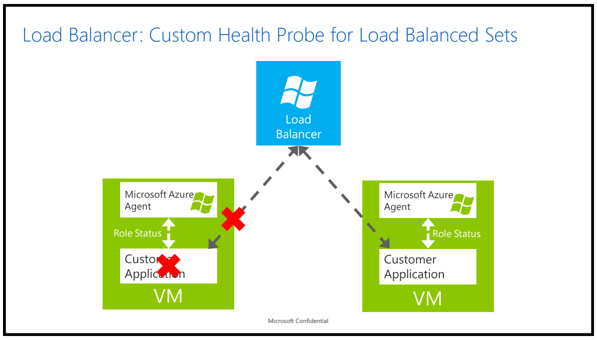


Azure Load Balancer



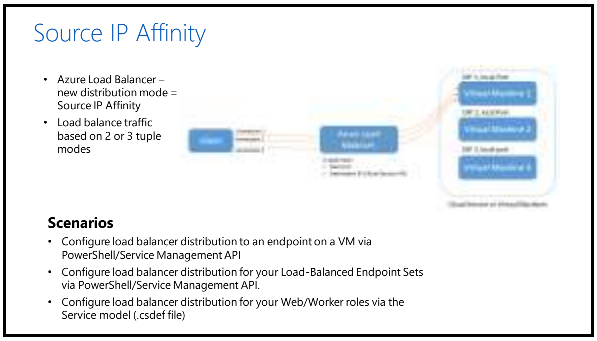
Load Balancer: Default Health Probe for Load Balanced Sets

Microsoft Confidential



Load Balancer: Custom Health Probe for Load Balanced Sets

Microsoft Confidential

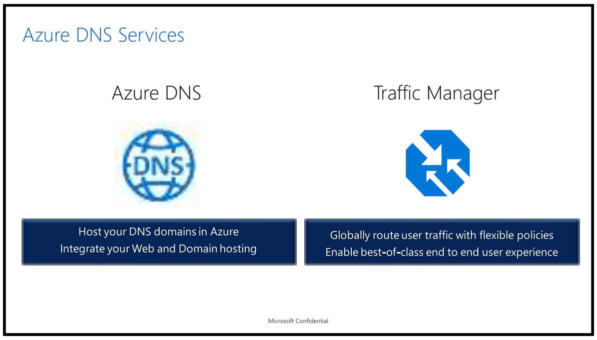


Source IP Affinity

- 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)

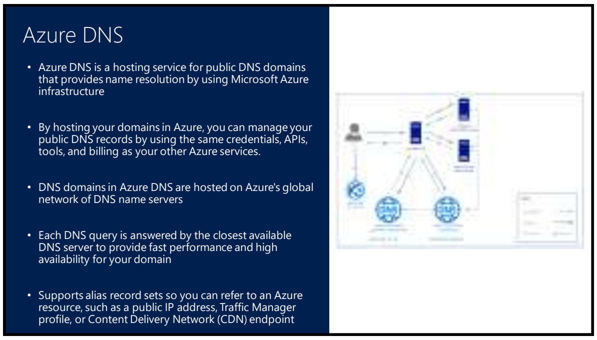


Azure DNS Services

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

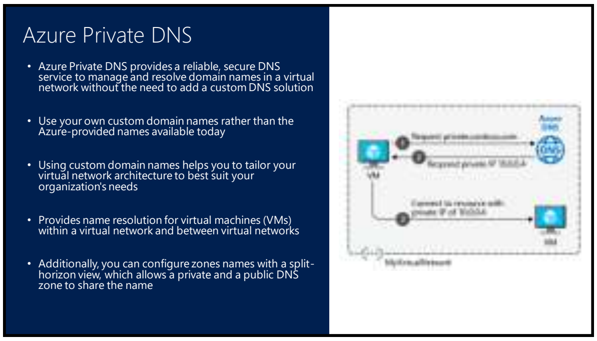
Globally route user traffic with flexible policies
Enable best-of-class end to end user experience

Microsoft Confidential



Azure DNS

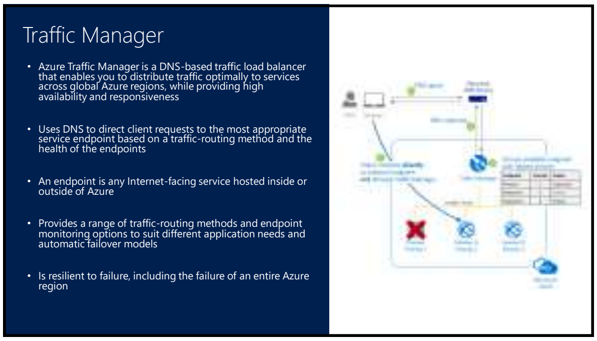
- Azure DNS is a hosting service for public DNS domains that provides name resolution by using Microsoft Azure infrastructure
- By hosting your domains in Azure, you can manage your public DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.
- DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers
- Each DNS query is answered by the closest available DNS server to provide fast performance and high availability for your domain
- Supports alias record sets so you can refer to an Azure resource, such as a public IP address, Traffic Manager profile, or Content Delivery Network (CDN) endpoint



Azure Private DNS

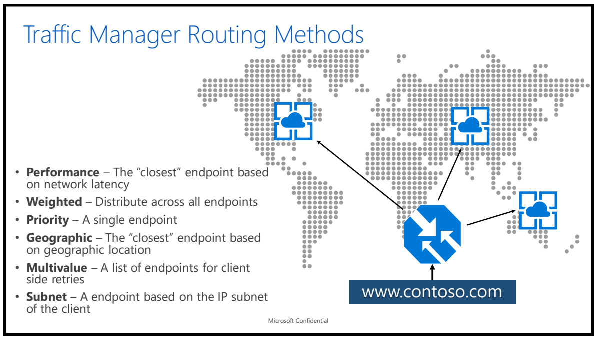
- Azure Private DNS provides a reliable, secure DNS service to manage and resolve domain names in a virtual network without the need to add a custom DNS solution
- Use your own custom domain names rather than the Azure-provided names available today
- Using custom domain names helps you to tailor your virtual network architecture to best suit your organization's needs
- Provides name resolution for virtual machines (VMs) within a virtual network and between virtual networks
- Additionally, you can configure zones names with a split-horizon view, which allows a private and a public DNS zone to share the name

Azure DNS
1
Request private.contoso.com
2
Respond private IP 10.0.0.4
DNS
VM
Connect to resource with private IP of 10.0.0.4
3
VM
MyVirtualNetwork



Traffic Manager

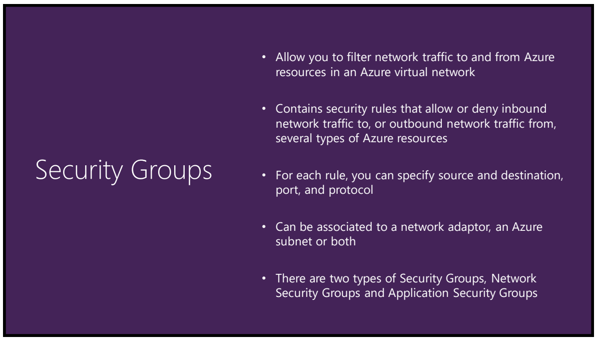
- Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness
- Uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints
- An endpoint is any Internet-facing service hosted inside or outside of Azure
- Provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models
- Is resilient to failure, including the failure of an entire Azure region



Traffic Manager Routing Methods

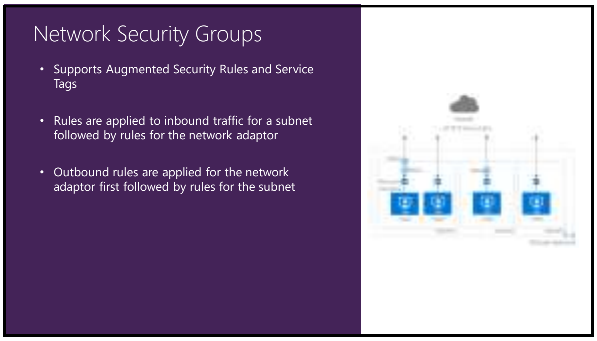
- **Performance** – The "closest" endpoint based on network latency
- **Weighted** – Distribute across all endpoints
- **Priority** – A single endpoint
- **Geographic** – The "closest" endpoint based on geographic location
- **Multivalue** – A list of endpoints for client side retries
- **Subnet** –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

Microsoft Confidential



Security Groups

- Allow you to filter network traffic to and from Azure resources in an Azure virtual network
- Contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources
- For each rule, you can specify source and destination, port, and protocol
- Can be associated to a network adaptor, an Azure subnet or both
- There are two types of Security Groups, Network Security Groups and Application Security Groups

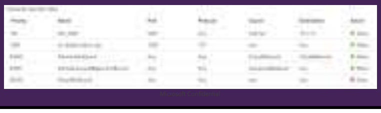


Network Security Groups

- Supports Augmented Security Rules and Service Tags
- Rules are applied to inbound traffic for a subnet followed by rules for the network adaptor
- Outbound rules are applied for the network adaptor first followed by rules for the subnet

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

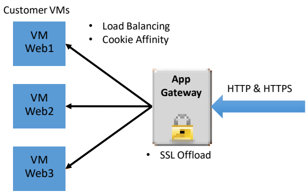


Application Security Groups

- Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups
- You can reuse your security policy at scale without manual maintenance of explicit IP addresses
- The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic

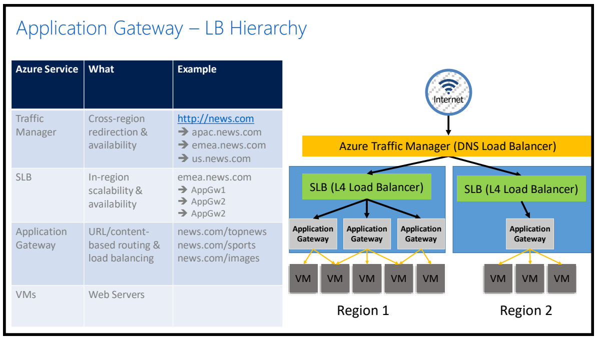
Azure Application Gateway

- Azure-managed, first-party virtual appliances
- HTTP routing based on app-level policies:
  - Cookie based session affinity
  - URL hash
  - Weight (load)
- SSL termination and caching
  - Centralize certificate management
  - Scalable backend provisioning



- Load Balancing
- Cookie Affinity

- SSL Offload



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	

Internet

Azure Traffic Manager (DNS Load Balancer)

SLB (L4 Load Balancer)

SLB (L4 Load Balancer)

Application Gateway

Application Gateway

Application Gateway

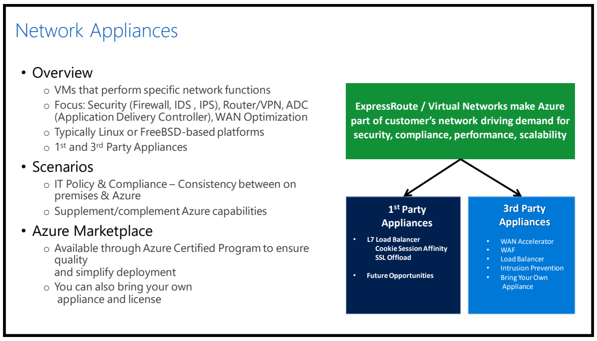
Application Gateway

VM VM VM VM VM

VM VM VM

Region 1

Region 2



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

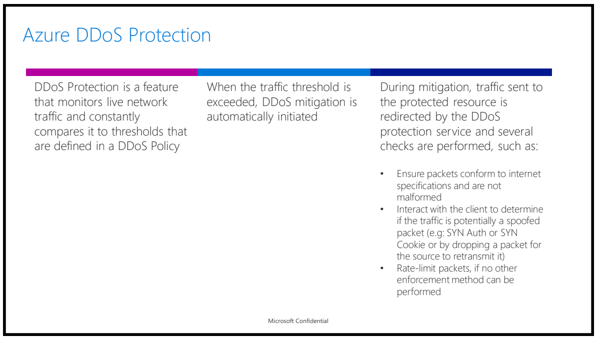
ExpressRoute / Virtual Networks make Azure part of customer's network driving demand for security, compliance, performance, scalability

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

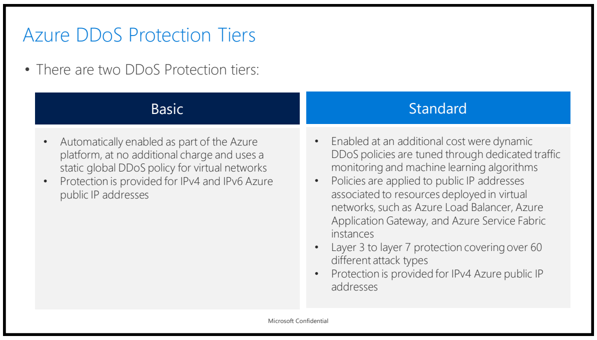
DDoS Protection is a feature that monitors live network traffic and constantly compares it to thresholds that are defined in a DDoS Policy

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

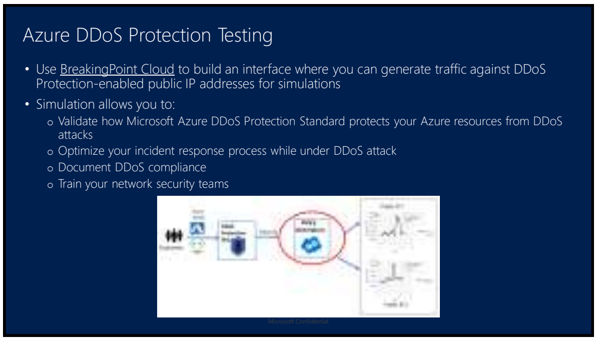


Azure DDoS Protection Tiers

- There are two DDoS Protection tiers:

Basic	Standard
• 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	• 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

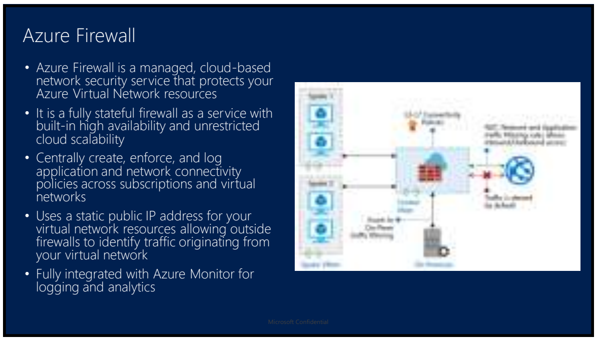
Microsoft Confidential



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

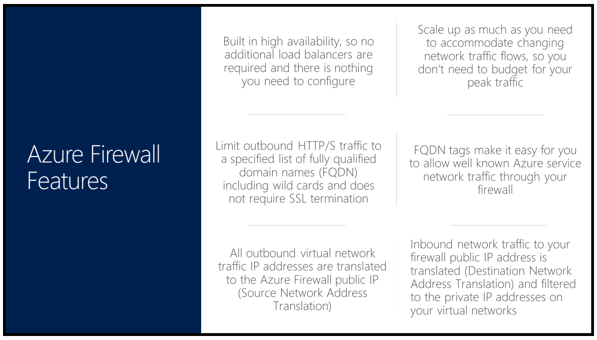
Microsoft Confidential



Azure 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

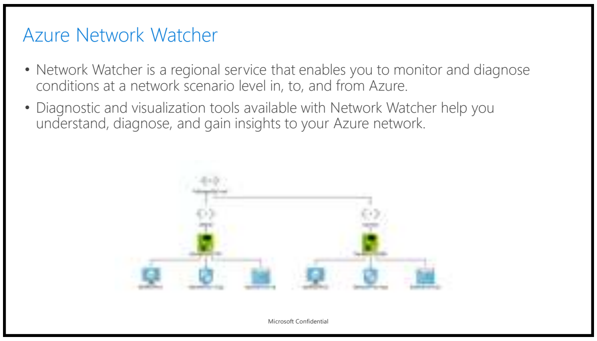
Scale up as much as you need to accommodate changing network traffic flows, so you don't need to budget for your peak traffic

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)

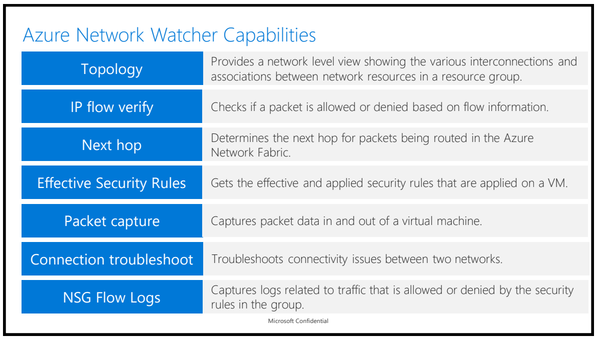
Inbound network traffic to your firewall public IP address is translated (Destination Network Address Translation) and filtered to the private IP addresses on your virtual networks



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.

Microsoft Confidential



Azure Network Watcher Capabilities

Topology	Provides a network level view showing the various interconnections and associations between network resources in a resource group.
IP flow verify	Checks if a packet is allowed or denied based on flow information.
Next hop	Determines the next hop for packets being routed in the Azure Network Fabric.
Effective Security Rules	Gets the effective and applied security rules that are applied on a VM.
Packet capture	Captures packet data in and out of a virtual machine.
Connection troubleshoot	Troubleshoots connectivity issues between two networks.
NSG Flow Logs	Captures logs related to traffic that is allowed or denied by the security rules in the group.

Microsoft Confidential

Demo: Azure DDoS Protection & Azure Network Watcher

Microsoft