Microsoft Azure: Infrastructure as a Service (IaaS)

Module 4: IaaS Virtual Networking

Azure Networking

Microsoft Azure Virtual Networks

- Your virtual branch office/data center in the cloud
  - Allows customers to extend their Enterprise Networks into Microsoft Azure
  - Networking on-ramp for migrating existing apps and services to Microsoft Azure
  - Allows customers to run hybrid apps that span the cloud and their on-premises setup
- A protected private virtual network in the cloud
  - Allows customers to set up secure private IPv4 networks fully contained within Microsoft Azure
  - IP address persistence capability
  - Inter-service (Dynamic IP address) DIP-to-DIP communication ~ PaaS/IaaS communication

Virtual Network Features

- Customer-managed private virtual networks within Microsoft Azure
  - "Bring your own IPv4 addresses"
  - Provides control over placement of Microsoft Azure VMs and roles within the network
  - Stable IPv4 addresses for VMs
- Hosted VPN Gateway that enables site-to-site connectivity
  - Automated provisioning and management
  - Support existing on-premises VPN devices
- Use on-premises DNS servers for name resolution or Azure DNS
  - Allows you to use your own on-premises DNS servers for name resolution
  - Allows VMs running in Microsoft Azure to be joined to corporate domains running on-premises (use your on-premises Active Directory)
- Can provide internal static IP addresses (via PowerShell) [DIP]
- Can provide public reserved IP addresses (via PowerShell) [VIP]
- Multiple virtual IP addresses per Cloud Service (classic) or per VM (V2) [ILPIP]

Microsoft Confidential

How to Setup Virtual Networks

- Portal
  - Wizard to create, and update virtual networks
  - Manage Gateway Lifecycle
- APIs and Scripting
  - REST APIs
  - PowerShell cmdlets
  - Network Configuration
- Operations on Network Configuration
  - Set Network Configuration
  - Get Network Configuration
- Azure Resource Manager (ARM) scripting/deployment

Microsoft Confidential

Configuring Virtual Networks
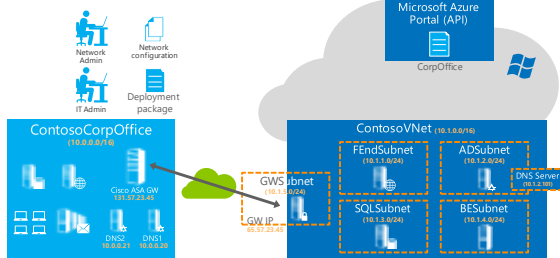
Microsoft Confidential

Demonstration: Deploying a Virtual Network

Module 4: IaaS Virtual Networking

Azure Connectivity

Glossary for Network basic components

- VIP (Virtual IP address)
  - A public IP address belongs to the cloud service. It also serves as an Azure Load Balancer which tells how network traffic should be directed before being routed to the VM.
  - It is possible to reserve an IP from the Microsoft pool
- DIP (Dynamic IP address):
  - An internal IP assigned by Microsoft Azure DHCP to the VM
  - Associated automatically with the VM when created
  - It is released when VM is deleted or deallocated (default)
  - It is possible to configure and static IP address
  - You can have more than one DIP per VM (Multi-NIC support)
- ILPIP (Instance Level Public IP)
  - A ILPIP is associated with the VM in addition to the VIP. Traffic to the ILPIP goes directly to the VM and is not routed through the Azure Load Balancer
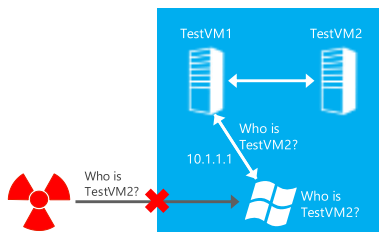
Glossary for Network basic components (con't)

- Azure Load Balancer (External LB)
  - All inbound traffic to the VIP is routed through the ELB which firewalls and distributes it. Allows only inbound TCP or UDP traffic. This is a software load balancer (SLB)
- Internal Load Balancer (ILB):
  - It is configured to port-forward or load-balance traffic inside a VNET or cloud service to different VMs.
- Endpoint (Classic)
  - Associates a VIP/DIP + port combination on a VM with a port on either the Azure Load Balancer for public-facing traffic or the Internal Load Balancer for traffic inside a VNET (or cloud service).
- Inbound Security Rule (V2)
  - Associated with a network security group. Associates a VIP/DIP + port combination on a VM with a port on either the Azure Load Balancer for public-facing traffic or the Internal Load Balancer for traffic inside a VNET
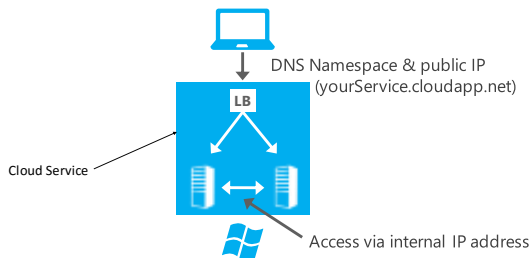
Microsoft Confidential

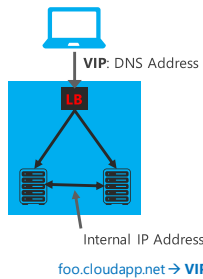## Microsoft Azure Provided DNS – Within a Cloud Service (Classic)

TestVM1   TestVM2

Who is TestVM2?
10.1.1.1

Who is TestVM2?

Who is TestVM2?

Microsoft Confidential

Overview: Basic Connectivity in Microsoft Azure (Classic)

DNS Namespace & public IP
(yourService.cloudapp.net)

LB

Cloud Service

Access via internal IP address

Microsoft Confidential

Overview: Existing Connectivity in Microsoft Azure (Classic)

VIP: DNS Address

DNS Address
- Load balanced endpoint. Stable VIP per service deployment
- Single port per endpoint with protocols HTTP, HTTPS, TCP
- Each individual VM can reserve a separate public IP address

Internal IP Addresses
- Instance-to-instance communication in Cloud Service
- Supported Protocols: TCP
- Port ranges supported
- Communication boundary = Deployment boundary

Name Resolution
Microsoft Azure–provided DNS service for Cloud service–level name resolution

Internal IP Addresses

foo.cloudapp.net → **VIP**

Microsoft Confidential

Internal IP Addresses (Classic)
- Open by default with VMs (Firewalls are not)
- Allows all IP traffic to flow
- Open ICMPv4 port to ping
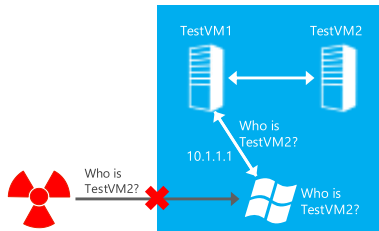- Can be used across Cloud Services within a single virtual network

Virtual Network

Cloud Service/Deployment

Cloud Service/Deployment 1

Cloud Service/Deployment 2

IP Traffic
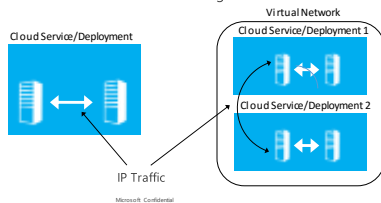
Microsoft Confidential

Virtual Machine Endpoints (Classic)
- VMs can automatically communicate with other VMs in the same cloud service or virtual network
- Endpoints 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
  - Windows PowerShell Remoting
  - Secure Shell (SSH)
- Each endpoint has a public port and a private port:
  - Public port: used by the Azure load balancer to listen for incoming traffic to the VM from the Internet
  - Private port: 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
  - Rules can allow or deny traffic from specific IPs and known IP address ranges
  - Rules are evaluated in order starting with the first rule and ending with the last rule
    - Rules should be ordered from least restrictive to most restrictive
  - If the virtual machine is in an Azure VNet, use Network Security Groups instead
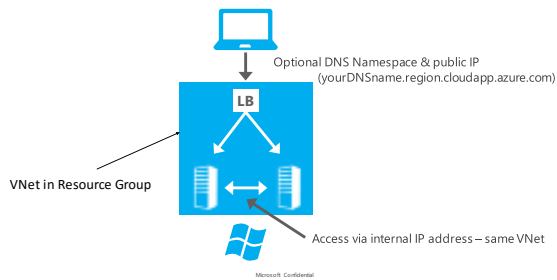
Microsoft Azure Provided DNS – Within a Virtual Network (V2)

TestVM1 TestVM2

Who is
TestVM2?

10.1.1.1

Who is
TestVM2?

Who is
TestVM2?

Microsoft Confidential

Overview: Basic Connectivity in Microsoft Azure (V2)

LB

Optional DNS Namespace & public IP
(yourDNSname.region.cloudapp.azure.com)

VNet in Resource Group

Access via internal IP address – same VNet

Microsoft Confidential

Overview: Existing Connectivity in Microsoft Azure (V2)

VIP: DNS Address

LB

Internal IP Addresses
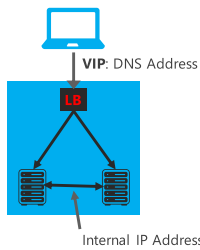
DNS Address

- Optional load balanced endpoint. Stable VIP per service deployment. You can choose not to have a VIP
- Single port per inbound security rule with protocols HTTP, HTTPS, TCP

Internal IP Addresses

- Instance-to-instance communication in same VNet
- Supported Protocols: TCP
- Port ranges supported
- Communication boundary = Deployment boundary

Name Resolution

Microsoft Azure-provided DNS service for VMs in the same virtual network/resource group

Dnsname.region.cloudapp.azure.com → **VIP**

Microsoft Confidential

Internal IP Addresses (V2)

- Open by default with VMs (Firewalls are not)
- Allows all IP traffic to flow
- Open ICMPv4 port to ping
- Can be used across VMs within a single virtual network

Microsoft Confidential
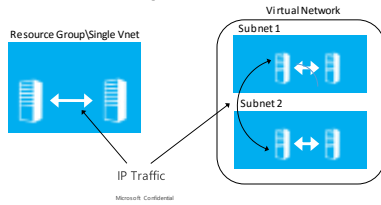
Virtual Machine Inbound Security Rules (V2)

- VMs can automatically communicate with other VMs in the same virtual network
- 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

Classic and V2 Comparison

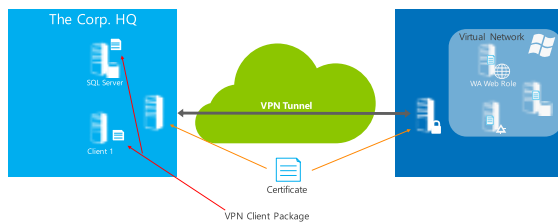|	Classic	V2
VM Container	Cloud Service	Resource Group + VNet
Region span	Single region	Multi-region
FQDN	Myapp.cloudapp.net	Optional - myDNS.region.cloudapp.azure.com
ILPIP	Optional - Supplied by Azure	Optional – supplied by Azure
VIP	Supplied by Azure	Optional – supplied by Azure
External Connectivity	Endpoints – RDP/SSH default	Inbound Security Rule – RDP by default
Virtual Network	Not required	Required
Azure DNS	Within Cloud Service	Within Virtual Network
API	REST / Azure Service Management	REST / Azure Resource Manager

Microsoft Confidential

Microsoft Azure External Connectivity Options

ENTERPRISE		CLOUD
	Data Synchronization Azure Data Factory	
	Application Layer Connectivity and Messaging Service Bus	
	Secure Machine-to-Machine Network Connectivity Point-to-Site (Classic Only)	
	Secure Site-to-Site Network Connectivity Microsoft Azure Virtual Network	
	Private Site-to-Site Connectivity Express Route	

Microsoft Confidential

Point-to-Site

The Corp. HQ

SQL Server

Client 1

VPN Tunnel

Certificate

VPN Client Package
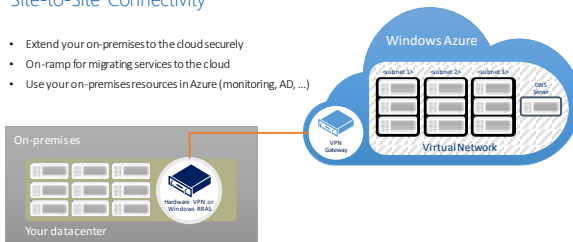
Virtual Network

WA Web Role

Microsoft Confidential
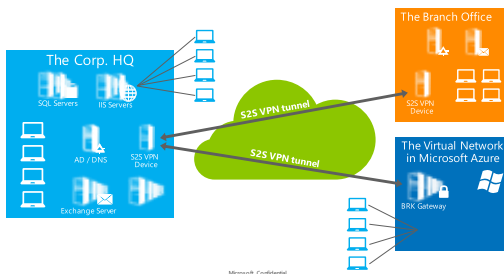

Site-to-Site Connectivity

- Extend your on-premises to the cloud securely
- On-ramp for migrating services to the cloud
- Use your on-premises resources in Azure (monitoring, AD, ...)

Windows Azure

subnet 1> subnet 2> subnet 3>

DNS Server

On-premises

VPN Gateway

Virtual Network

Hardware VPN or Windows RRAS

Your datacenter

Microsoft Confidential
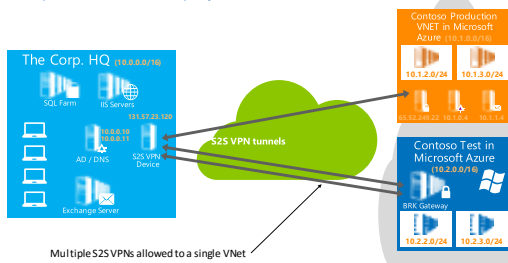
VPN Gateways

The Virtual Branch Office

Multi-Site VPN

- Create a multi-site VPN in order to connect multiple on-premises sites to a single virtual network gateway
- Requires dynamic routing configured on the VNet gateway
  - Can change the gateway type without needing to rebuild the virtual network to accommodate multi-site
  - Need to ensure on-premises VPN gateway supports dynamic routing VPN.
- Add configuration settings to the network configuration file
- Changes to the VNet won't be available through the Management Portal
  - Can use it for everything else except making configuration changes to this particular virtual network.

Microsoft Confidential

Example: Contoso's Deployment

The Corp. HQ **(10.0.0.0/16)**
SQL Farm   IIS Servers
131.57.23.120
10.0.0.10
10.0.0.11
AD / DNS   S2S VPN Device
S2S VPN tunnels
Exchange Server

Contoso Production VNET in Microsoft Azure (10.1.0.0/16)
10.1.2.0/24   **10.1.3.0/24**

Contoso Test in Microsoft Azure **(10.2.0.0/16)**
BRK Gateway
10.2.2.0/24   **10.2.3.0/24**

Multiple S2S VPNs allowed to a single VNet

Microsoft Confidential

VNet to VNet Connectivity

- Cross region geo-redundancy and geo-presence
  - You can set up your own geo-replication or synchronization with secure connectivity without going over internet-facing endpoints
  - With Azure Load Balancer and Microsoft or third party clustering technologies, you can setup highly available workloads with geo-redundancy across multiple Azure regions
- Regional multi-tier applications with strong isolation boundary
  - Within the same region, you can setup multi-tier applications with multiple virtual networks connected together with strong isolation and secure inter-tier communication
- Cross subscription, inter-organization communication in Azure
  - Connect workloads from different subscriptions together securely between virtual networks
  - Enable cross organization communication with secure VPN technology within Azure.

Microsoft Confidential

What is ExpressRoute?

ExpressRoute provides organizations a private, dedicated, high-throughput network connection between Windows Azure datacenters and their on-premises IT environment.
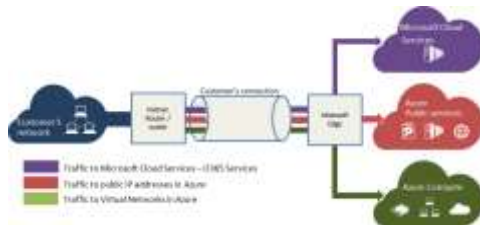
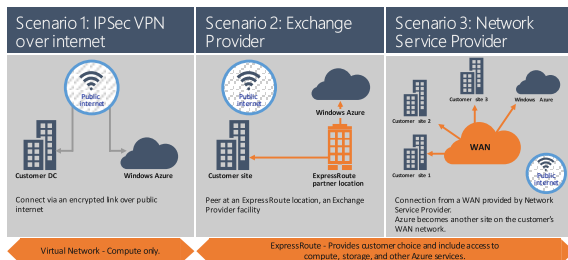| Predictable performance | ☑ |
Security	🔒
High throughput	
Lower cost	$

ExpressRoute Peerings

Public, Private and Microsoft peering

Virtual Network and ExpressRoute

Scenario 1: IPSec VPN over internet	Scenario 2: Exchange Provider	Scenario 3: Network Service Provider
Connect via an encrypted link over public internet	Peer at an ExpressRoute location, an Exchange Provider facility	Connection from a WAN provided by Network Service Provider. Azure becomes another site on the customer's WAN network.
Virtual Network - Compute only.	ExpressRoute - Provides customer choice and include access to compute, storage, and other Azure services.	

VPN GW S2S and ExpressRoute coexistence

- VPN gateway allows you to have Site-to-Site (S2S) VPN connectivity to a Virtual Network that also has a gateway connected to an ExpressRoute circuit.
- This enables new connectivity scenarios:
  - You can now use S2S VPN tunnel as a backup for your ExpressRoute connection.
  - You can connect branch offices that aren't part of your WAN to your Azure virtual networks that are also connected via ExpressRoute.
  - You can have Point-to-Site connections to the same Virtual Network that is also connected via ExpressRoute enabling dev/test and mobile worker scenarios.

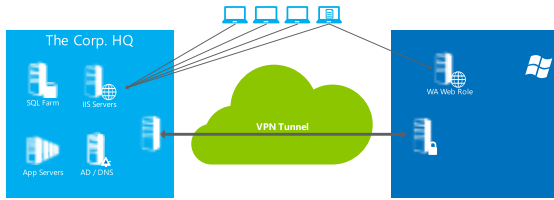Module 4: IaaS Virtual Networking

Networking Scenarios

Microsoft Confidential

Virtual Network Scenarios

- Hybrid Public/Private Cloud
  - Enterprise app in Microsoft Azure requiring connectivity to on-premises resources
- Enterprise Identity and Access Control
  - Manage identity and access control with on-premises resources (on-premises Active Directory)
- Monitoring and Management
  - Remote monitoring and troubleshooting of resources running in Microsoft Azure (SCOM)
- Advanced Connectivity Requirements
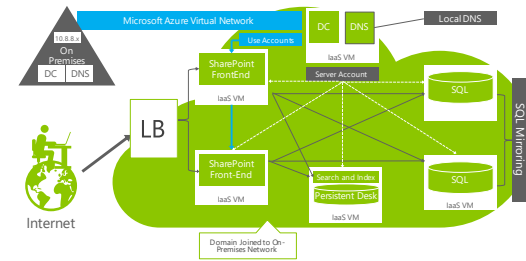 - Cloud deployments requiring persistent IP addresses and direct connectivity across services

Microsoft Confidential

Application Migration

The Corp. HQ

SQL Farm   IIS Servers

App Servers   AD / DNS

VPN Tunnel

WA Web Role

Microsoft Confidential

SharePoint in Microsoft Azure

Microsoft Azure Virtual Network

10.8.8.x
On Premises
DC   DNS

Use Accounts

DC   DNS   Local DNS

IaaS VM

SharePoint FrontEnd

IaaS VM

Server Account

SQL

LB

SharePoint Front-End

IaaS VM

Search and Index

Persistent Desk

IaaS VM

SQL

IaaS VM

SQL Mirroring

Internet

Domain Joined to On-Premises Network

Microsoft Confidential
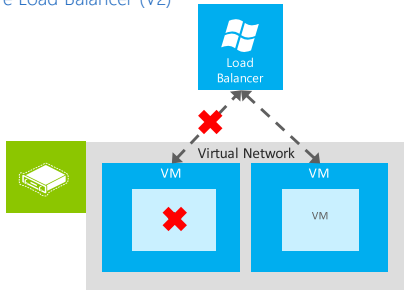
Module 4: IaaS Virtual Networking

High Availability
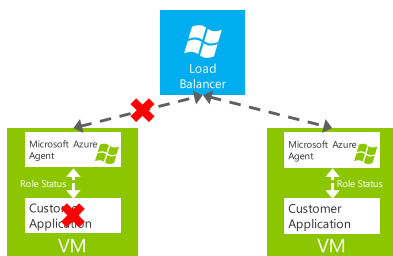
Microsoft Confidential

Azure Load Balancer (Classic)
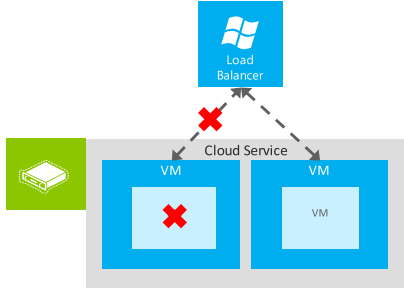
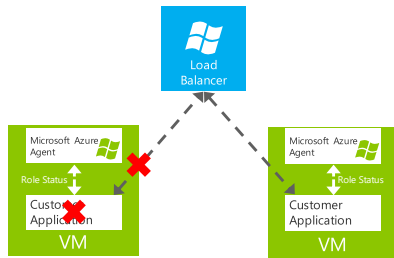
Azure Load Balancer (V2)

Load Balancer: Default Health Probe for Load Balanced Sets

## Load Balancer: Custom Health Probe for Load Balanced Sets

Azure Internal Load Balancer - ILB

- Provides load balancing for machines inside of a Cloud Service or Virtual network
  - Between virtual machines in the same Cloud Service (Classic)
  - Within a virtual network, from virtual machines in a virtual network to a set of virtual machines that reside within the same cloud service of the virtual network.
  - For a cross-premises virtual network, from on-premises computers to a set of virtual machines that reside within the same cloud service of the virtual network
  - Between virtual machines in a virtual network (V2)
- Using ILB
  - Internet-facing, multi-tier applications in which the back-end tiers are not Internet-facing but require load balancing for traffic from the Internet-facing tier.
  - Load balancing for line-of-business (LOB) applications hosted in Azure without requiring additional load balancer hardware or software.
- ILB Setup
  - PowerShell Only
    - Add-AzureInternalLoadBalancer
    - Add-AzureRMLoadBalancerFrontendIPConfig
    - Add-AzureRMLoadBalancerBackendAddressPoolConfig

ILB Scenario

- Intranet app running on Azure IaaS
- Cross-premises Azure virtual network
- Load balance not internet facing machines
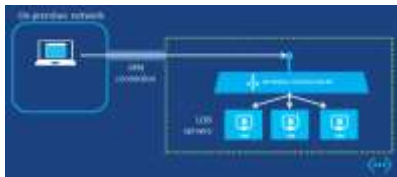
## Internet IP Addresses and Load Balancing

Public IP Addresses in Azure
- Can be used for instance (VM) level access or load balancing

Instance-level IP (ILPIP)
- Internet IP assigned exclusively to single VM Entire port range accessible by default
- Primarily for targeting a specific VM

Load balanced IP (VIP)
- Internet IP load balanced among one or more VM instances
- Allows port redirection
- Primarily for load balanced, highly available, or auto-scale scenarios
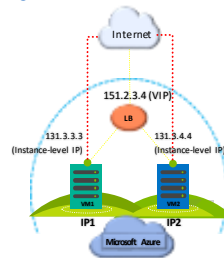
Microsoft Confidential

Azure DNS Services

Azure DNS *Preview*   Traffic Manager

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

Traffic Manager

Traffic Management Policies

- **Latency** – Direct to "closest" service
- **Round Robin** – Distribute across all services
- **Failover** – Direct to "backup" if primary fails
- **Nested** – Flexible multi-level policies

www.contoso.com
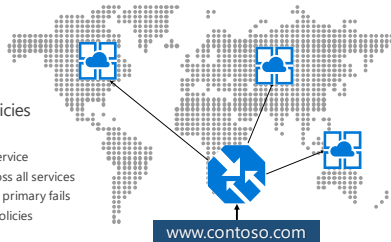
Microsoft Confidential

Module 03: IaaS Virtual Networking

Other Features

Microsoft Confidential

Network Security Groups (NSG)

- Define access control rules for inbound/outbound traffic to a VM 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 VM in a VNet
  - A subnet in a VNet
  - A VM 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)
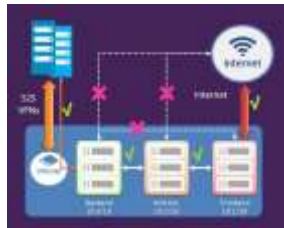
Network Security Groups (continued)

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


```
Example PowerShell:
New-AzureNetworkSecurityGroup -Name "MyVNetSG" -Location uswest
-Label "Security group for my Vnet in West US"

Get-AzureNetworkSecurityGroup -Name "MyVNetSG" | Set-
AzureNetworkSecurityRule -Name WEB -Type Inbound -Priority 100
-Action Allow -SourceAddressPrefix 'INTERNET' -SourcePortRange
'*' -DestinationAddressPrefix '*' -DestinationPortRange '*' -
Protocol TCP
```
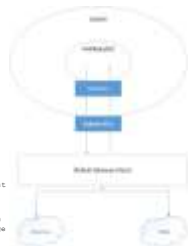
Multi-NIC Support

- Using multiple NICs on your VM allows you to manage network traffic better (16)
- 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-premise VM's with multiple NIC's migrated to Azure won't work – VM must be built in Azure

Forced Tunneling

- Force internet-bound traffic from a Cloud application back through on-premises network via Site-to-Site VPN/Express Route
- 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
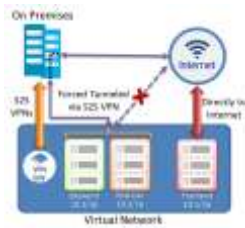
Source IP Affinity

- 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
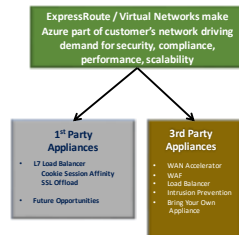

Module 4: IaaS Virtual Networking

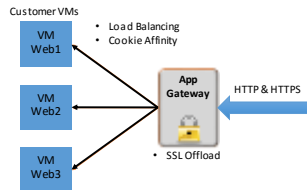Virtual Network Appliances

Microsoft Confidential

Virtual 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 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

Customer VMs

VM Web1

VM Web2

VM Web3

App Gateway

- Load Balancing
- Cookie Affinity

HTTP & HTTPS

- 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 (x3)   Application Gateway

VM VM VM VM VM   VM VM VM

Region 1   Region 2

Microsoft