

Windows Azure 虚拟网络

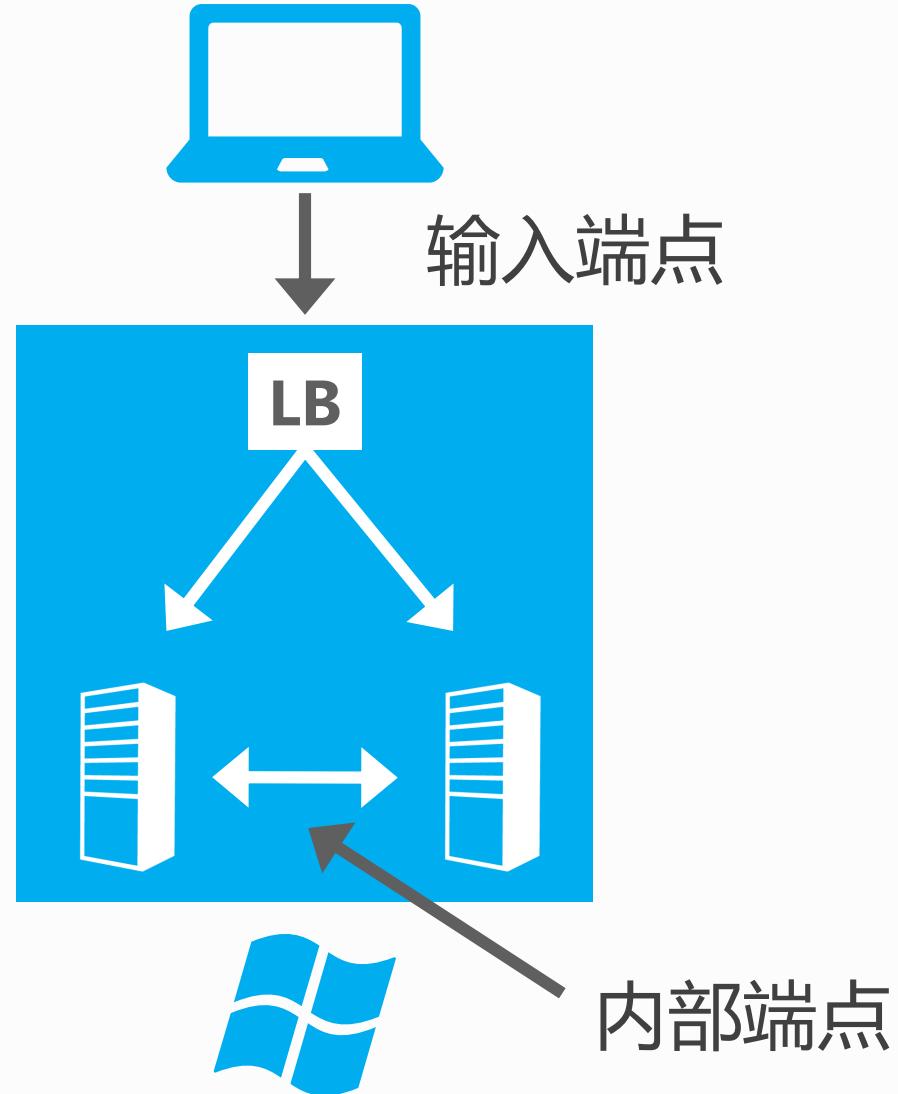
演讲者
职位
组织

日程

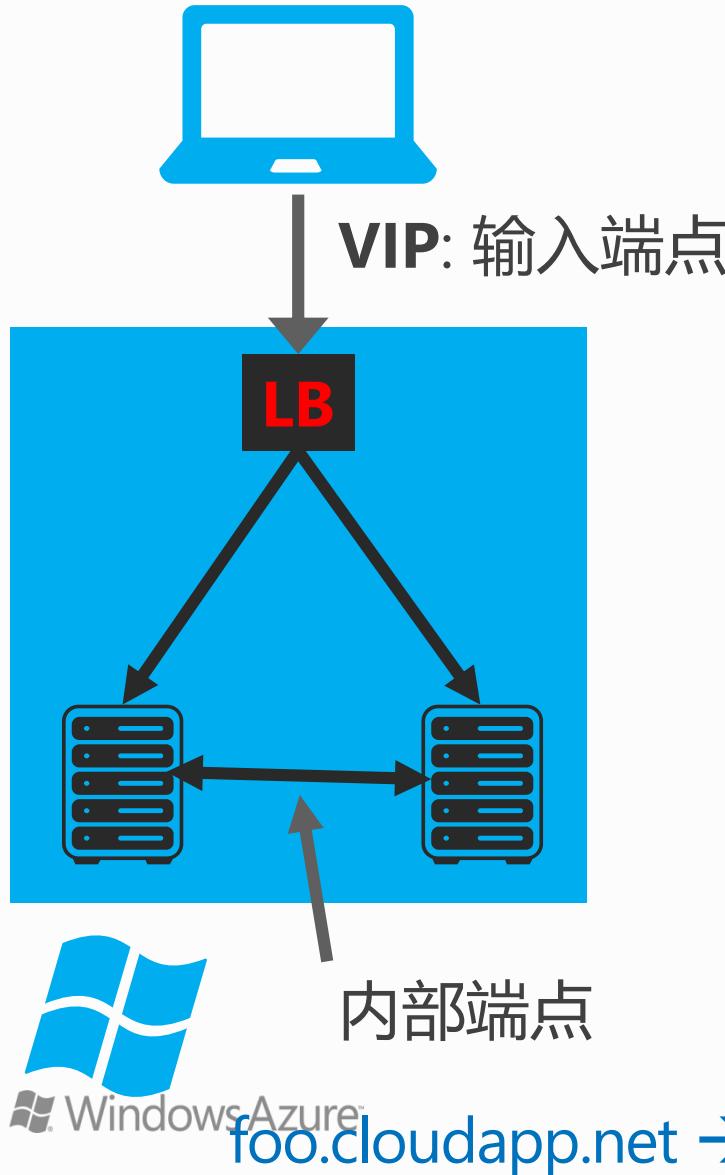


端点和连接性
负载均衡支持的新特性
DNS和名字解析

概述: Azure中的可连接性



概述: Azure中现有的连接



输入端点

负载均衡的端点. 稳定的每服务虚拟IP.
每个端点支持一个端口
支持的协议: HTTP, HTTPS, TCP

内部端点

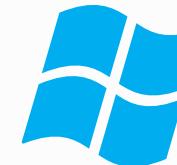
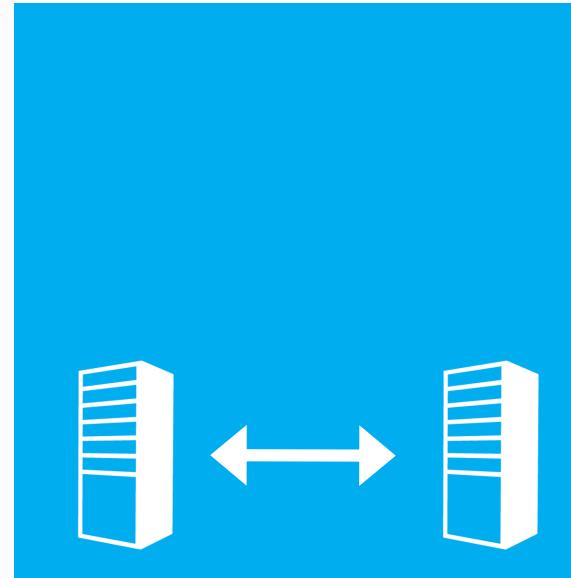
实例到实例的通讯
支持的协议: TCP
支持端口范围
通讯边界 = 开发边界

名称解析

Windows Azure为服务级别提供的DNS服务
为实例确认提供运行时API

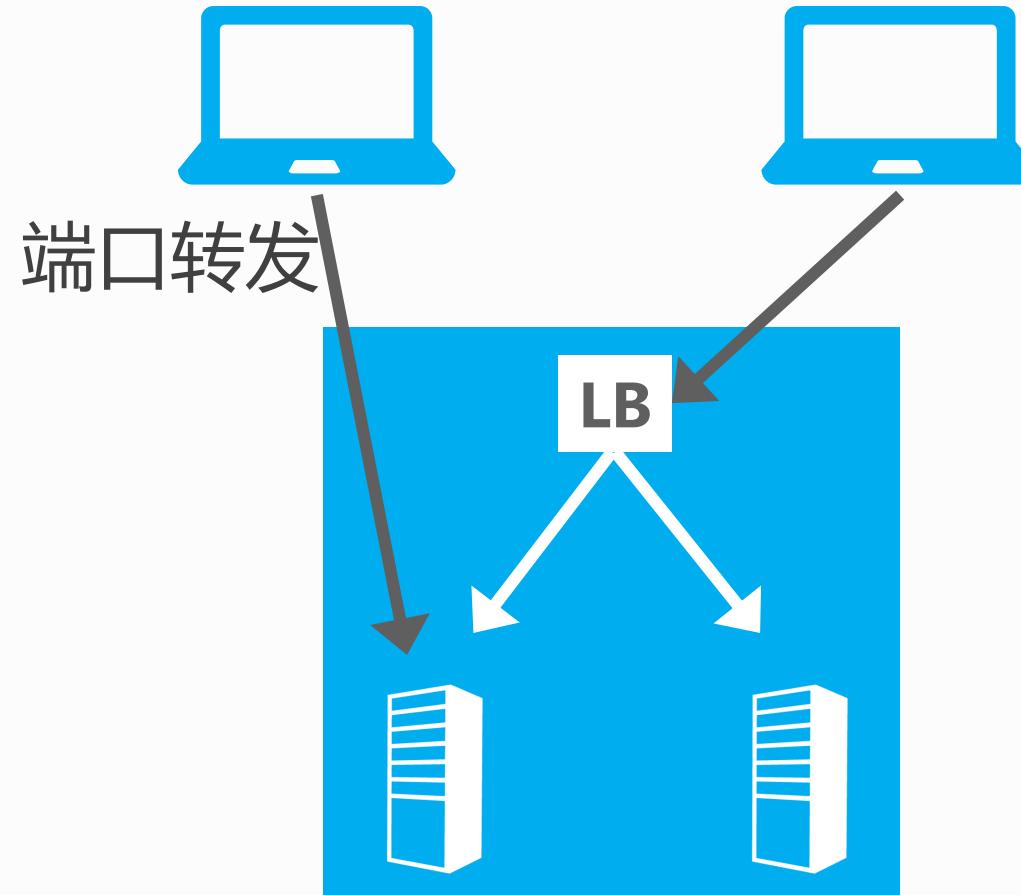
在部署中使用任何IP协议

默认内部VM之间端点是开放的
(防火墙不是)



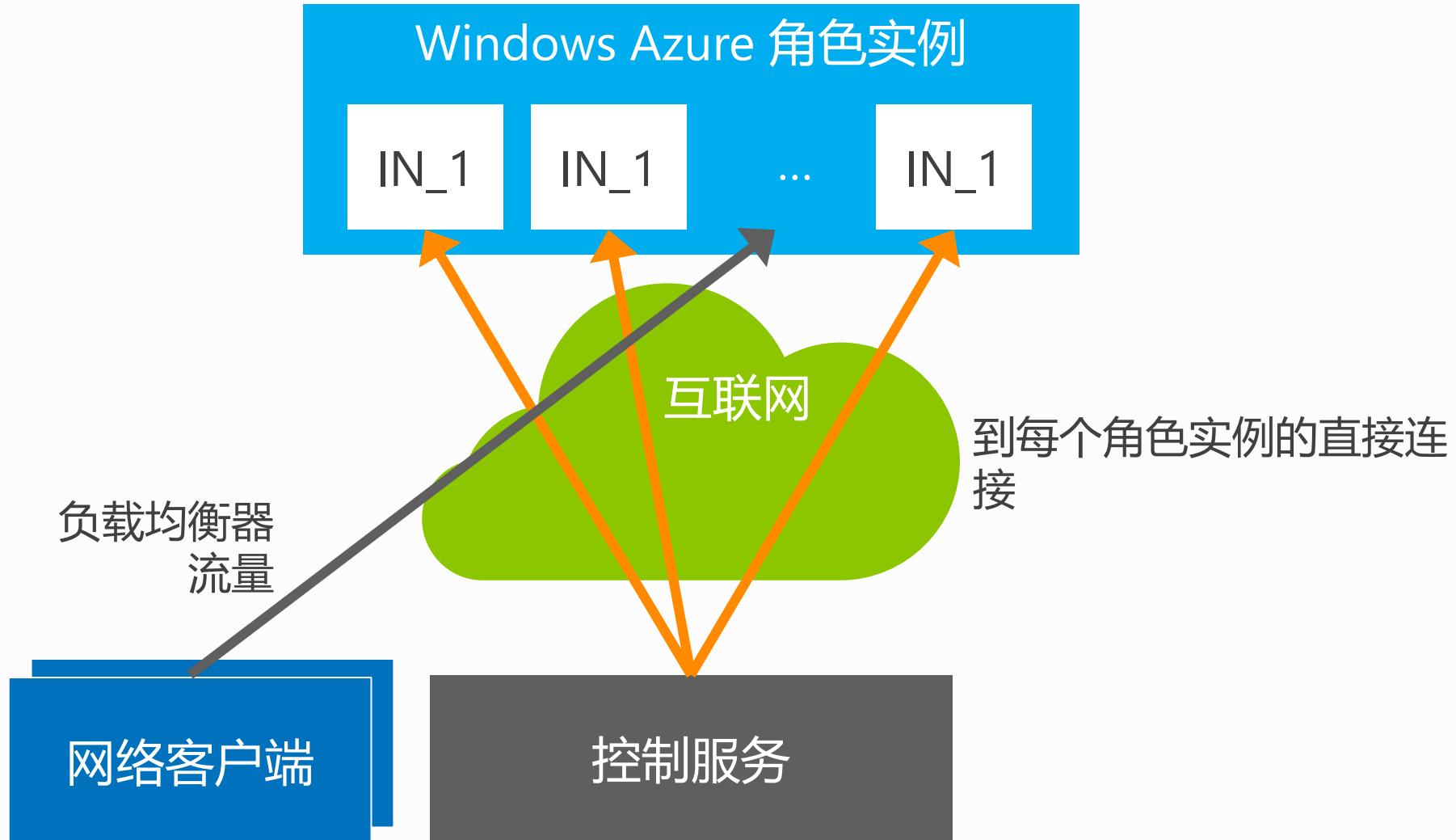
IP 流量

在部署中使用任何IP协议

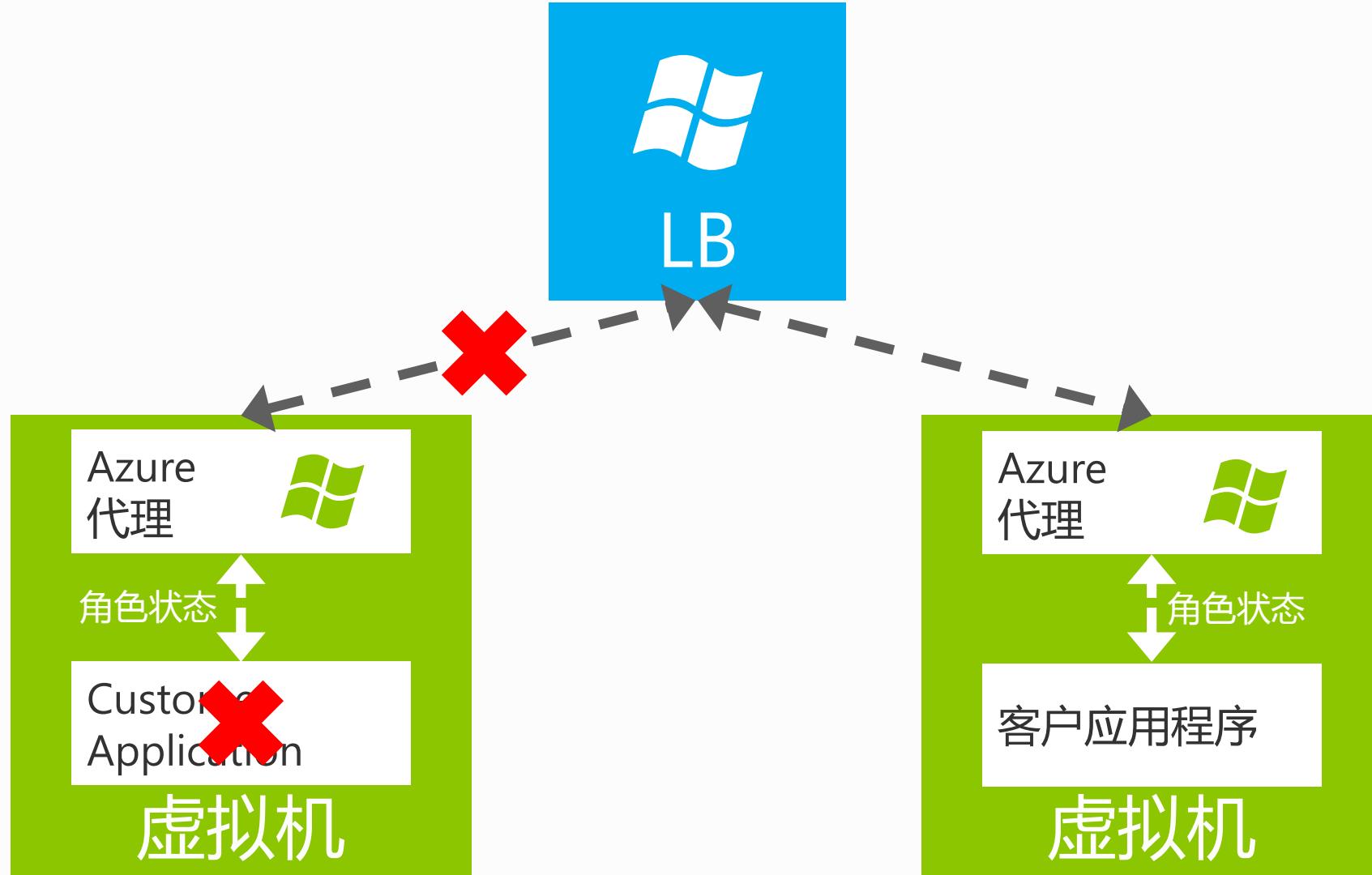


UDP 流量

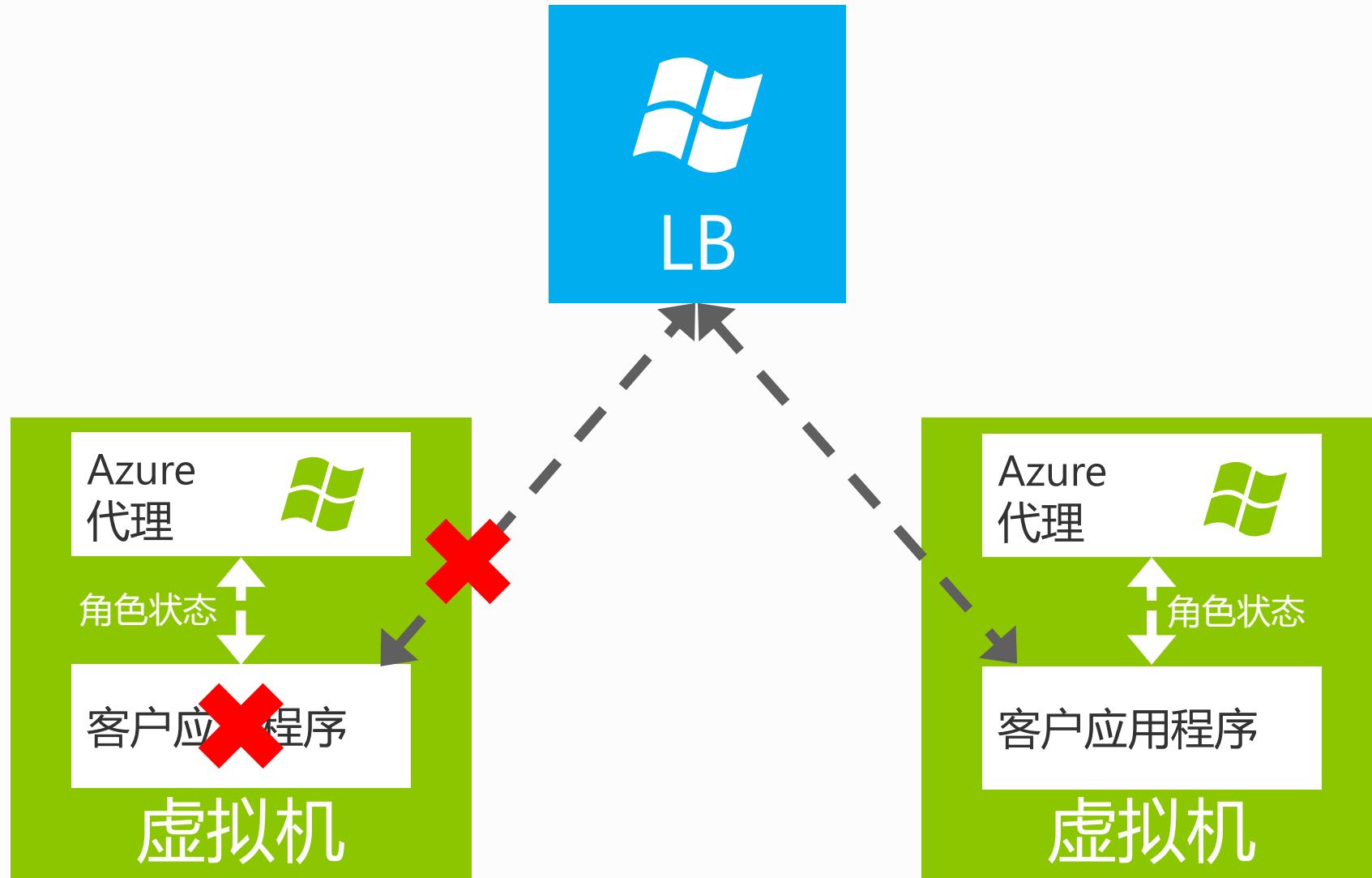
端口转发



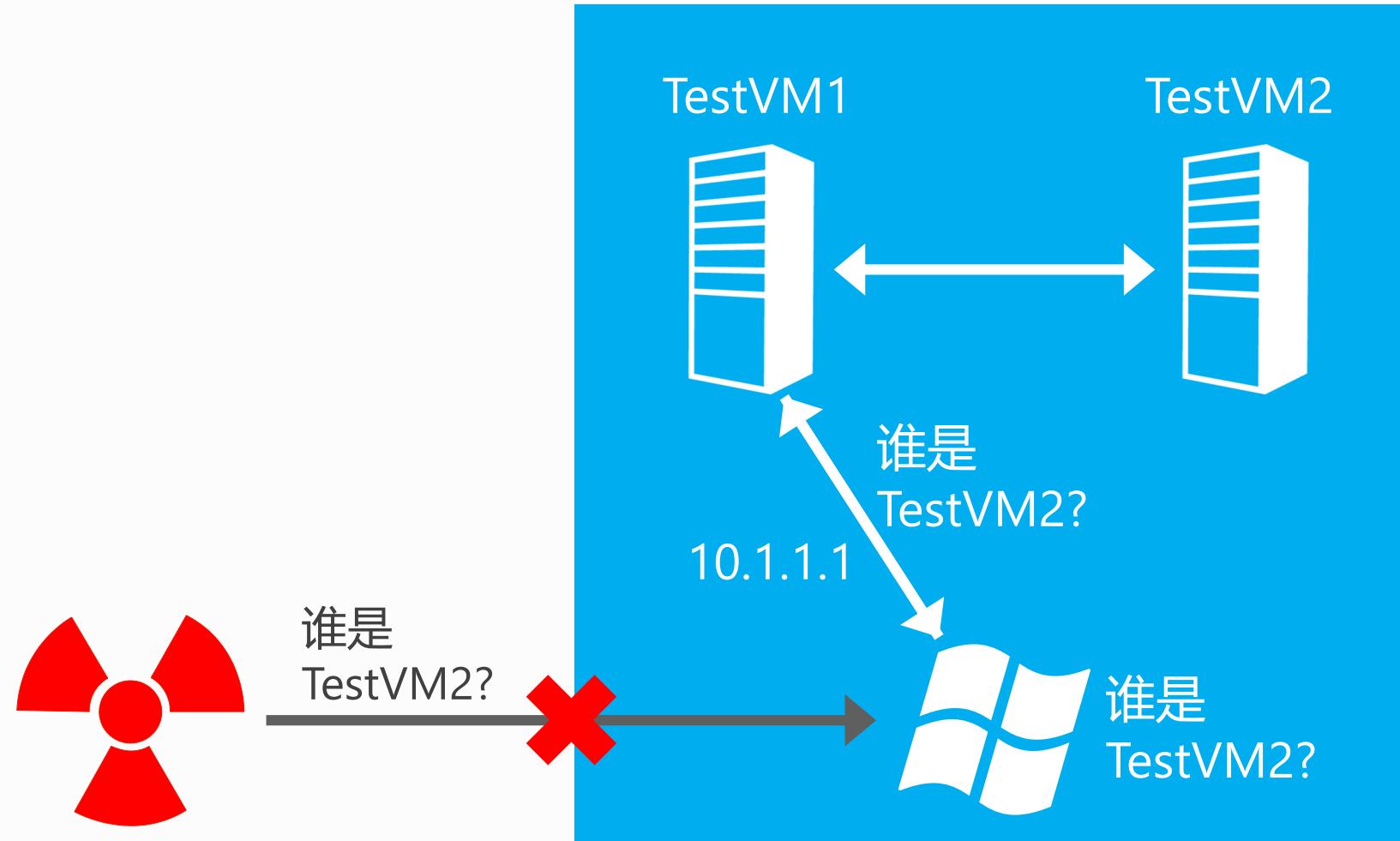
负载均衡器: 默认的状态探测



负载均衡器：自定义的状态探测



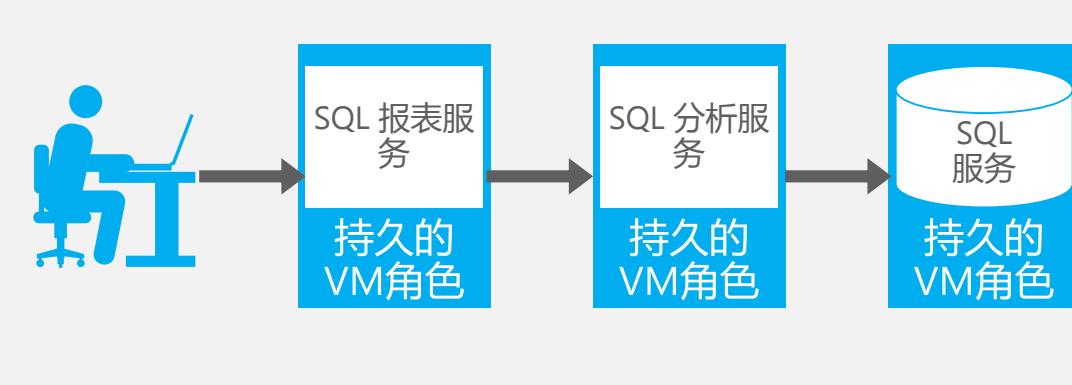
Windows Azure 提供的DNS



DNS 场景

Windows Azure DNS 场景

A. 使用持久VM的客户端-服务器应用程序

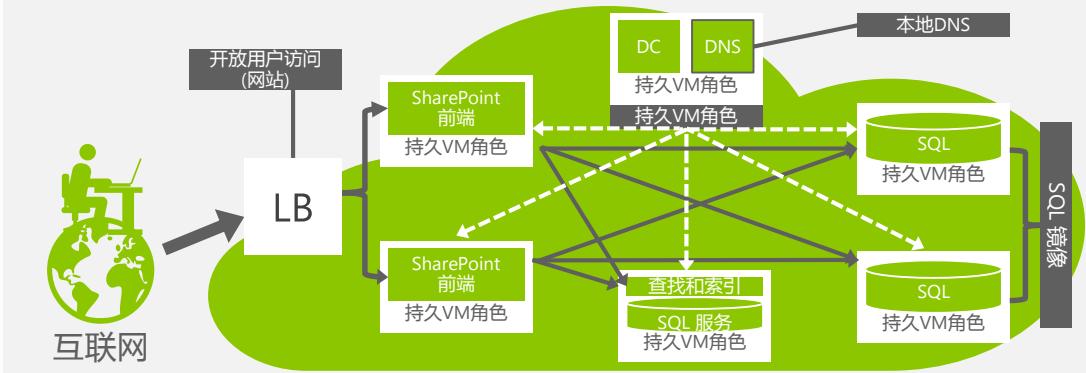


自定义DNS 场景

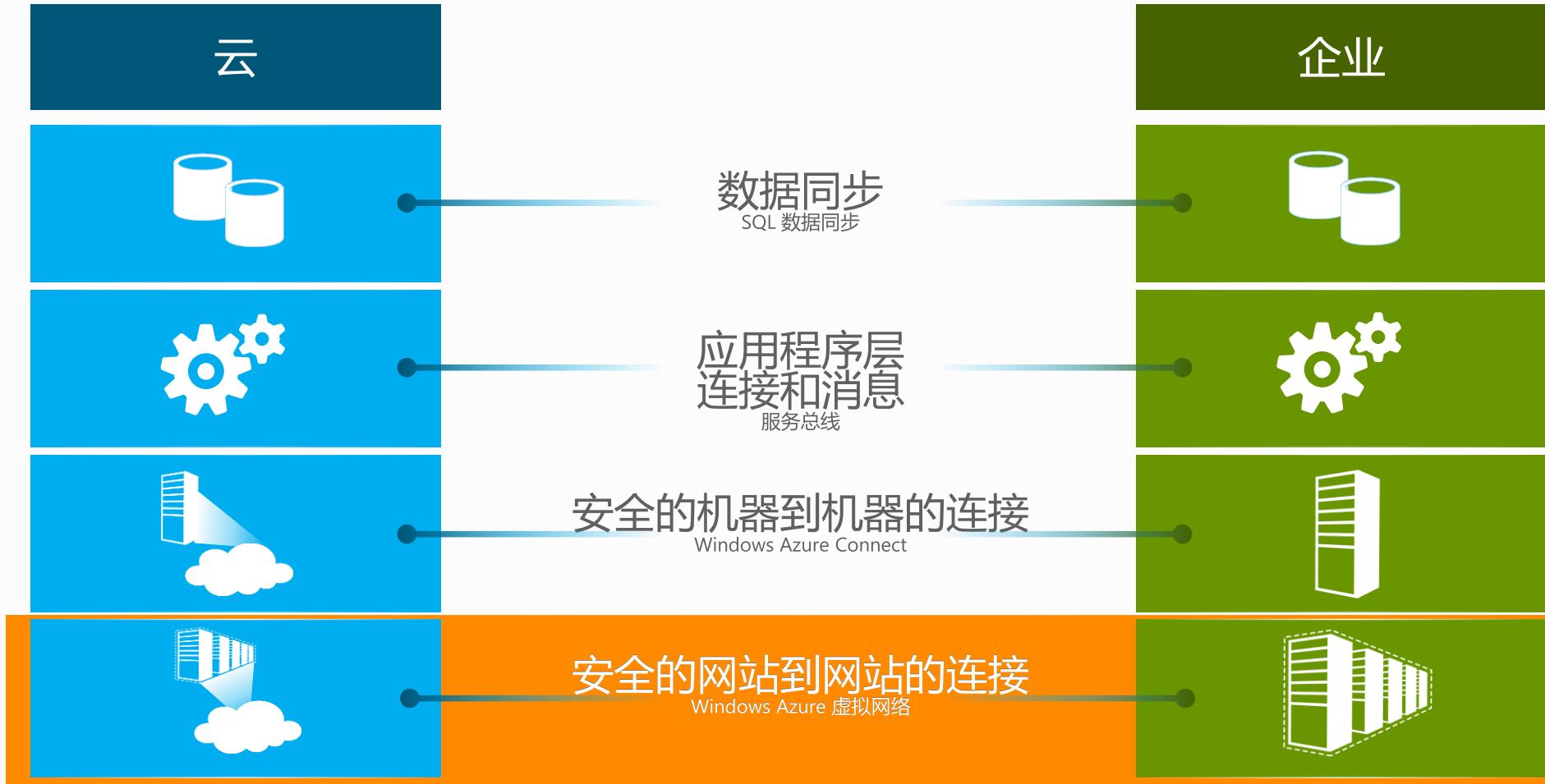
B. 内部的混合连接(内部的DNS)



C. 有自定义DNS的SharePoint (持久VM)



Windows Azure 连接选项



Windows Azure 虚拟网络

您在云中的虚拟“办公室”/数据中心

能够让客户将他们的公司网络扩展到Windows Azure中。

迁移现有的应用和服务到Windows Azure中

允许客户在云和内部环境中运行混合的应用程序

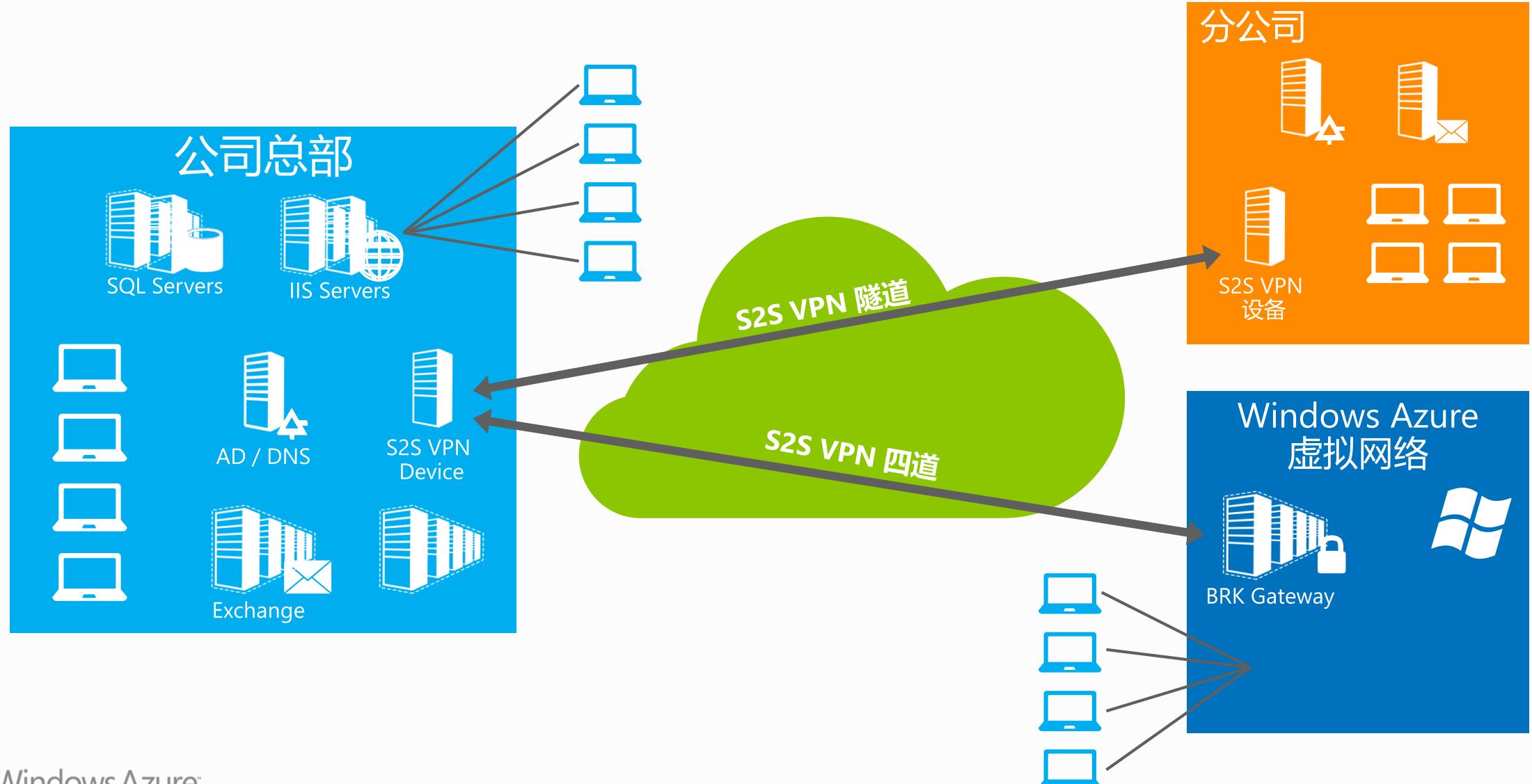
云中被保护的私有网络

允许客户在Windows Azure中设置私有的IPv4网络

IP地址保持

内部IP直接通讯

虚拟办公室



虚拟网络的特性

在Windows Azure中用户管理的私有网络

“带来您自己的IPv4地址”

在网络中直接控制Windows Azure的角色

稳定的IPv4地址

VPN网关允许站点到站点的连接

自动提供和管理

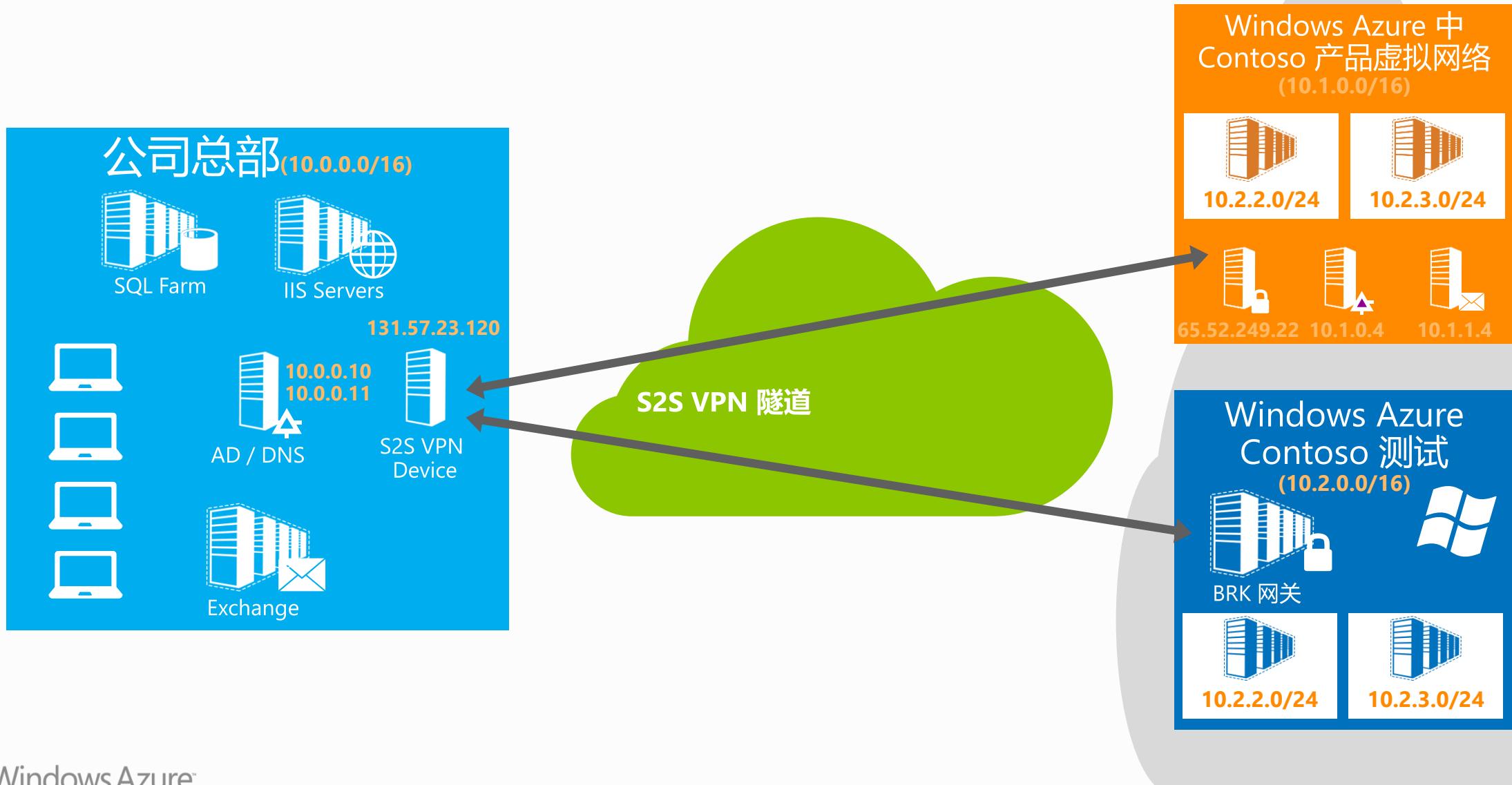
支持现有的VPN设备

使用内部的DNS服务器进行名成解析

允许客户使用自有的内部DNS服务器进行名称解析

允许Windows Azure上的VM加入公司域

举例: Contoso's 部署



场景



虚拟网络场景

混合的公有/私有云

Azure中的企业应用需要连接到内部的资源

企业的认证和访问控制

使用内部资源管理认证和访问控制(内部的活动目录)

监控和管理

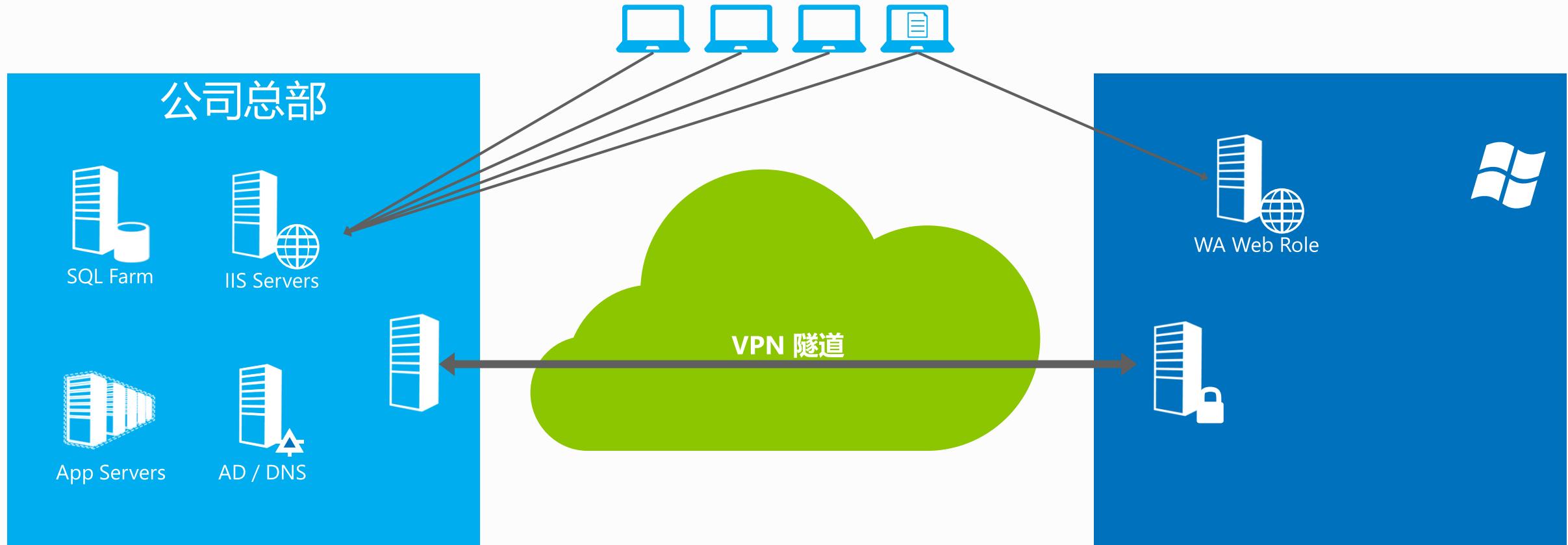
对Azure中运行的资源进行远程监控和解决问题

高级连接需求

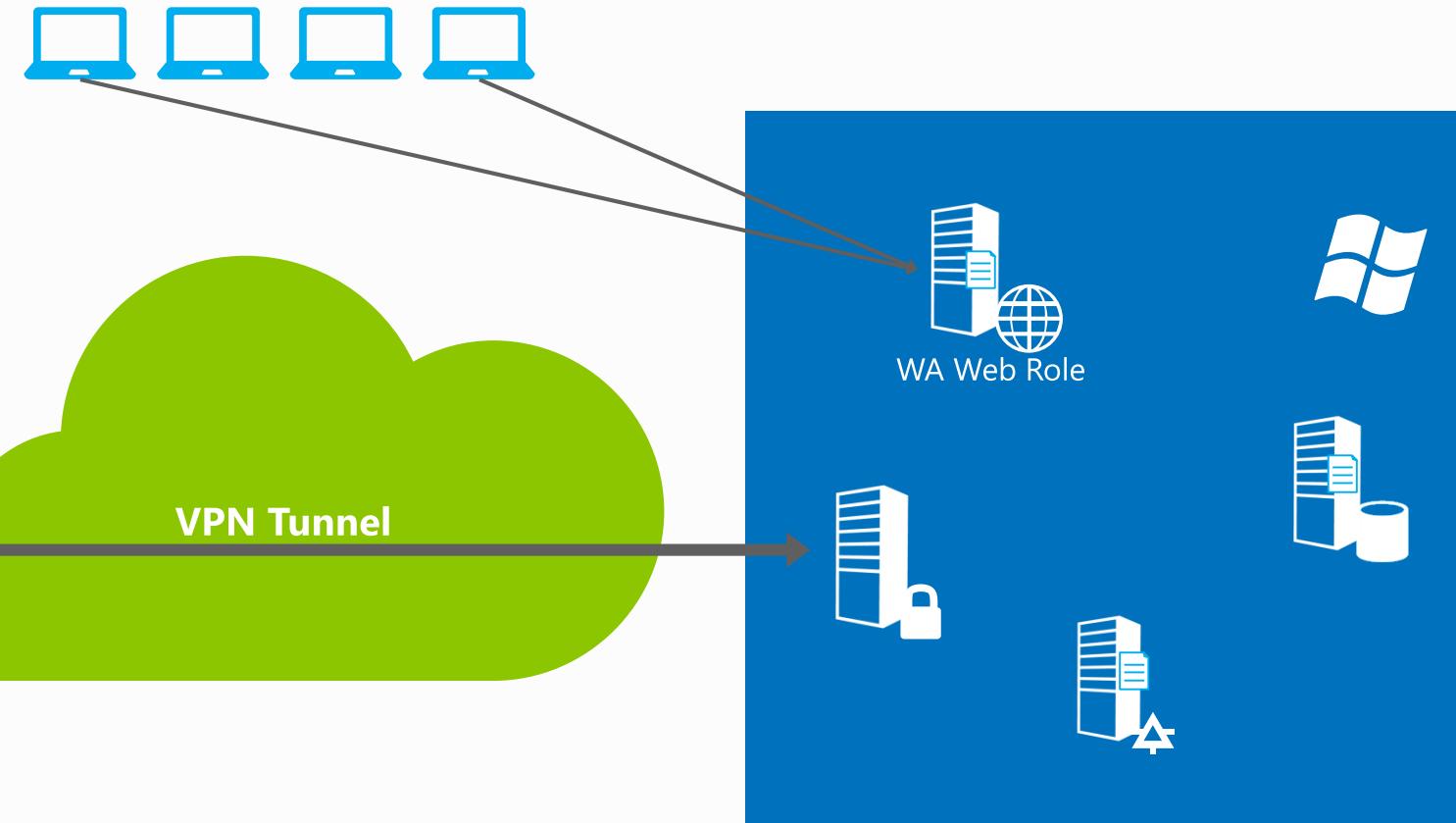
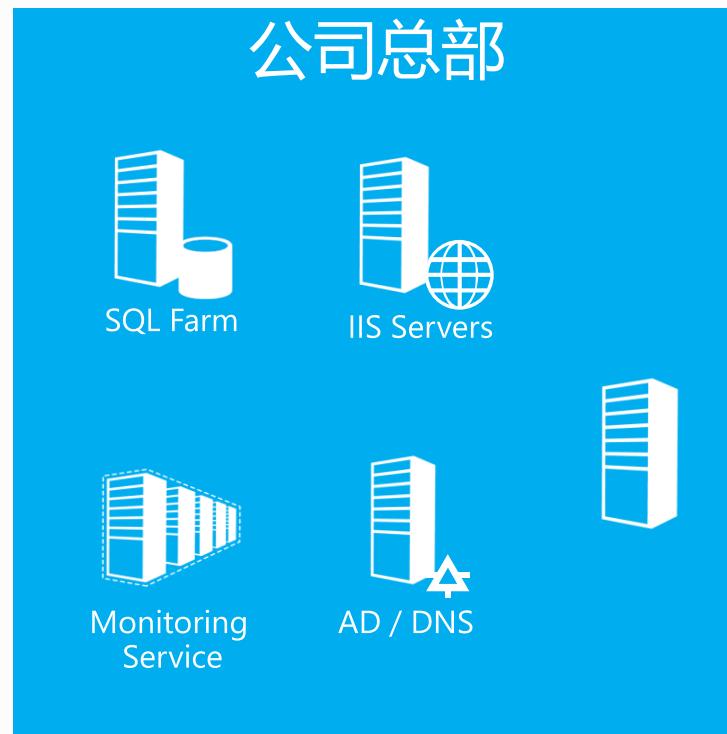
云的部署需要持续的IP地址和服务间的直接连接



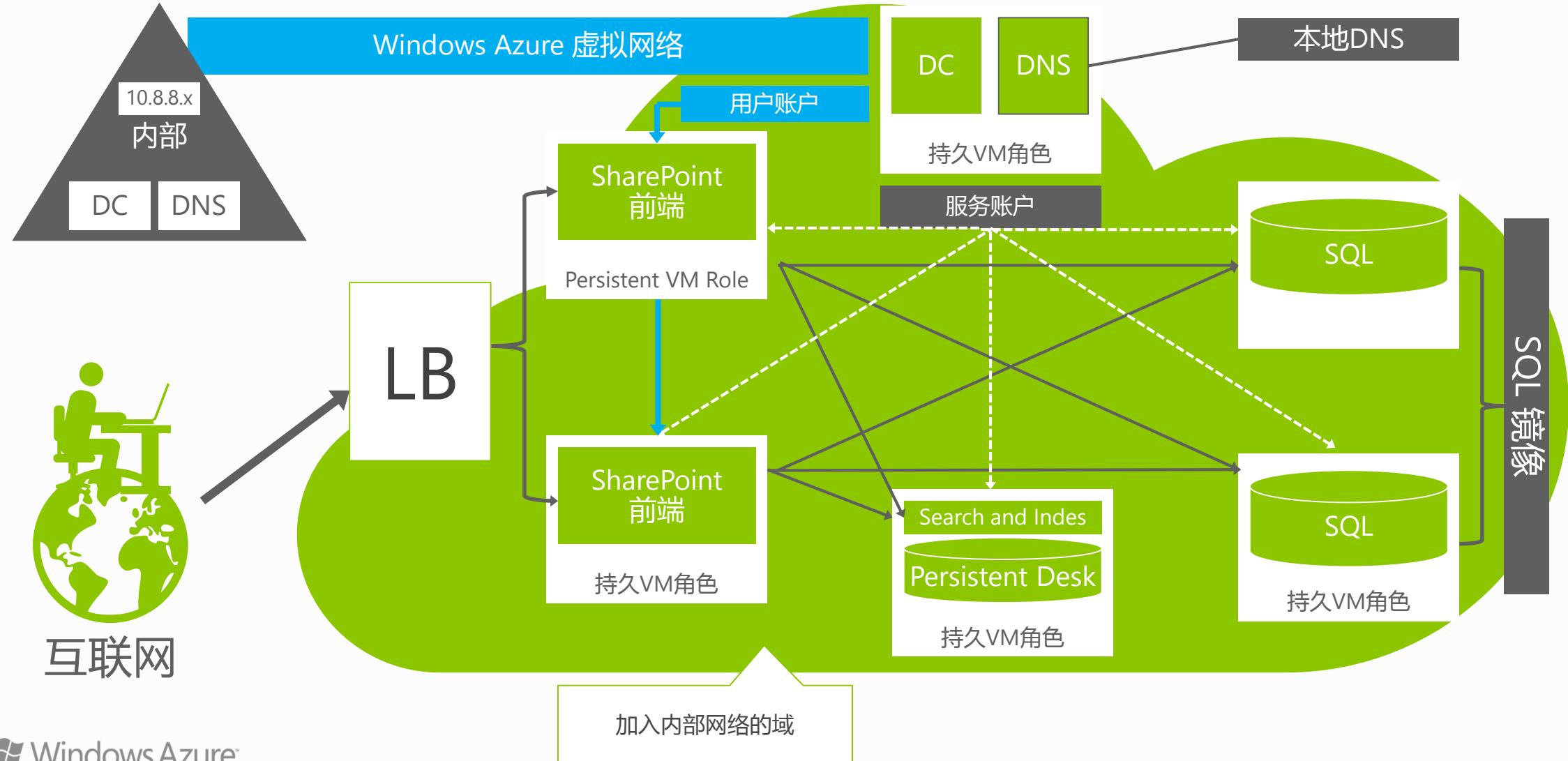
应用程序迁移



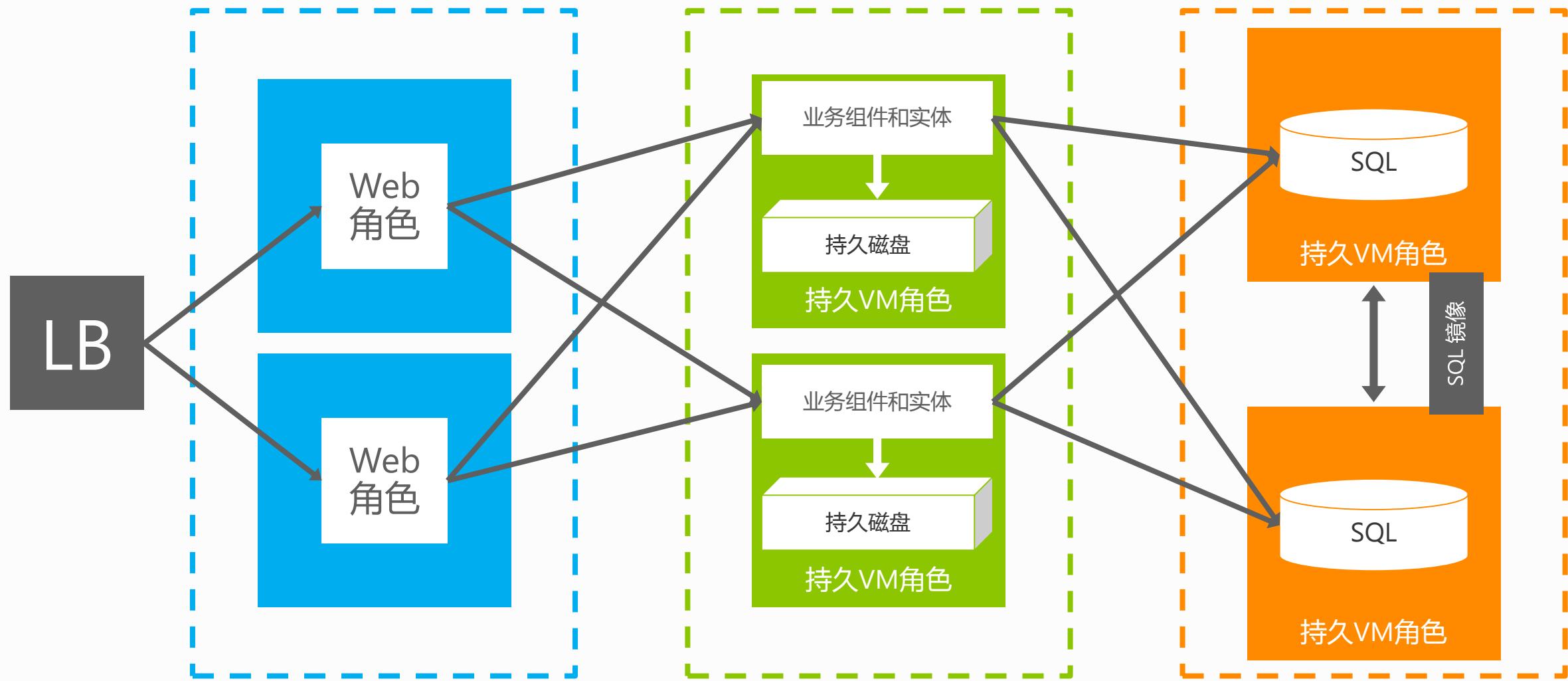
监控



Windows中的SharePoint

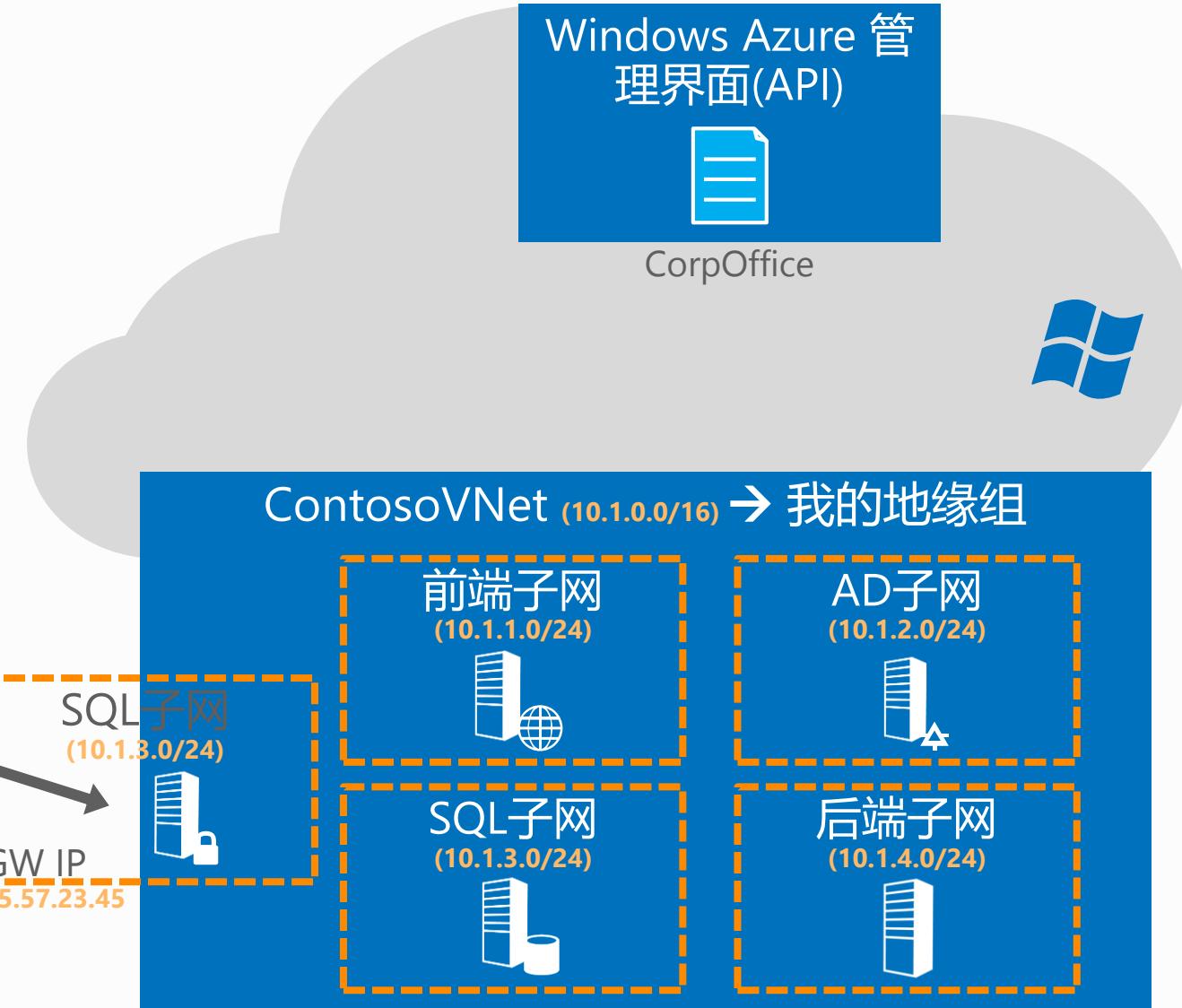
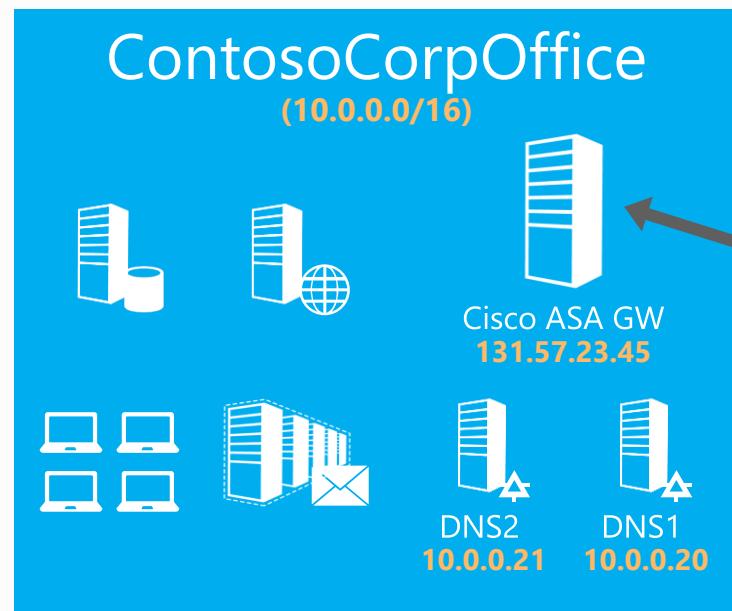


虚拟网络的混合模式



如何配置虚拟网络？

配置虚拟网络



管理界面体验, APIs 和服务模型

管理界面

向导来创建和更新虚拟网络

管理网关生命周期

APIs 和脚本

REST APIs

PowerShell Cmdlets

服务模型

网络配置

网络配置的操作

设置网络配置

获得网络配置

网关管理器上的操作

创建网关

删除网关

获得网关

获得网关共享密钥

重置网关密钥

列出连接

连接到本地网络站点

从本地网络站点断开

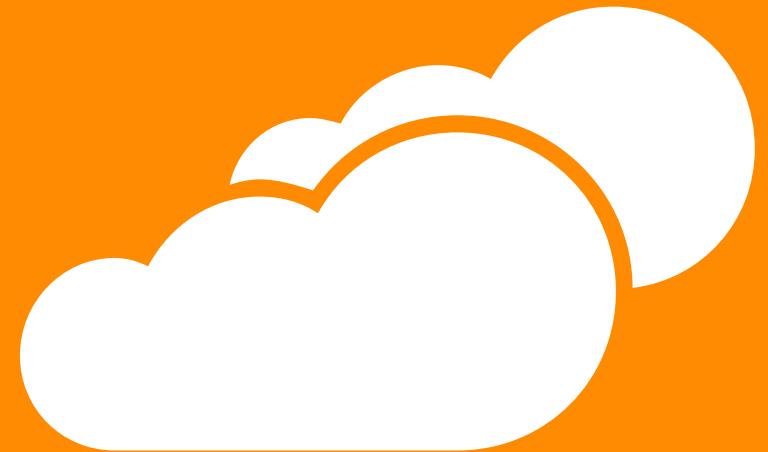
测试本地网络站点

获得操作状态

列出操作状态

设置虚拟网络

演示



虚拟网络V1功能集



支持的VPN 设备列表

Cisco

平台	OS 家族	举例
ASA 5500 Series (Adaptive Security Appliances)	ASA Software 8.4+	5505, 5550
ASR 1000 Series Aggregation Services Routers	IOS XE 2.1+	1002
ISR Series Integrated Services Routers	IOS 12.2+	2801, 2901, 2911

Juniper

平台	OS 家族	举例
SRX Series Routers	JunOS 10.2+	210, 650
J Series Routers	JunOS 9.4+	4350
ISG Series Routers	ScreenOS 6.2+	SX2
SSG Series Routers	ScreenOS 6.2+	550

一般的VPN设备必须支持

- IKE v1
- AES 128, 256
- SHA1, SHA2

网关冗余和可用性的备注

每个虚拟网络只支持一个IPSec隧道

Azure这边的网关有2个实例 (active-passive mode)

隧道只能通过一个公共IP

一对VPN设备能通过使用工业标准协议而成为互相冗余的。

HSRP(热备份路由器协议)

VRRP(虚拟路由器冗余协议)

限制 (V1发布)

订阅限制

一个订阅最多5个虚拟网络，每个订阅最多5个sites

一个地缘组一个VNET

一个订阅最多9个DNS服务器

虚拟网络站点

只能使用RFC1918中定义的地址

只能连到一个站点

子网没有限制

本地网络站点

允许共有/私有的IP

每个站点只有一个网关IP

网关

一个网关一个虚拟网络(通过Windows Azure管理)
站点和虚拟网络之间只有一个活跃的隧道

没有地址空间重叠

V1的限制

虚拟网络

- 只允许IPv4地址
- 不支持 MCAST / BRCAST
- 不支持BYO MAC 地址
- 不支持为虚拟机分配静态IP
- 不支持活跃路由 (BGP)
- 不支持强制隧道
- 对虚拟网络地址空间没有动态更新

跨网络连接性

- 不支持IKE v2
- 不支持基于证书的认证
- 不支持2-factor 认证
- 不支持基于软件的VPN解决方案

区别

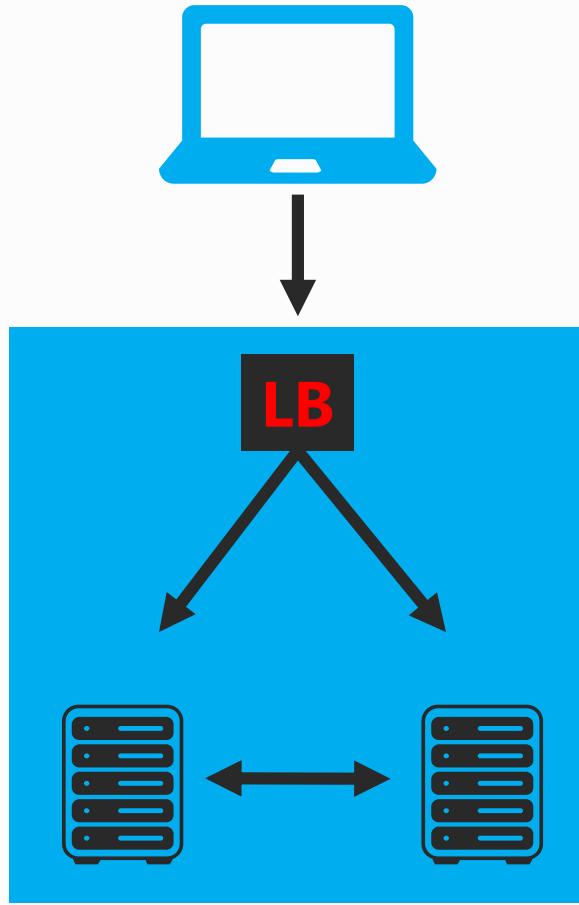
客户内部的网络

客户对L2及以上拥有完全的控制
MAC 地址说明和VLANs 支持
支持静态和 DHCP 地址
支持MCAST, BROADCAST
路由必须显式定义
信任边界 = VLAN 边界
支持几种不同的VPN 连接 (SSL, Ipsec, ...)
WAN 优化器可以被用于优化跨网的连接

Azure中的虚拟网络

客户只能定义一些L3的属性
不支持MAC and VLANs
只支持Azure管理的DHCP 地址
不支持MCAST , BROADCAST
路由是隐式的
信任边界= 虚拟网络边界
只支持IKEv1的Ipsec
不支持WAN 优化器

总结



输入端点

支持的协议: HTTP, HTTPS, TCP, UDP
虚拟机的负载平衡
自定义的负载平衡探测

内部端点

实例到实例的通讯
支持的协议: TCP, UDP, 任何基于IP的协议

Name Resolution

Windows Azure DNS提供服务级的域名解析
提供API进行实例的确认
Azure提供服务级名称解析
Azure提供虚拟机级名称解析
使用自己的DNS服务器进行名称解析

Windows Azure 流量管理

Windows Azure 虚拟网络混合场景



Windows Azure™



© 2012 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.
Translated to Chinese Simplified Version by Shanghai Yungoal Info Tech Co., Ltd. [YunGoal](#)