



Microsoft Online Tech Forum

微软在线技术峰会

如何实现云计算网络的纵深防御体系

王文斌

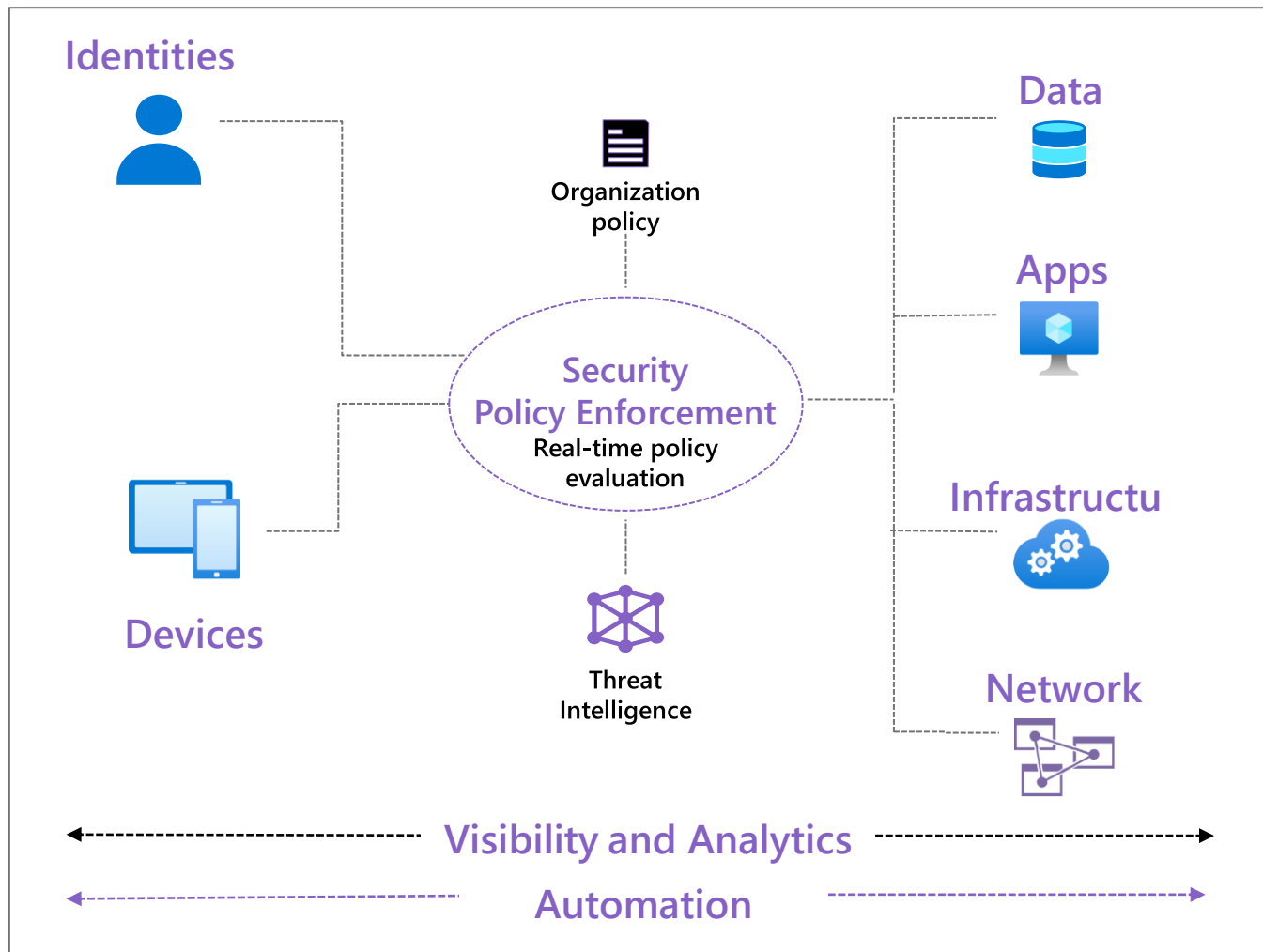
Agenda

- Azure 网络安全概览
- Azure DDoS 防护
- Azure 网络安全组
- Azure 用户定义路由
- Azure 防火墙
- Azure 应用程序防火墙
- Azure 网络虚拟设备
- 案例：混合网络部署



Azure 网络安全概览

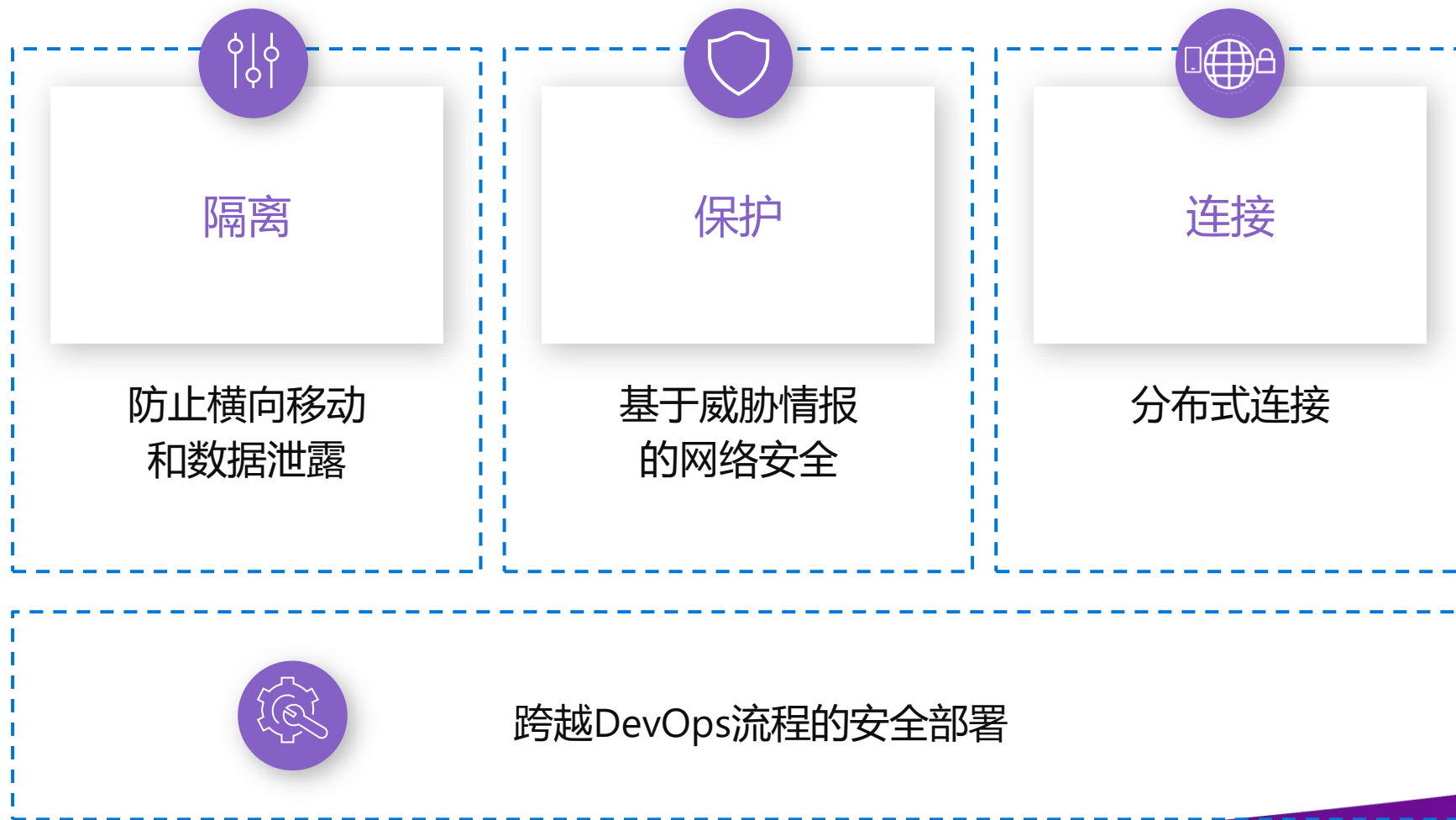
零信任模型



零信任的指导原则:

1. 明确验证
2. 最低权限访问
3. 假设违反

Azure 网络安全



利用Azure产品实现零信任网络

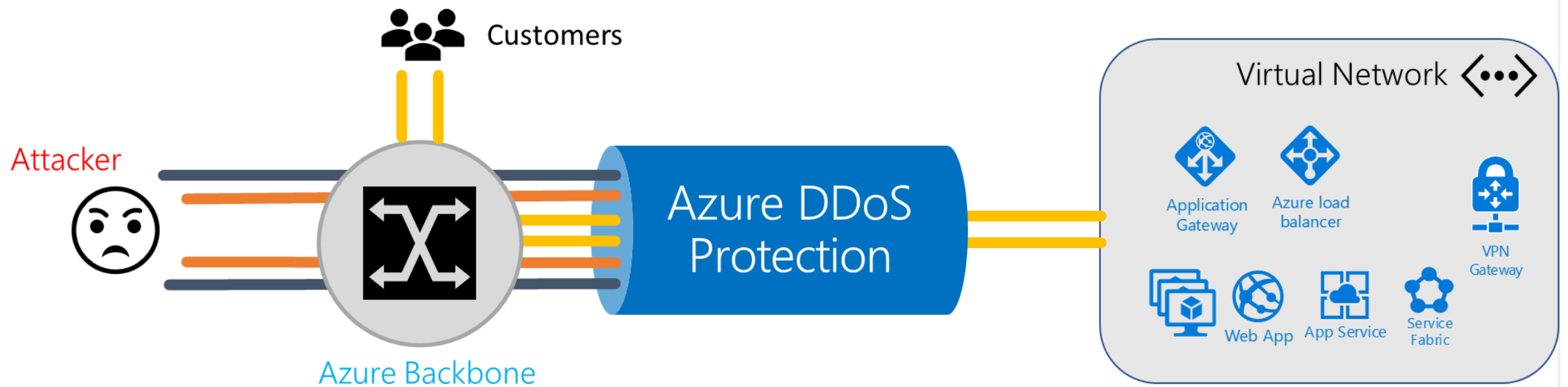




Azure DDoS防护

保护应用程序免遭分布式拒绝服务 (DDoS) 攻击。

Azure DDoS防护



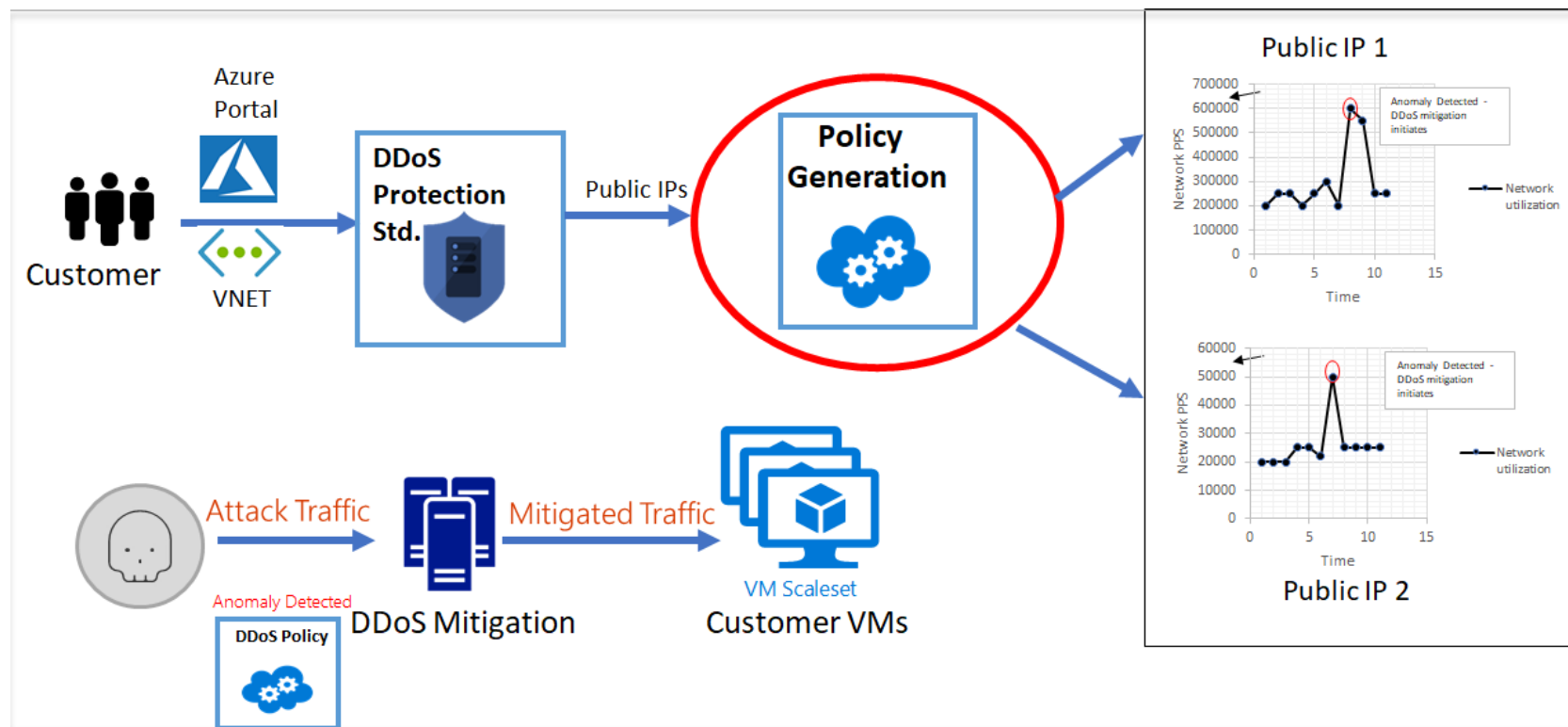
Azure DDoS防护

基本DDoS防护



Azure DDoS防护

标准DDoS防护





网络安全组

筛选进出 Azure 虚拟网络中的 Azure 资源的网络流量。

网络安全组

Home > Network security groups > bob-arm-nsg

 **bob-arm-nsg**
Network security group

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets
- Properties
- Locks
- Export template
- Monitoring
- Diagnostic settings

Move Delete Refresh


Essentials

Inbound security rules

Priority	Name	Port	Prot
110	any4	Any	Any
120	appgw	65200-65535	Any
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Outbound security rules

Priority	Name	Port	Prot
100	any	Any	Any
65000	AllowVnetOutBound	Any	Any
65001	AllowInternetOutBound	Any	Any
65500	DenyAllOutBound	Any	Any

 **any4**
bob-arm-nsg

Save Discard Basic Delete

Source * ⓘ
Any

Source port ranges * ⓘ
*

Destination * ⓘ
Any

Destination port ranges * ⓘ
*

Protocol *
Any TCP UDP ICMP

Action *
Allow Deny

Priority * ⓘ
110

Name
any4

Description

网络安全组

- **服务标记**

服务标记表示给定 Azure 服务中的一组 IP 地址前缀。它有助于最大程度地减少对网络安全规则的频繁更新的复杂性。

- **应用程序安全组**

使用应用程序安全组可将网络安全配置为应用程序结构的固有扩展，从而可以基于这些组将虚拟机分组以及定义网络安全策略。可以大量重复使用安全策略，而无需手动维护显式 IP 地址。

用户定义路由

确保特定设备或设备组中的所有流量通过特定位置进入或离开虚拟网络。

用户定义路由

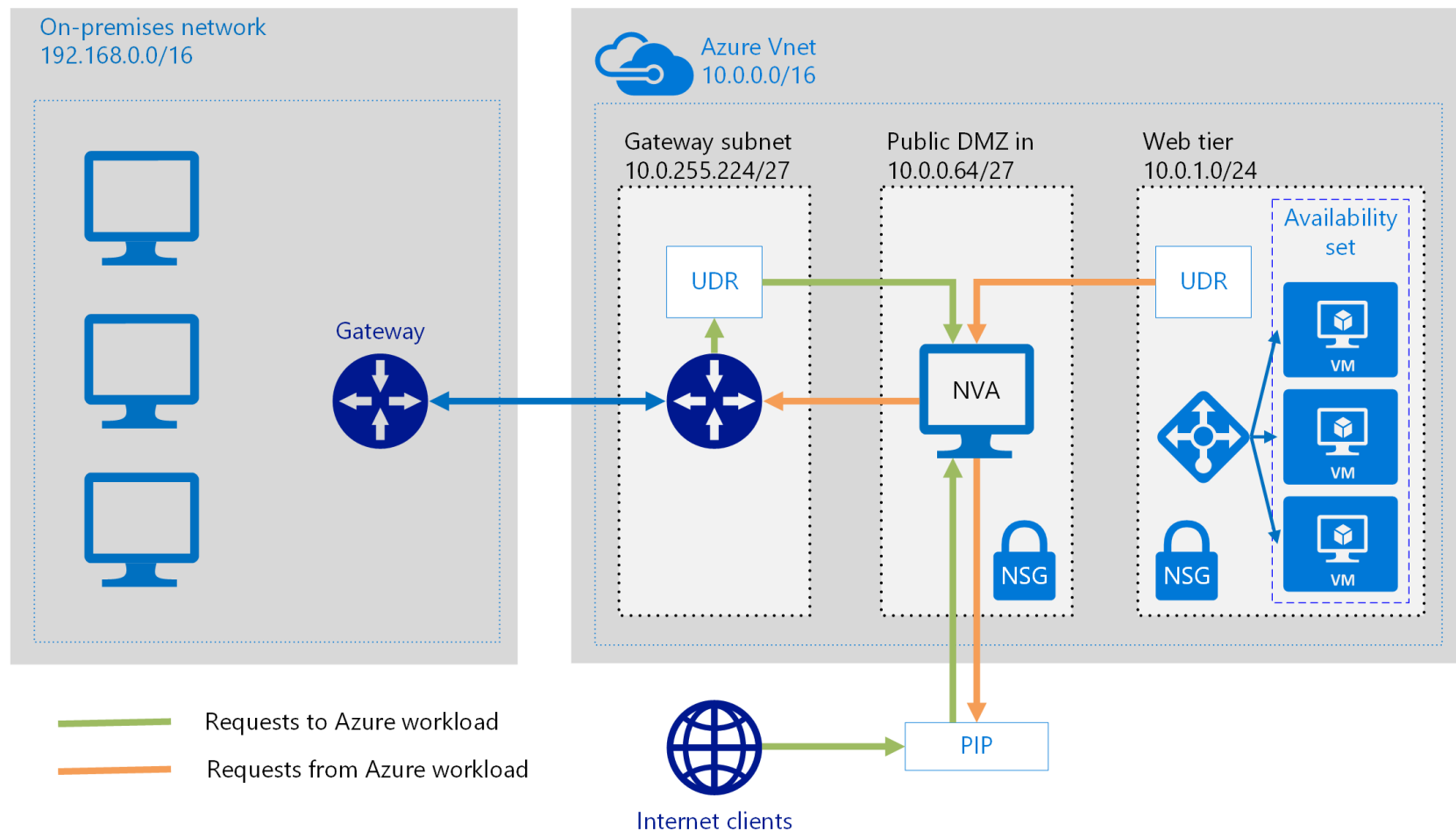
系统路由



Source	地址前缀	下一跃点类型
默认	对虚拟网络唯一	虚拟网络
默认	0.0.0.0/0	Internet
默认	10.0.0.0/8	无
默认	192.168.0.0/16	无
默认	100.64.0.0/10	无

用户定义路由

自定义路由



用户定义路由

- Azure 如何选择路由

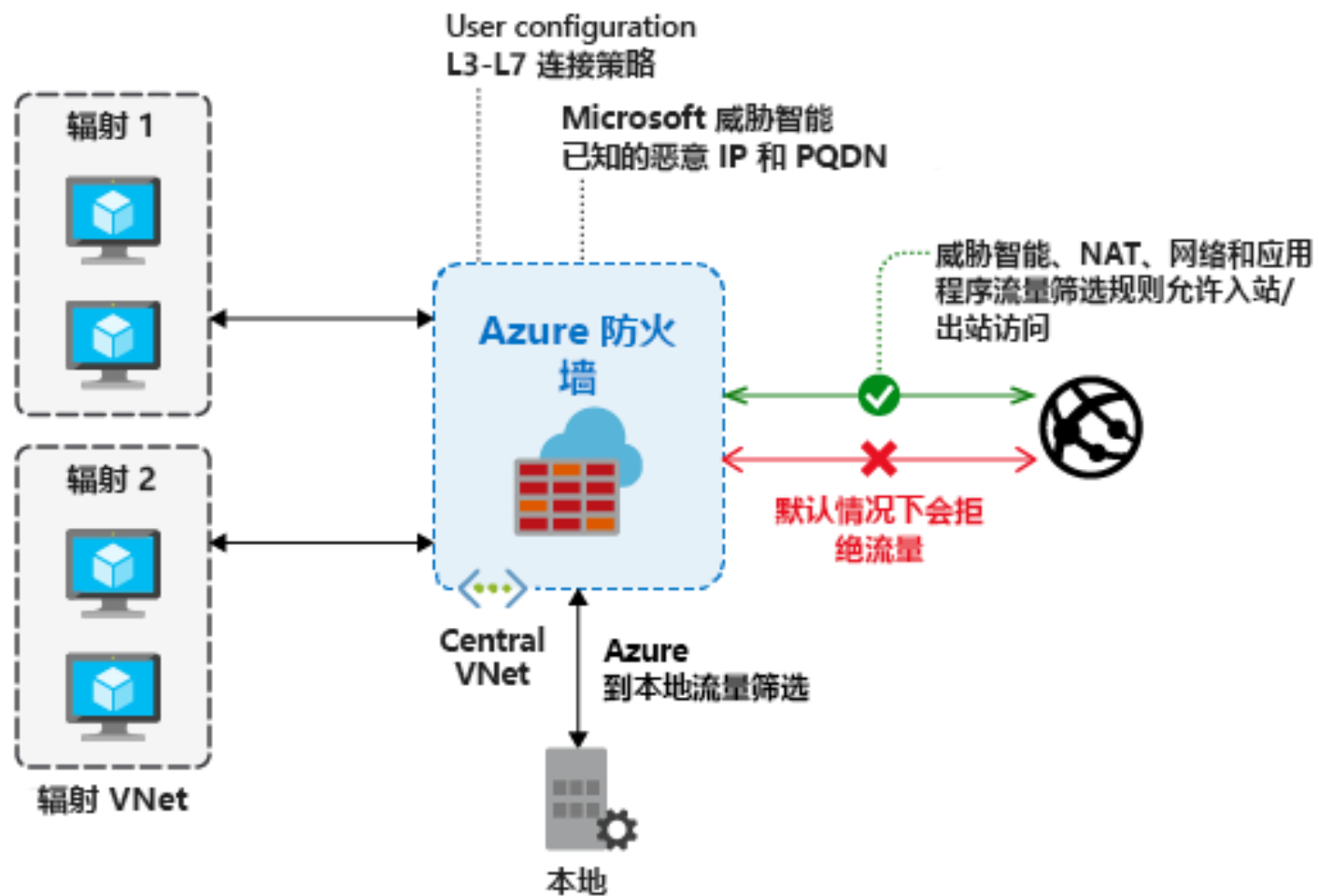
- Azure 使用最长前缀匹配算法，根据目标 IP 地址选择路由
- 如果多个路由包含同一地址前缀，Azure 根据以下优先级选择路由类型：
 1. 用户定义的路由
 2. BGP 路由
 3. 系统路由



Azure 防火墙

原生防火墙功能，内置有高可用性、提供无限的云可伸缩性且无需维护。

Azure 防火墙



Azure 防火墙

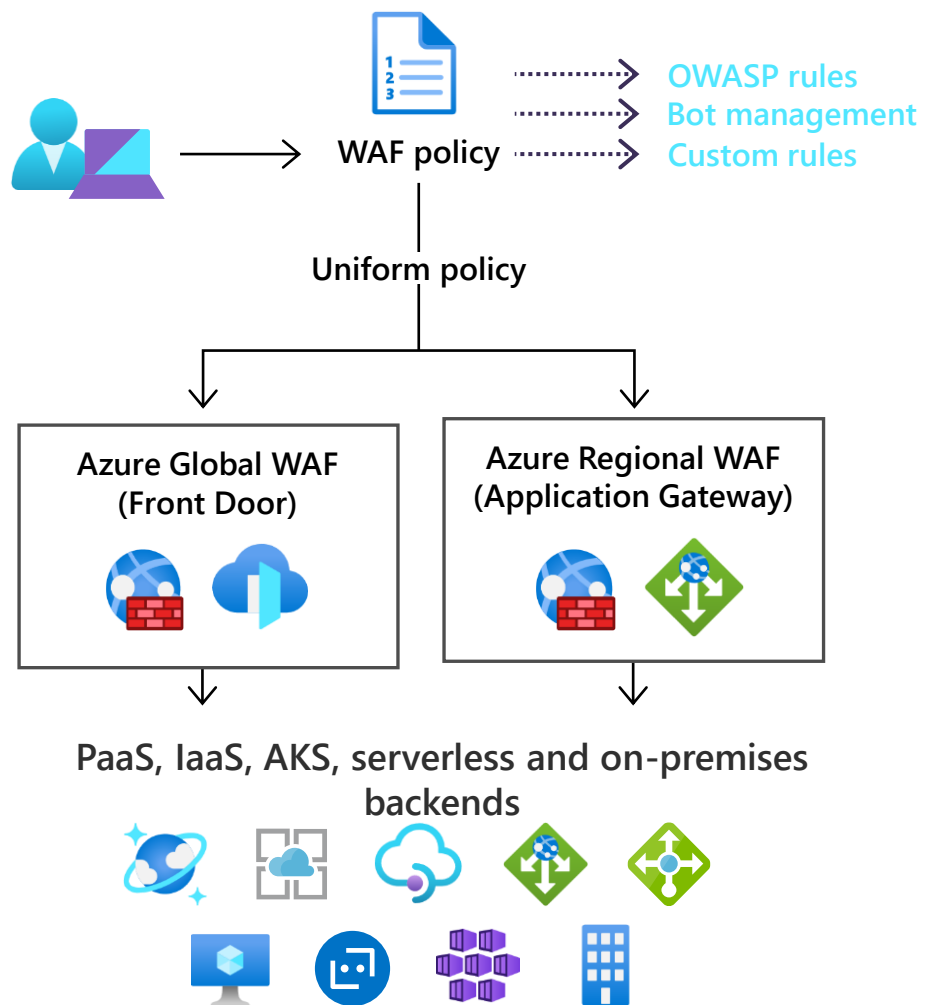
- 不受限制的云可伸缩性
- 应用程序 FQDN 筛选规则
- 网络流量筛选规则
- FQDN 标记
- 服务标记
- 威胁情报
- 出站 SNAT 支持
- 入站 DNAT 支持



Azure 应用程序防火墙

为 Web 应用提供强大保护的云原生 Web 应用程序防火墙 (WAF) 服务。

Azure应用程序防火墙



- 微软智能安全
 - 保护应用免受自动化攻击
 - 使用机器人防护规则集删选正常/恶意机器人
- 基于站点或URI路径指定WAF策略
 - 基于不同主机/侦听器或者URI路径部署自定义WAF策略，以实现更精细化的保护
- 基于地理位置的流量过滤
 - 增强自定义策略的批评场景
- 通过以下服务进行部署：
 - Azure 应用层网关
 - Azure Front Door
 - Azure CDN（预览版）

Azure应用程序防火墙

- WAF 策略和规则

- 自定义规则

- IP 允许列表和阻止列表
 - 基于地理位置的访问控制
 - 基于 HTTP 参数的访问控制
 - 基于请求方法的访问控制
 - 大小约束
 - 速率限制规则

- Azure 托管的规则集

- 基于开放 Web 应用程序安全项目 (OWASP) 中的核心规则集 (CRS) 3.1、3.0 或 2.2.9。
 - 机器人防护规则集 (预览版)

- WAF 工作模式

- 检测模式
 - 阻止模式



Azure 网络虚拟设备

在云上使用你熟悉的网络设备。

Azure 网络虚拟设备

选择您信赖的品牌



Azure 网络虚拟设备

Azure 防火墙与Azure NVA对比



Feature	Azure Firewall	NVAs
FQDN filtering (no SSL termination)	✓	✓
Inbound/Outbound traffic filtering rules by IP address (source and destination), port, and protocol (5-tuple rules)	✓	✓
Network Address Translation (SNAT+DNAT)	✓	✓
Traffic filtering based on threat intelligence feed to identify high risk sources/destinations (e.g., C&C, botnet, etc.)	✓	✓
Full logging including SIEM integration	✓	✓
Built-in HA with unrestricted cloud scalability (auto scale as traffic grows)	✓	VMSS (vendor dependent)
Azure Service Tags and FQDN Tags for easy policy management	✓	
Integrated monitoring and management, zero maintenance—cloud service model	✓	
Easy DevOps integration using Azure REST/PS/CLI/Templates	✓	Templates
SSL termination with Deep Packet Inspection (IDPS) to identify known threats (e.g., viruses, spyware)	Roadmap	✓
Traffic filtering rules by target URI (full path - incl. SSL termination)	Roadmap	✓
Central management	Using partners (in preview)	✓
Application and user aware traffic filtering rules	Roadmap	✓
IPSEC and SSL VPN gateway	Azure VPN GW	✓
Advanced Next Generation Firewall features (e.g. Sandboxing)		Vendor Dependent

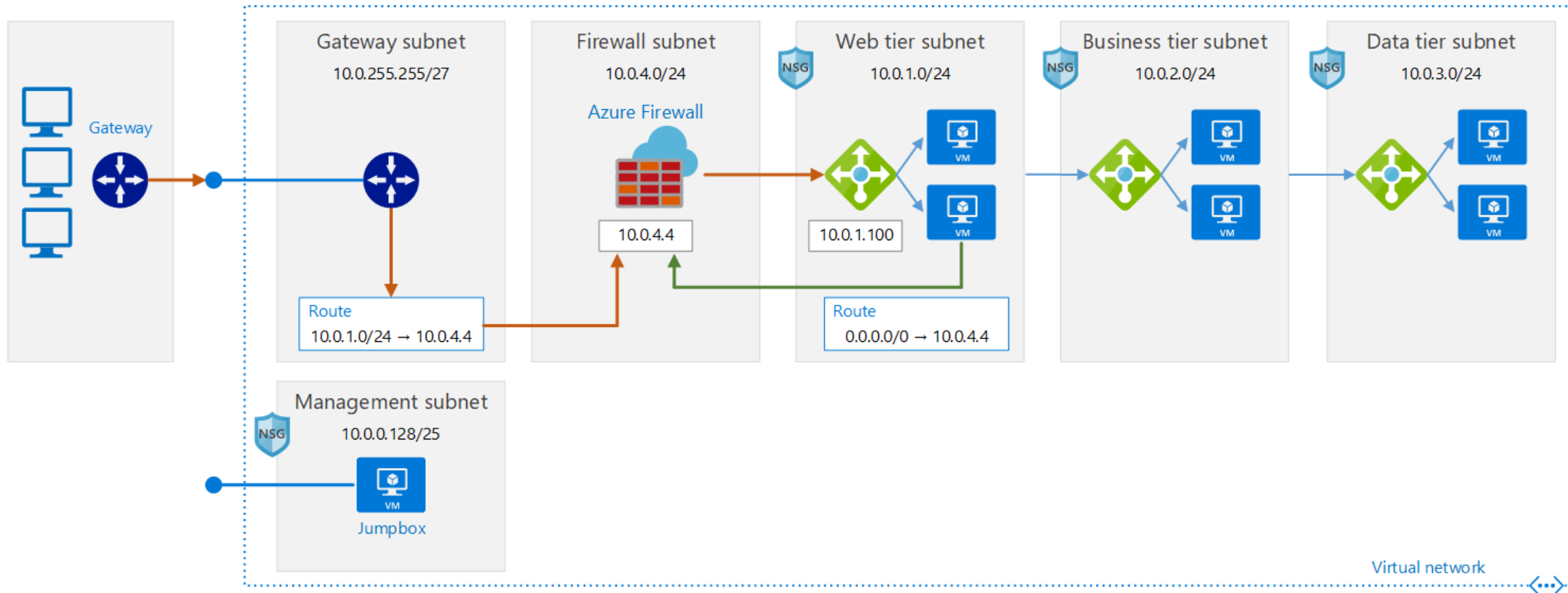


案例：混合网络部署

案例：混合网络部署

On-premises network

Azure virtual network





扫码下载讲师PPT
更多精彩尽在【微软市场活动】