AWS Summit

AWS 技术峰会 · 北京 2014

基于AWS云服务的企业混合IT架构和网络实现

Jenny Sun 孙素梅 AWS解决方案架构师

December 12, 2014

日程

- 什么是混合IT架构
- AWS支持混合IT架构
- 基于AWS的混合IT架构的网络实现

日程

- 什么是混合IT架构
- AWS支持混合IT架构
- 基于AWS的混合IT架构的网络实现

混合IT架构的定义

> “Hybrid IT is the result of combining internal and external services, usually from a combination of internal and public clouds, in support of a business outcome.”
>
> Gartner

http://www.gartner.com/technology/research/technical-professionals/hybrid-cloud.jsp

amazon web services

混合IT架构的定义

Services

Build

Solutions

SAP

Microsoft

JASPERSOFT
THE INTELLIGENCE INSIDE

ORACLE

informatica

Deliver

Business Outcomes

混合IT架构是未来的趋势

“Nearly half of large enterprises will have hybrid cloud deployments by the end of 2017.”

http://www.gartner.com/newsroom/id/2599315 - October 1, 2013

企业需要混合IT架构

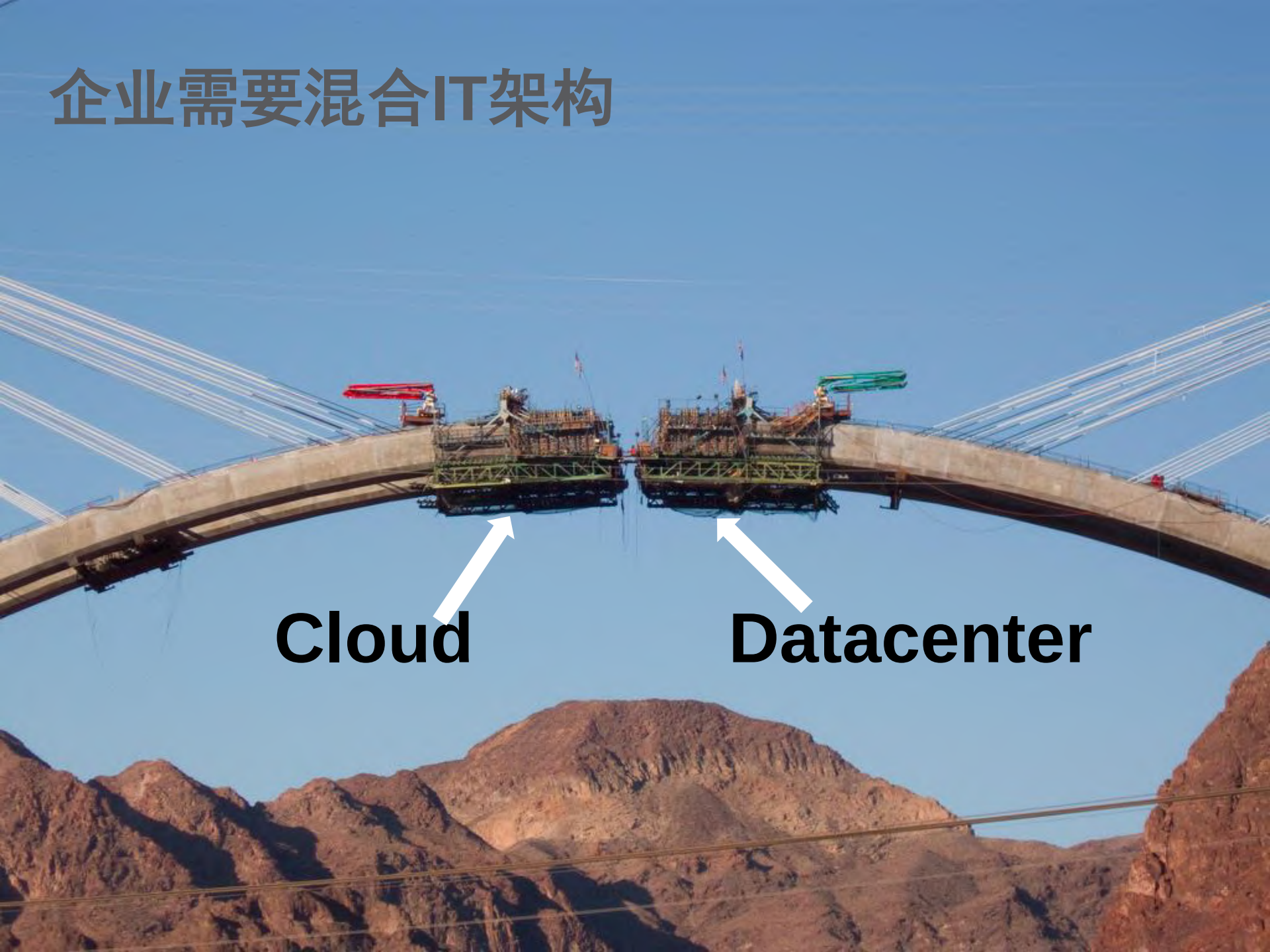
Power Constraints

Space Constraints

处理能力有限

很多新想法和新项目想要尝试

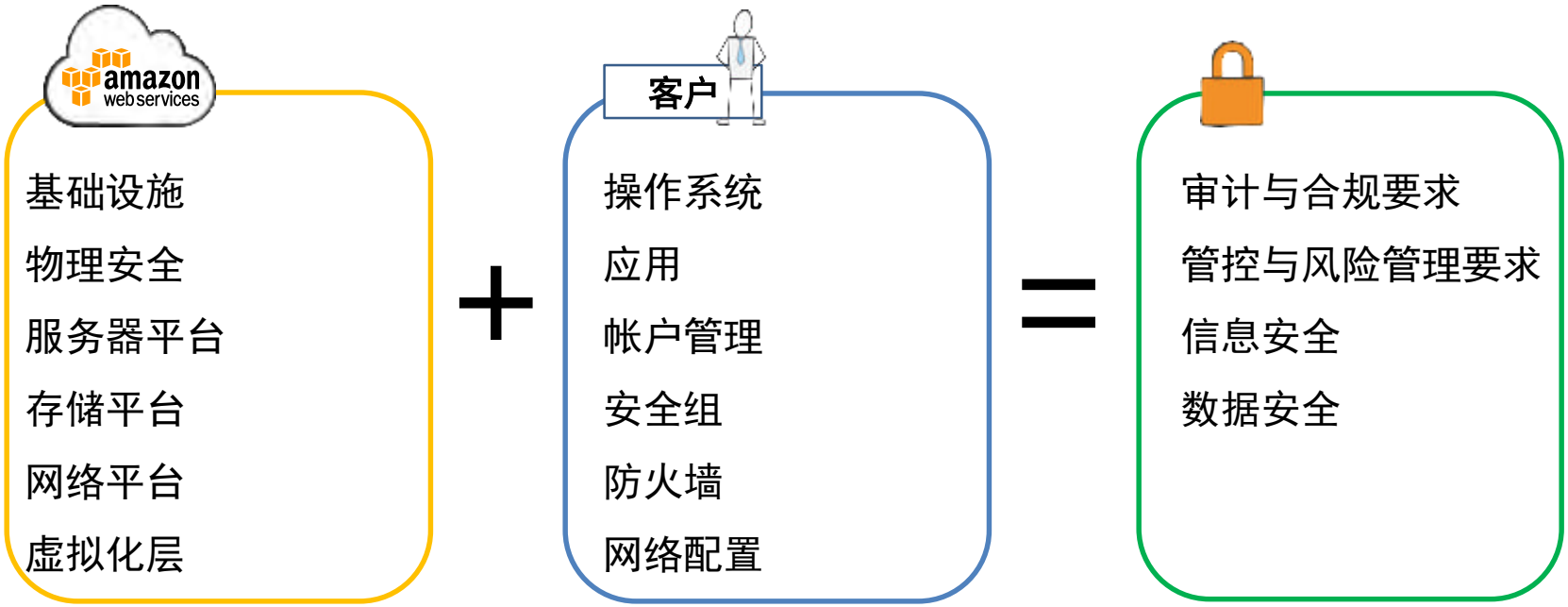
企业需要混合IT架构



日程

- 什么是混合IT架构
- AWS支持混合IT架构
- 基于AWS的混合IT架构的网络实现

AWS安全职责共担模型



AWS安全认证

http://aws.amazon.com/compliance/

- ✓ ISO 27001
- ✓ ISO 9001
- ✓ SOC 1/SSAE 16/ISAE 3402
- ✓ SOC 2
- ✓ SOC 3
- ✓ HIPAA
- ✓ PCI DSS Level 1
- ✓ MPAA
- ✓ CSA
- ✓ MTCS Tier 3 Certification
- ✓ FedRAMP(SM)
- ✓ DIACAP & FISMA
- ✓ ITAR
- ✓ DoD CSM Levels 1-2 and 3-5
- ✓ FIPS 140-2

AWS提供给用户的安全技术与工具

- ✓ VPC虚拟私有云/私有网络/VPN
- ✓ 安全组防火墙
- ✓ 数据加密/Cloud HSM
- ✓ IAM身份认证和访问管理
- ✓ 安全日志AWS Cloud Trail
- ✓ AWS Trusted Advisor
- ✓ ……

AWS支持混合IT架构

你的数据中心

自有环境上的应用

私有连接

工作负载与数据迁移

+

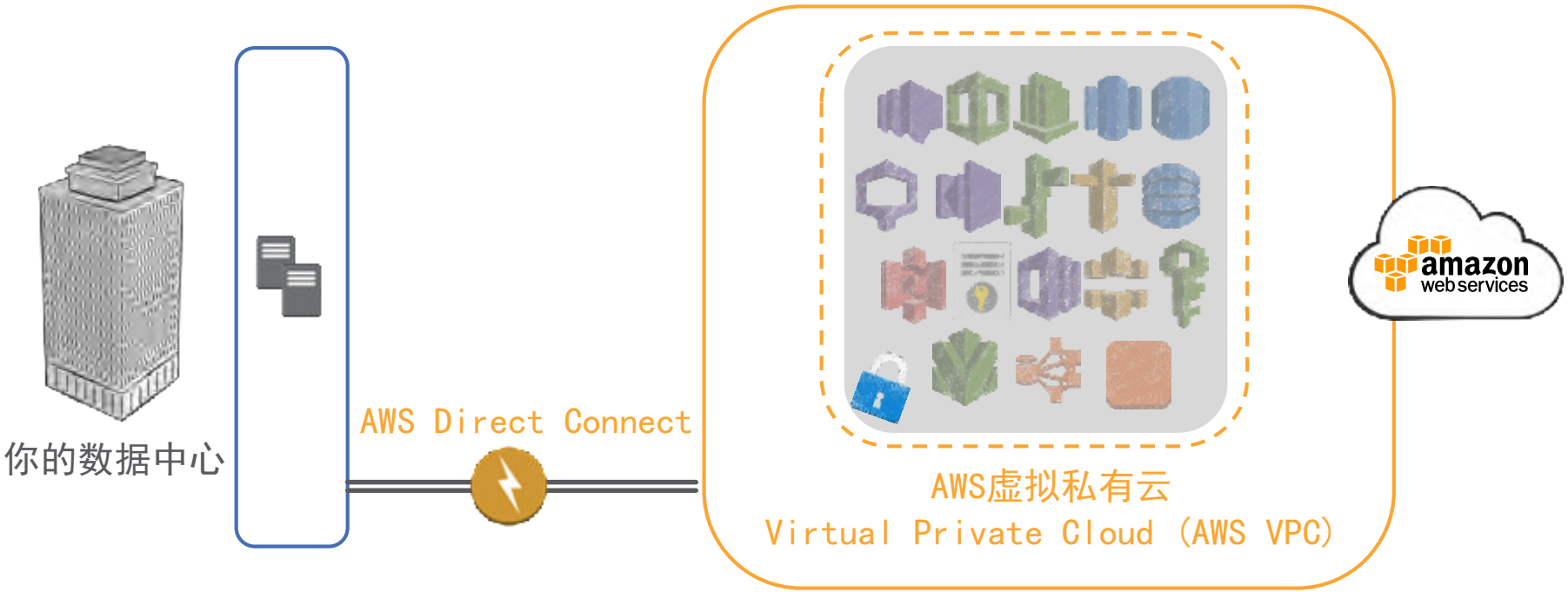
访问控制集成

与现有的管理工具一起使用

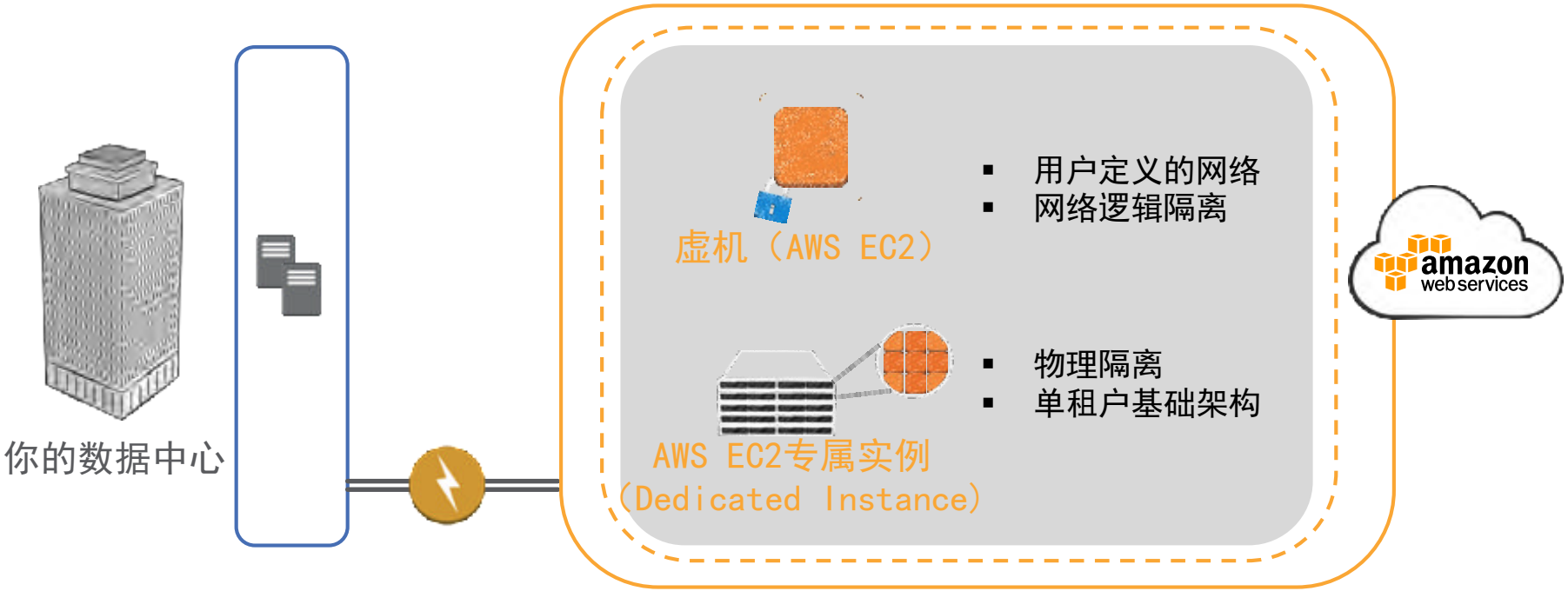
云应用

amazon web services

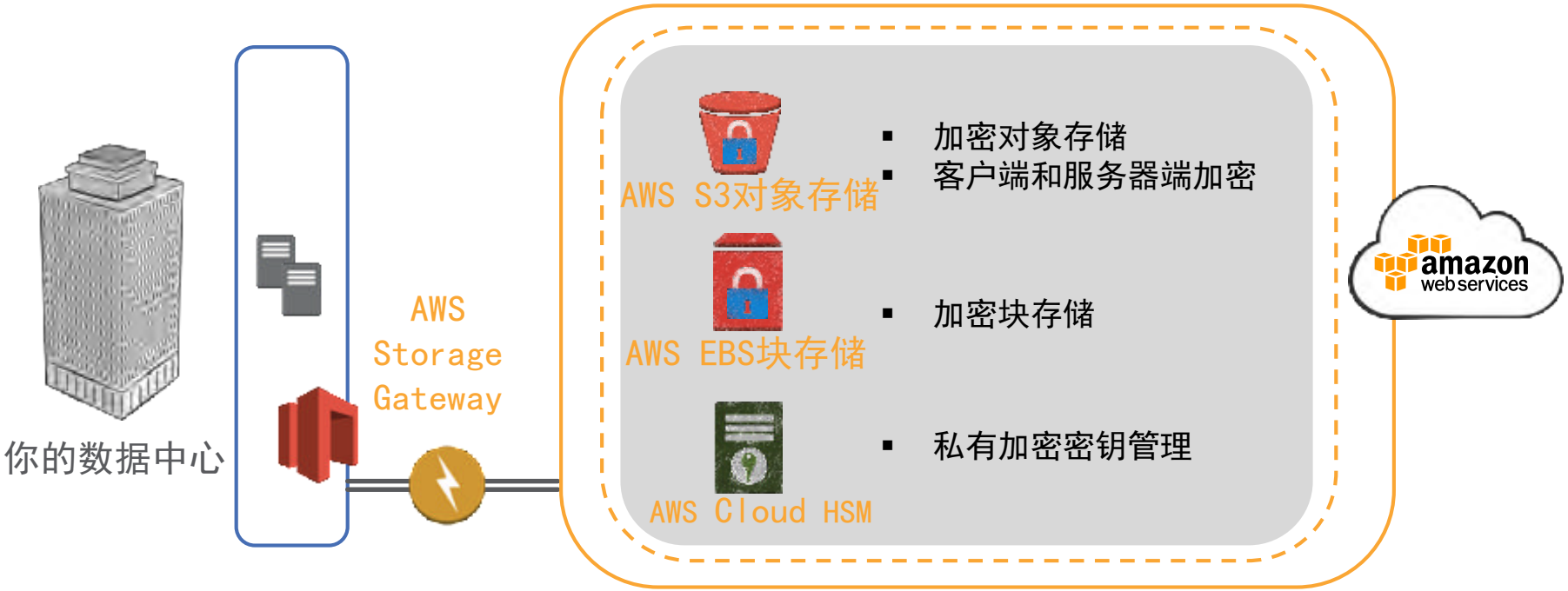
AWS的“私有”网络能力


你的数据中心
AWS Direct Connect
AWS虚拟私有云
Virtual Private Cloud (AWS VPC)
amazon
web services

AWS的“私有”计算能力


你的数据中心
虚机（AWS EC2）
用户定义的网络
网络逻辑隔离
AWS EC2专属实例
（Dedicated Instance）
物理隔离
单租户基础架构
amazon
web services

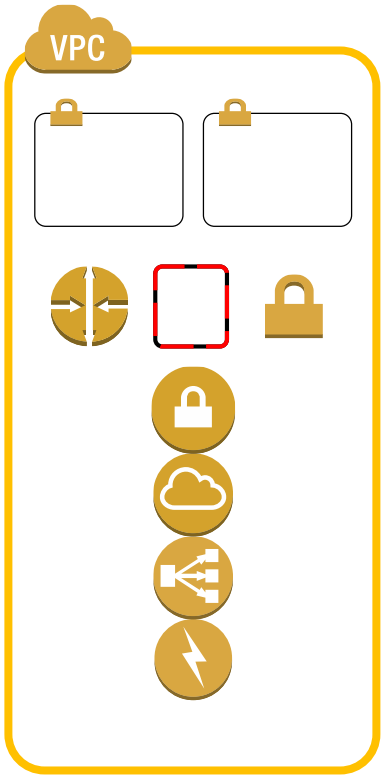
AWS的“私有”存储能力


你的数据中心
AWS
Storage
Gateway
AWS S3对象存储
加密对象存储
客户端和服务器端加密
AWS EBS块存储
加密块存储
AWS Cloud HSM
私有加密密钥管理
amazon
web services

日程

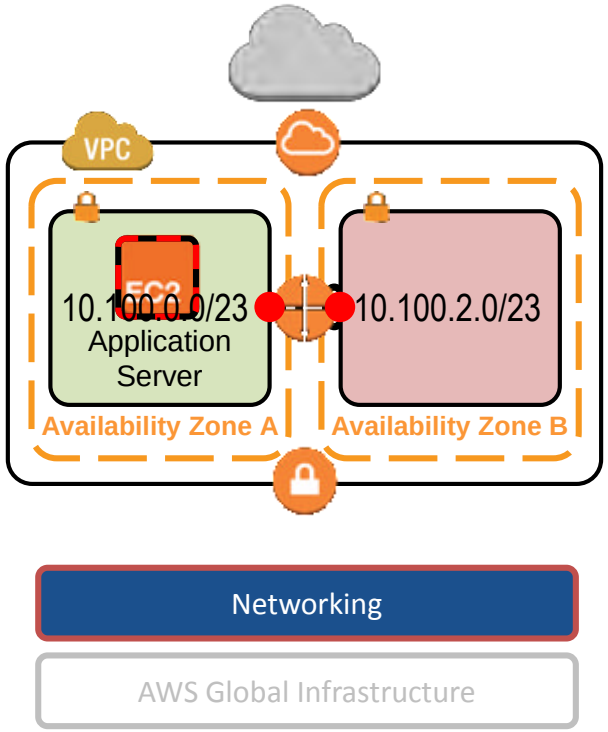
- 什么是混合IT架构
- AWS支持混合IT架构
- 基于AWS的混合IT架构的网络实现

AWS VPC介绍



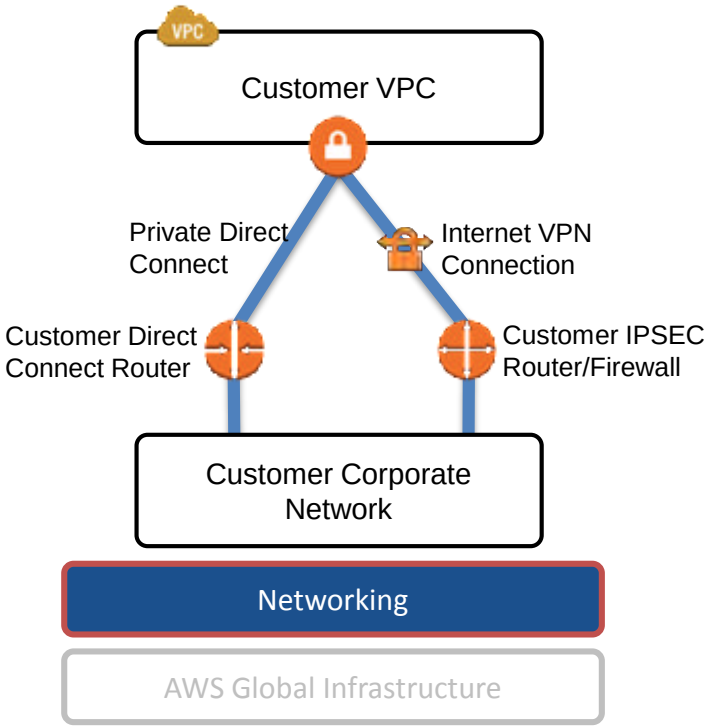
- 虚拟私有云（VPC, Virtual Private Cloud)
- 子网（Subnets）
- 路由表（Route Tables），安全组（Security Groups），网络访问控制列表（NACL）
- 虚拟私有网关（Virtual Private Gateway）
- Internet网关（Internet Gateway）
- 弹性IP和负载均衡（Elastic IPs and Load Balancers）
- AWS Direct Connect

将企业数据中心扩展到Amazon VPC



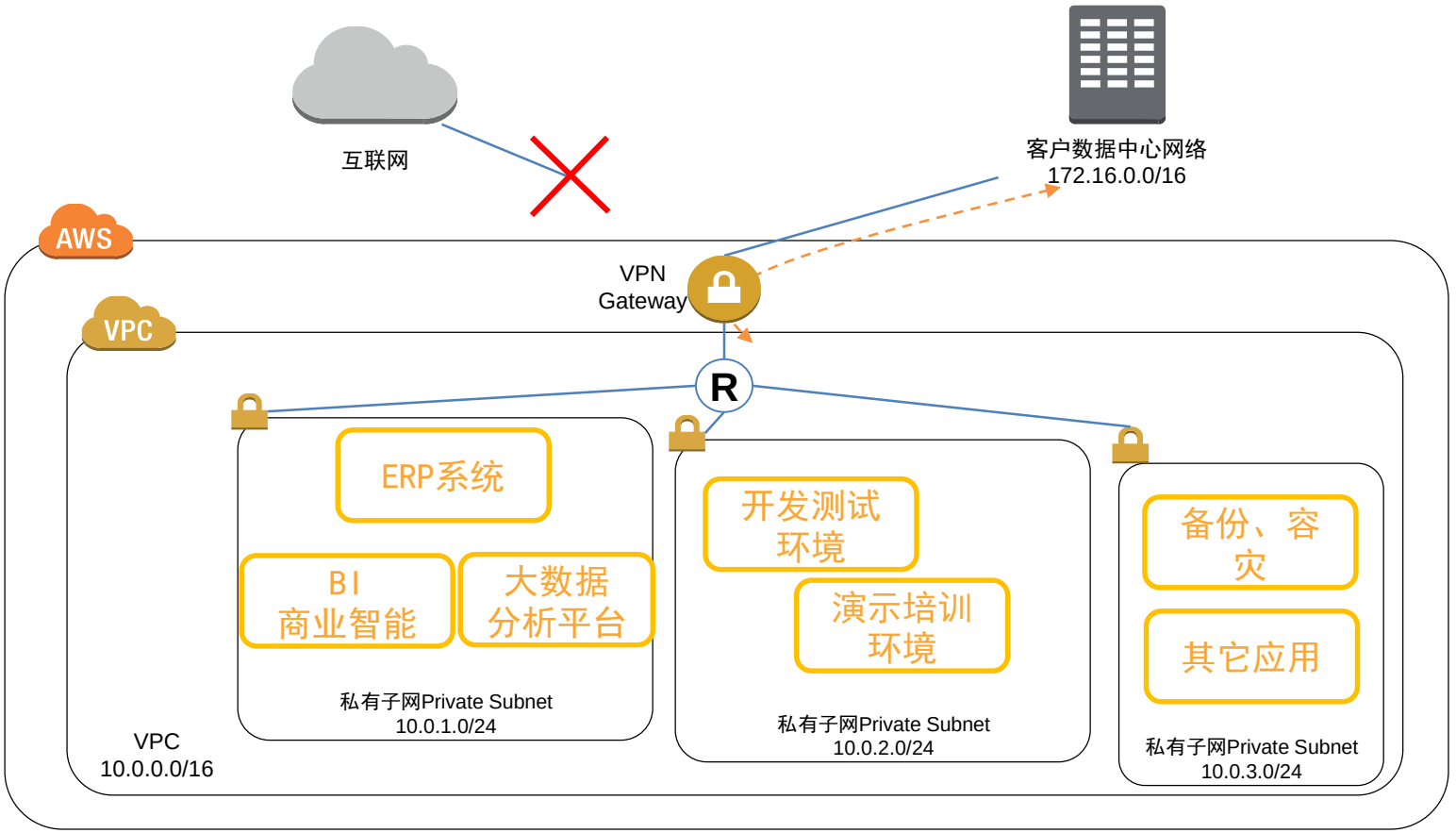
- 用企业自己指定的IP地址段在AWS cloud上创建逻辑上隔离的网络
- 企业拥有对虚拟网络环境完全的控制权，包括创建子网，定义IP地址，路由表和网关
- 在多个AZ创建公有和私有子网
- 企业自己选择将EC2实例部署到哪个子网
- 企业使用NACL管理子网层面的网络安全
- 企业自己管理EC2实例的安全组，为每个EC2实例提供网络防火墙

将企业数据中心扩展到Amazon VPC

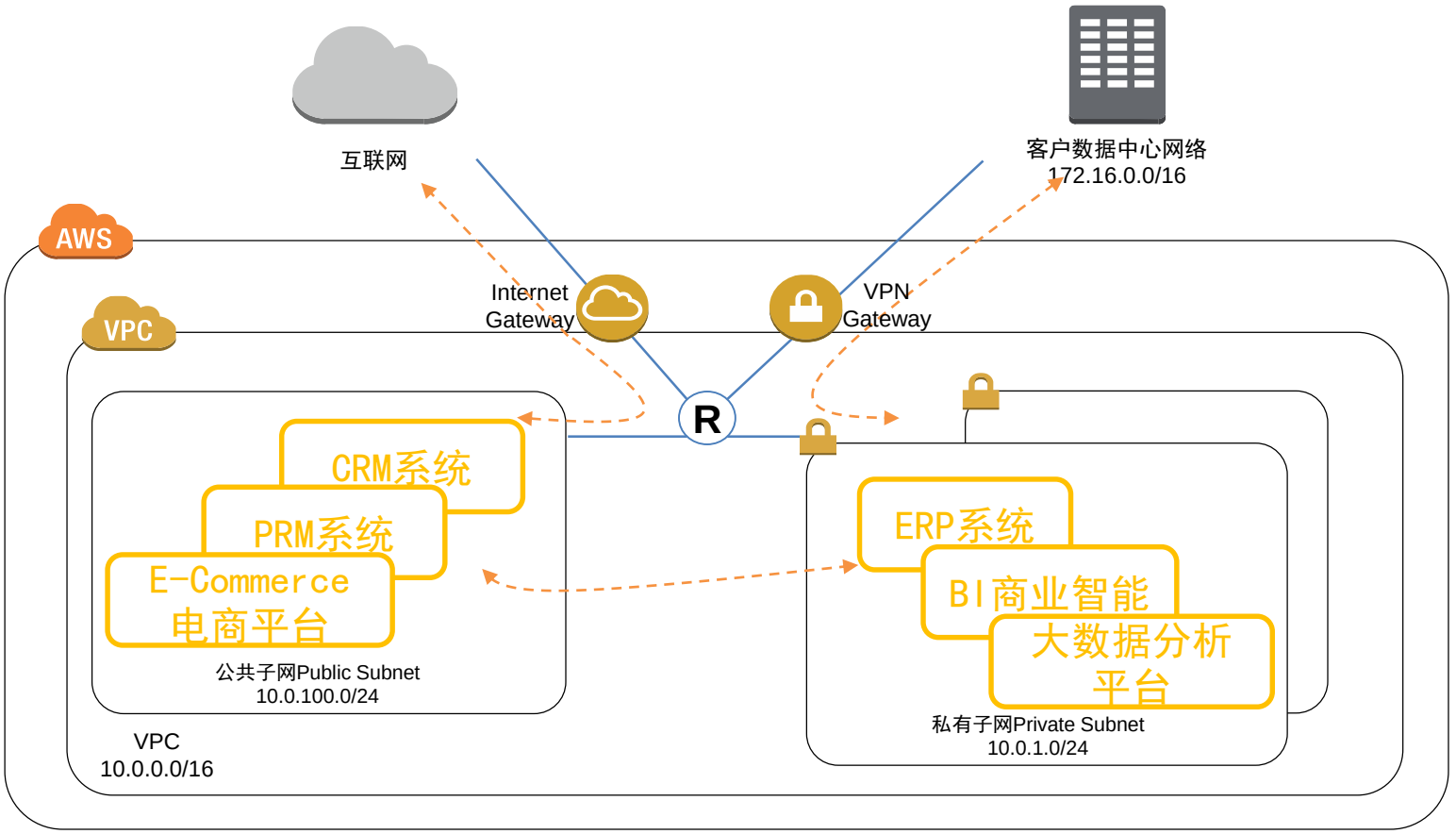


- 通过标准的基于互联网的IPSEC VPN tunnels
  - $0.05 per VPN Connection Hour ($36 per month)
  - Cisco, Juniper, Yamaha, Astaro, Fortinet, Vyatta,etc
  - 支持BGP和静态路由
- 通过AWS Direct Connect，或者两者的结合
  - Direct Connect的连接速度支持从50M to 10G, 企业自己选择

AWS VPC应用场景示例一：数据中心扩展



AWS VPC应用场景示例二：混合IT架构



AWS VPC:按照企业级的安全要求构建

“亚马逊的虚拟私有云（VPC）是一个独特的选择，它提供了一层额外的安全和一个让我们可以与已有的基础设施进行集成的能力。”

Dr. Michael Miller, 研发团队负责人

Pfizer

http://aws.amazon.com/cn/solutions/case-studies/pfizer/

亚马逊 aws

AWS VPC:按照企业级的安全要求构建

WITH **AWS CLOUD**, WE MET OUR **RELIABILITY** AND **PERFORMANCE OBJECTIVES** AT A **FRACTION OF THE COST**; WE WOULD HAVE SPENT **$34 MILLION DOLLARS** IN HARDWARE AND MAINTENANCE EXPENSES DURING THE FIRST TWO YEARS

- **Chun Kang**
Principal Engineer,
Visual Display Division

比传统的托管服务节约了85%

节约了3400万美元

SAMSUNG

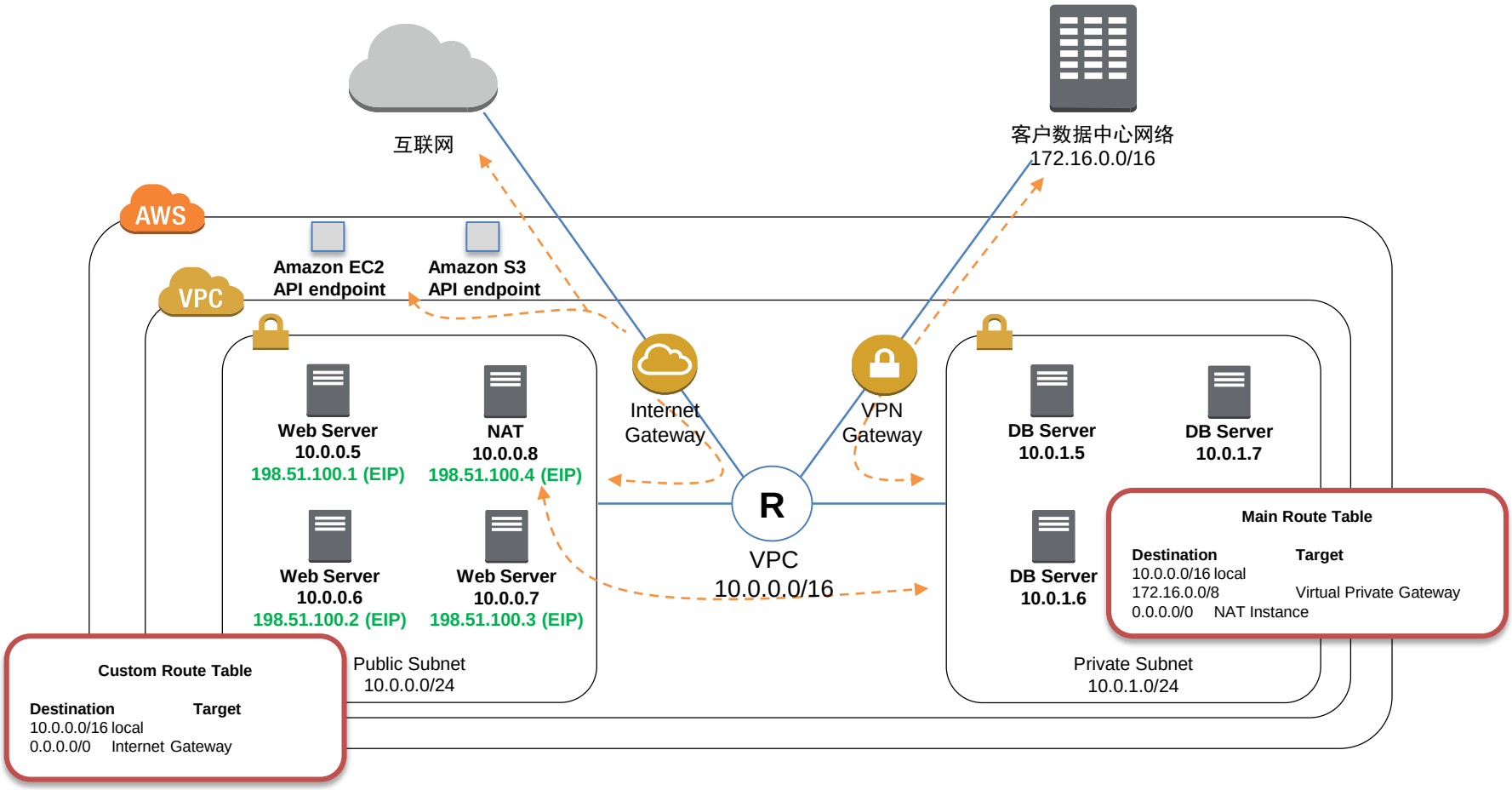
亚马逊 aws

NASA JPL – 混和IT架构

- NASA – license servers, ISMS, Deep Space Network, RADAR
- AWS –工作流SWF，存储, 计算, 负载均衡，大数据分析，内容分发 …

http://aws.amazon.com/cn/swf/testimonials/swfnasa/

AWS VPC演示：五分钟构建属于你自己的数据中心



谢谢大家！

亚马逊AWS中文博客：http://blog.csdn.net/awschina

AWS VPC： http://aws.amazon.com/vpc