RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

软件定义的网络与安全

臧铁军 CISSP

VMware

RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

专题会议编号：CS-2005

专题会议分类：云安全

议程

- 数据中心的变革
- 软件定义的网络
  - 数据中心网络虚拟化
  - 云环境下的新一代网络虚拟化
- 软件定义的安全
  - 云环境下的安全挑战
  - 基于软件的安全性

议程

- 数据中心的变革
- 软件定义的网络
  - 数据中心网络虚拟化
  - 云环境下的新一代网络虚拟化
- 软件定义的安全
  - 云环境下的安全挑战
  - 基于软件的安全性

硬件功能软件化是发展趋势

THE WALL STREET JOURNAL.

ESSAY | AUGUST 20, 2011

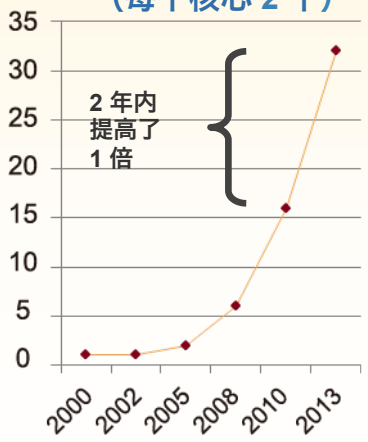
Why Software Is Eating The World

By MARC ANDREESSEN

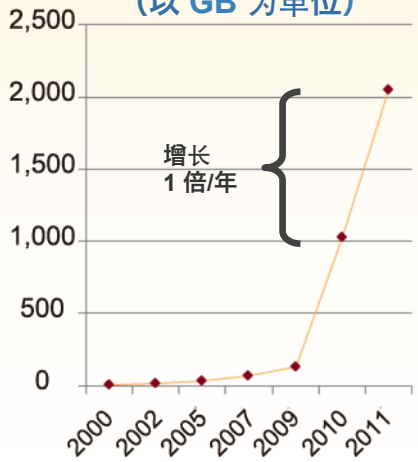
用软件取代硬件成为数据中心发展趋势

驱动数据中心变革的三股力量

每个插槽线程数（每个核心 2 个）

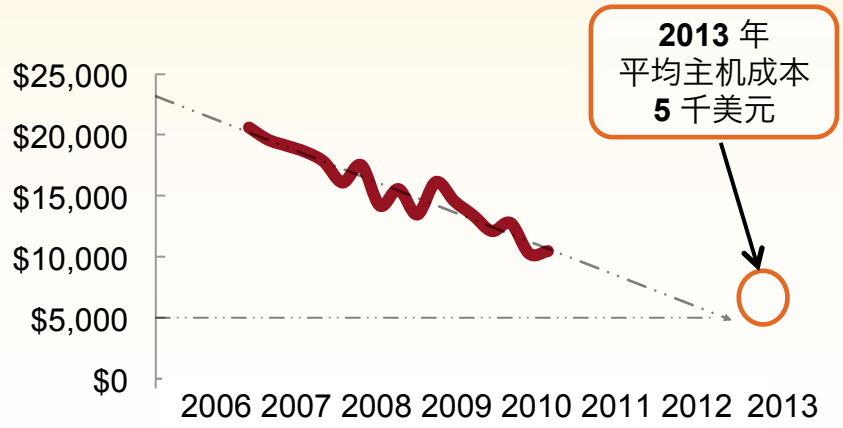


最大内存（以 GB 为单位）



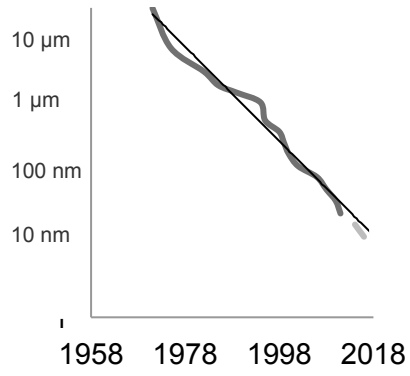
资料来源：Forrester Research，*x86* 服务器的兴衰（2010 年 10 月 8 日）

每个虚拟化服务器的平均成本

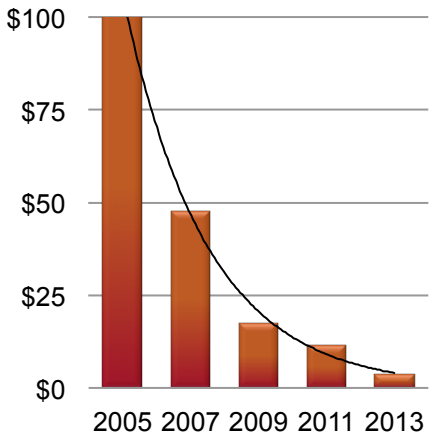


资料来源：IDC Worldwide Virtualization Tracker，2010 年

CPU处理技术



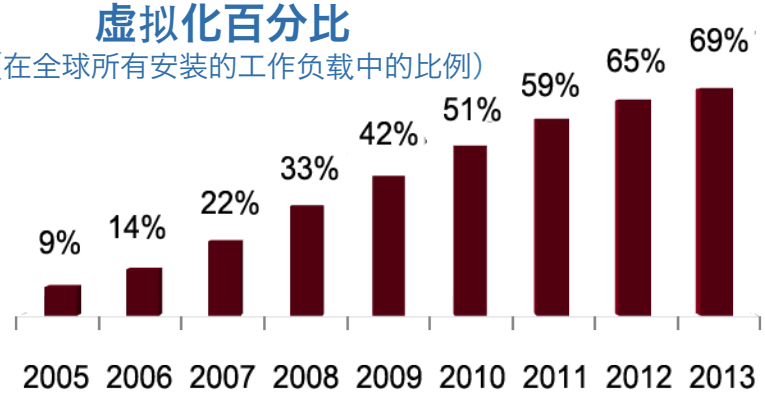
DRAM GB价格(美元)



资料来源：Gartner Dataquest，预测：*DRAM* 市场统计（2011 年第 1 季度）

虚拟化百分比

（在全球所有安装的工作负载中的比例）



新的数据中心体系架构

资料来源：IDC Worldwide Virtualization Tracker，2010 年

结果？全新的数据中心！

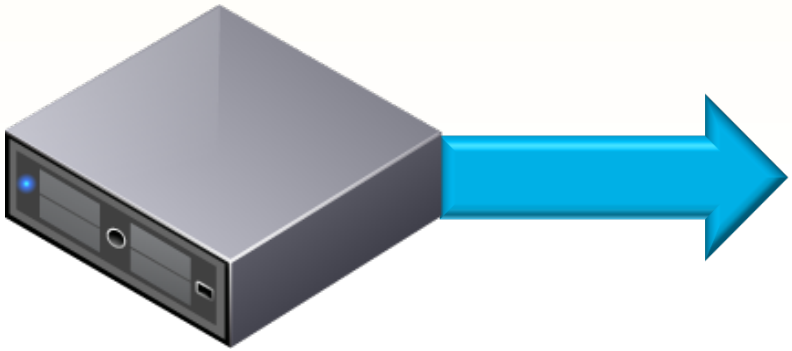
- 到2014年，平均每台服务器将拥有：
  - 2个CPU，每CPU16核心
  - 300GB内存
  - 承载320个虚拟机

对于一家拥有*5,000*名员工的中型公司，
其信息系统可容纳于冰箱大小的空间！

基于*x86*架构，由软件定义的数据中心

降低成本，提高敏捷度

过去……



$10,000
10周

现在……

$30,000
2分钟

企业存储

VLAN网络

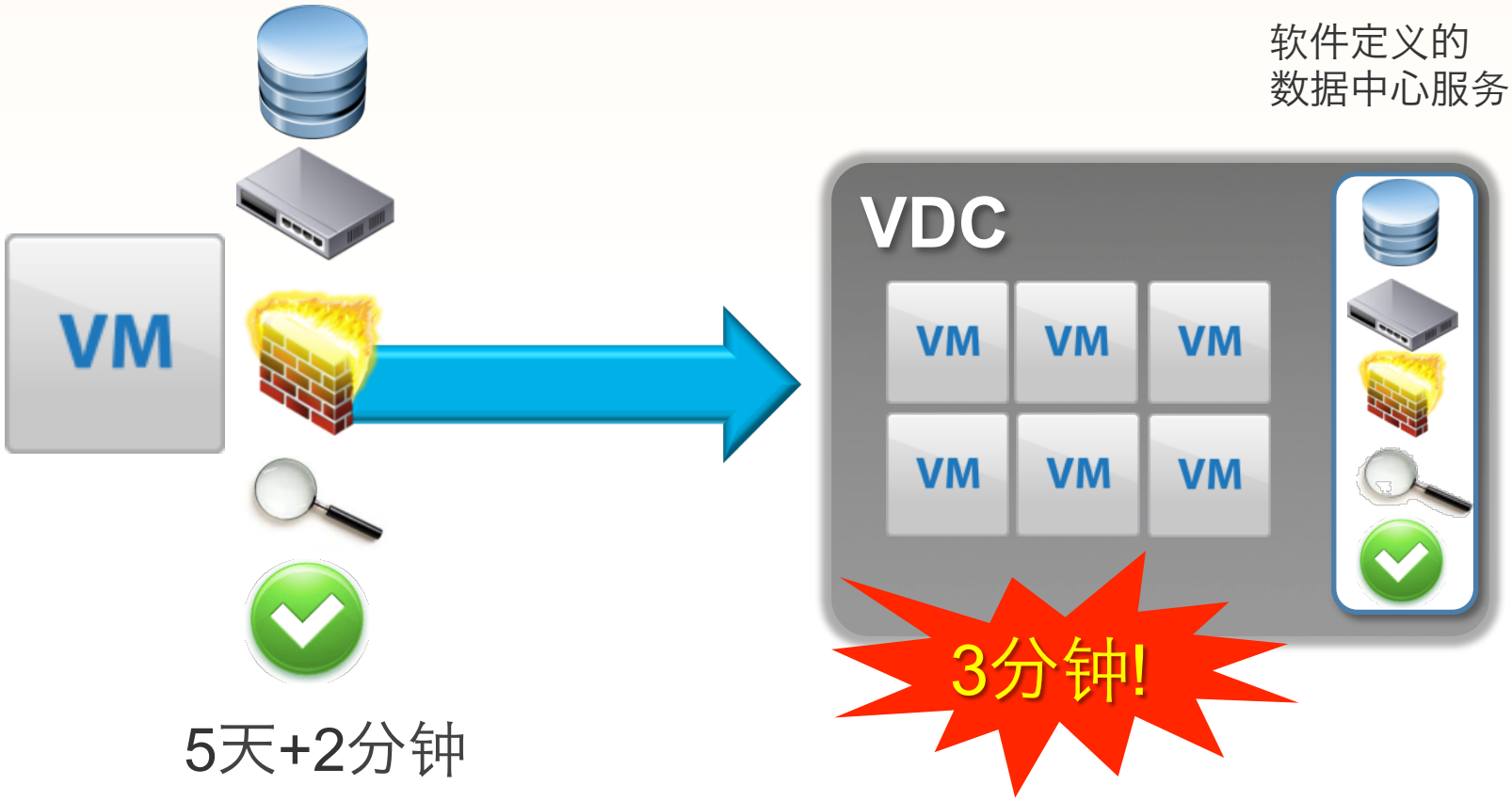
防火墙,
负载平衡

IDS, 安全监控

可用性

虚拟化更多服务资源

未来……

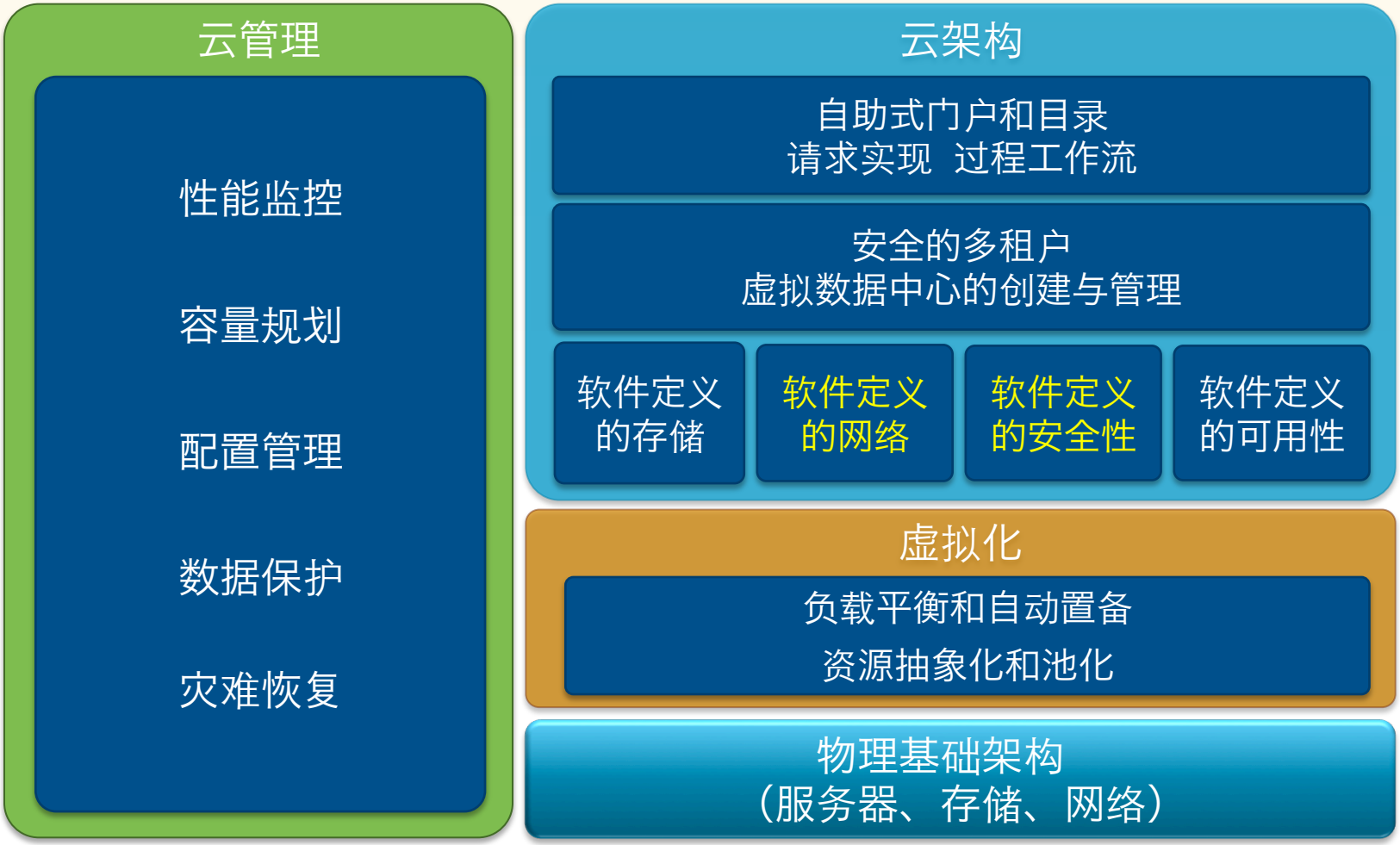


软件定义的
数据中心服务

5天+2分钟

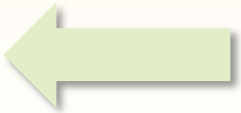
在软件定义的数据中心里……

云基础架构与管理组件

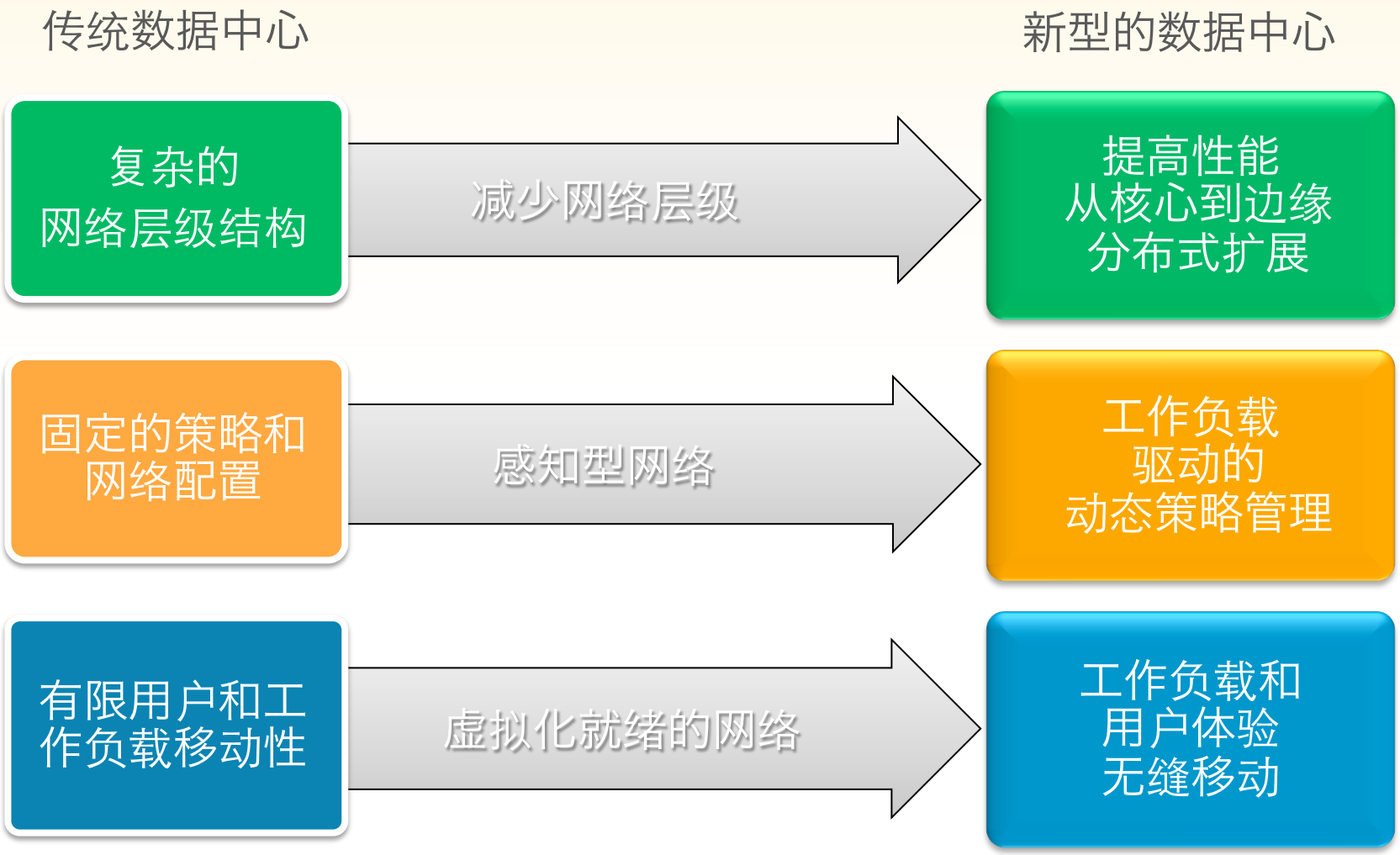

云管理
性能监控
容量规划
配置管理
数据保护
灾难恢复
云架构
自助式门户和目录
请求实现 过程工作流
安全的多租户
虚拟数据中心的创建与管理
软件定义的存储
软件定义的网络
软件定义的安全性
软件定义的可用性
虚拟化
负载平衡和自动置备
资源抽象化和池化
物理基础架构
（服务器、存储、网络）

议程

- 数据中心的变革
- 软件定义的网络
  - 数据中心网络虚拟化
  - 云环境下的新一代网络虚拟化
- 软件定义的安全
  - 云环境下的安全挑战
  - 基于软件的安全性



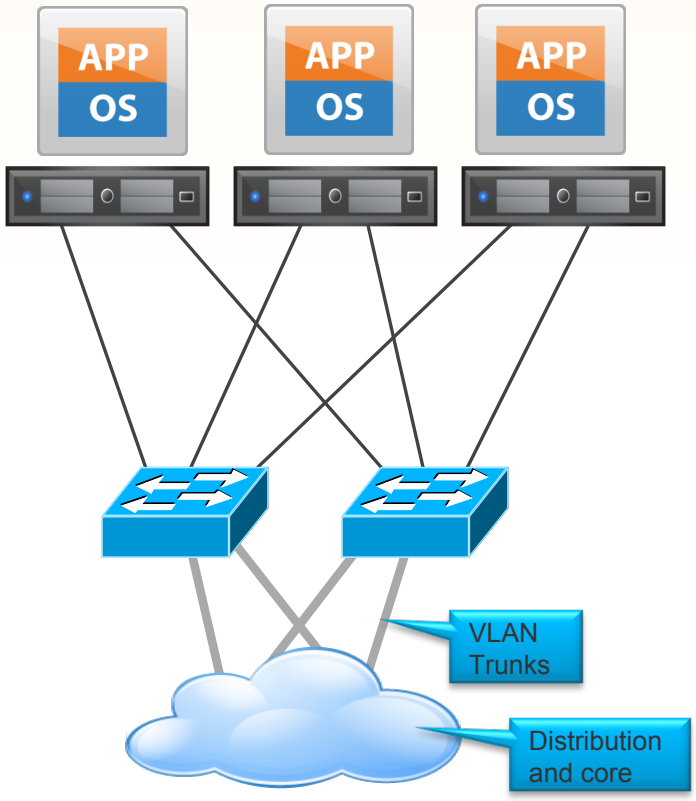
快速交付应用的分布式扁平网络



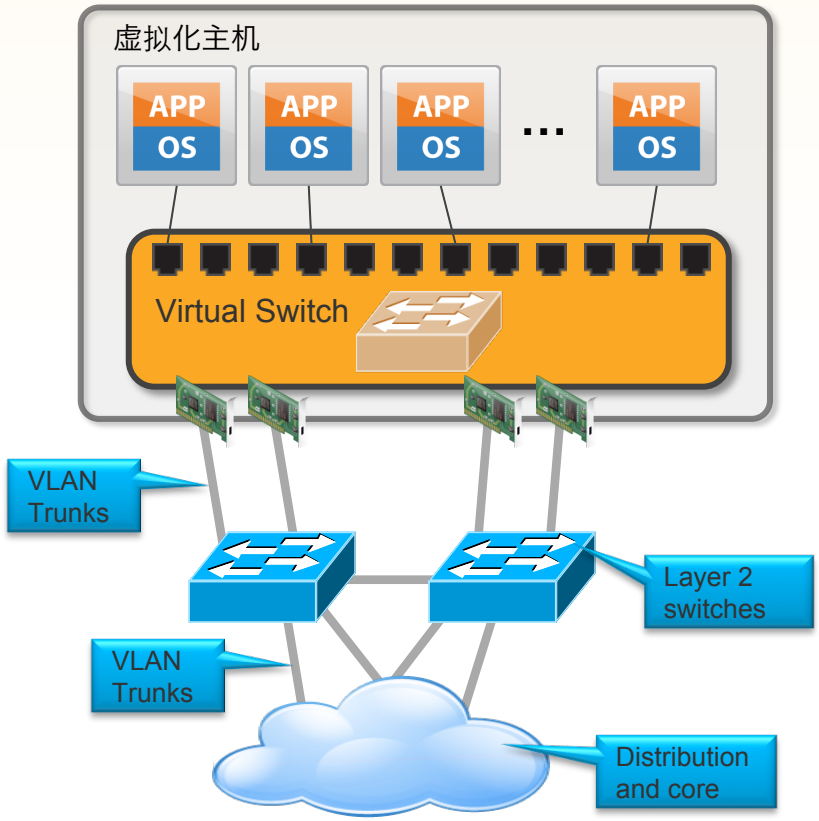
混乱的网络接入

第1代虚拟交换机：简化接入层

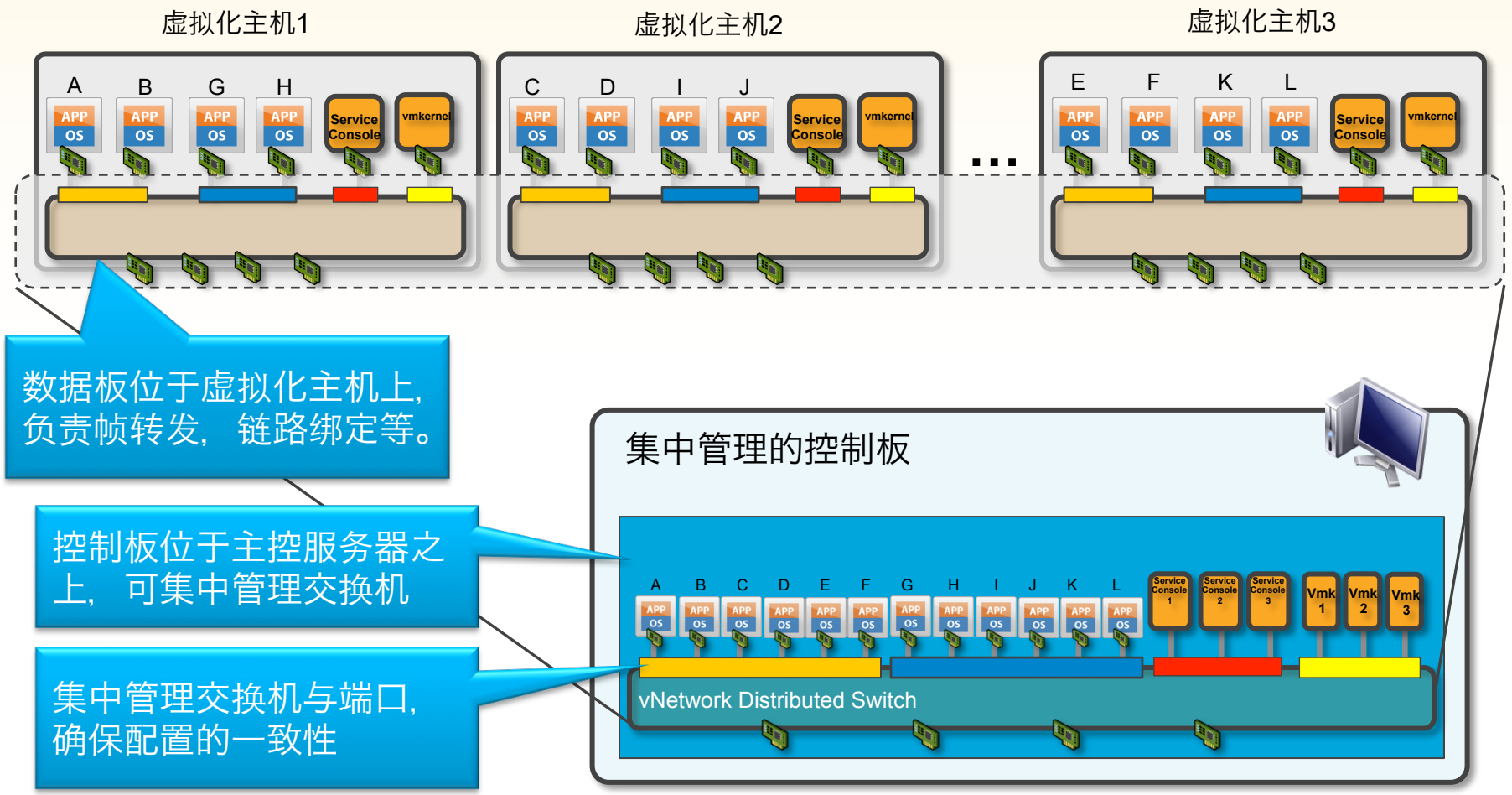
未采用虚拟化技术



采用虚拟化技术



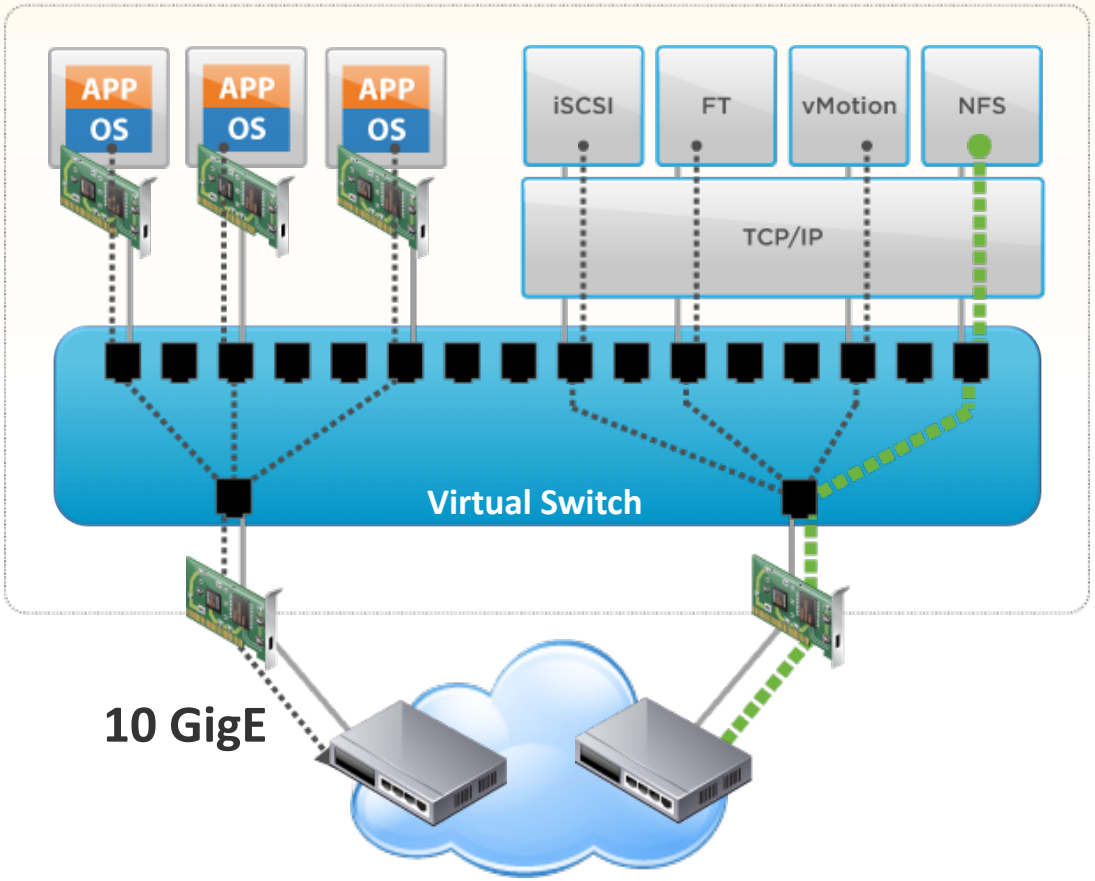
第2代虚拟交换机：进一步简化管理

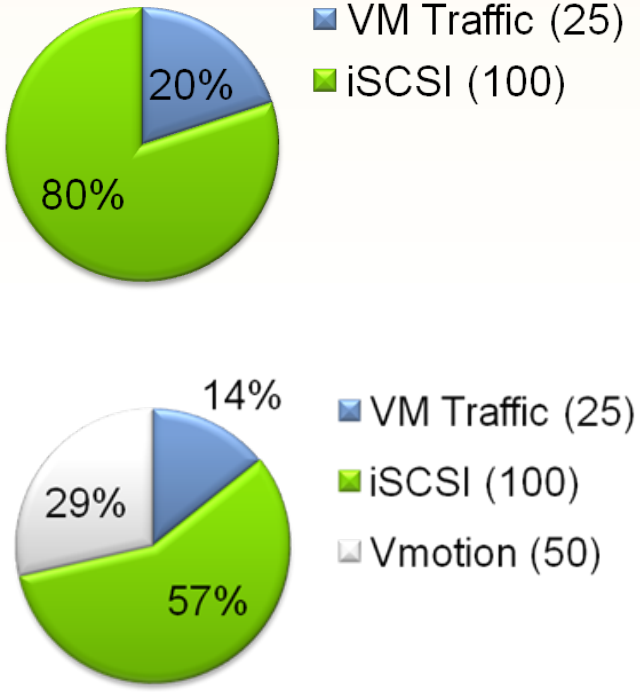


虚拟化平台网络流量分类

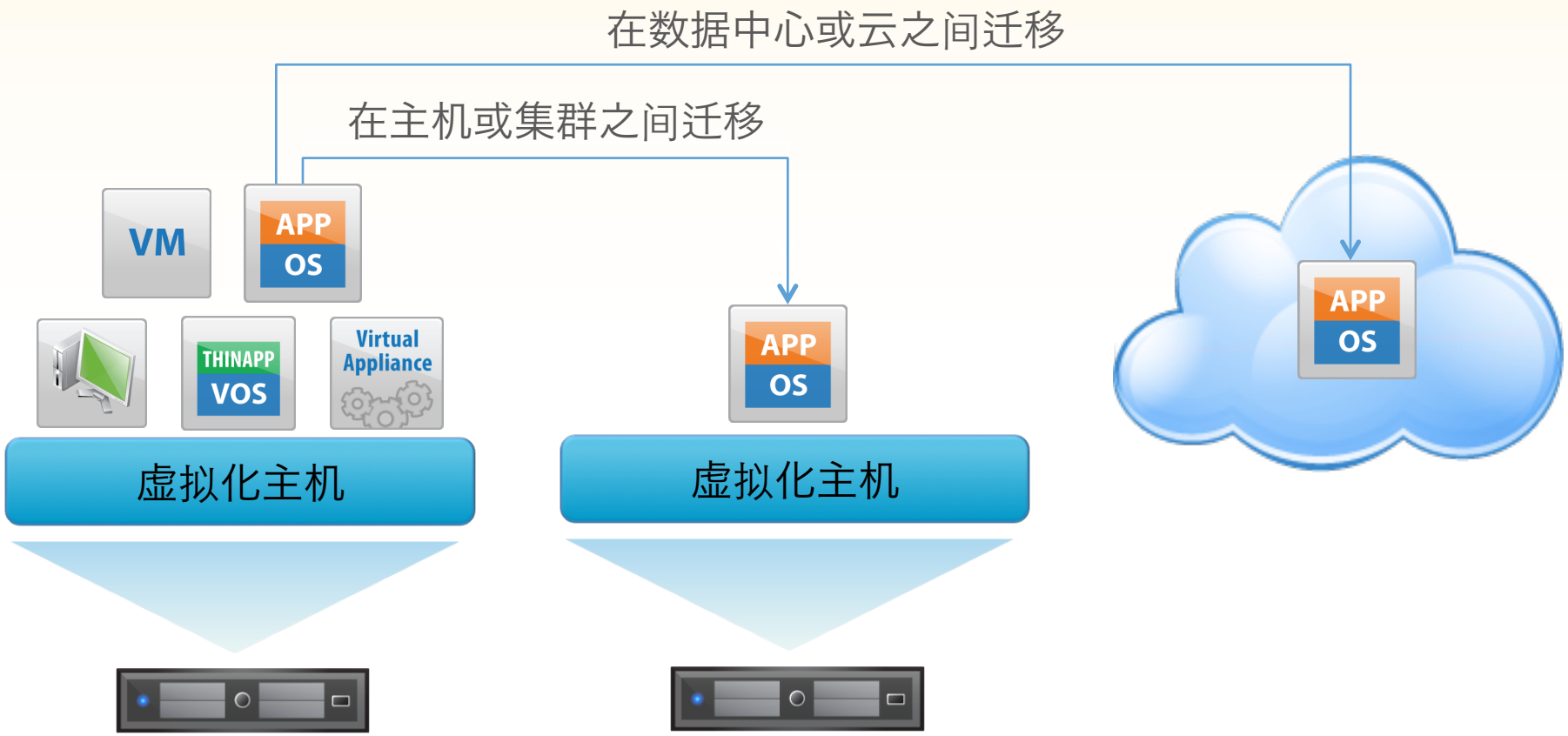
- Management Traffic – 管理流量
  - 低利用率
  - 相对重要
- Ethernet Storage – iSCSI, NAS IP存储流量
  - 高重要度
  - 高利用率
- Virtual Machine Traffic – 生产虚拟机流量
  - 中等利用率
  - 高重要度
- vMotion – 在线迁移流量
  - 突发性流量
  - 高带宽占用
- Fault Tolerance – 状态同步流量
  - 高度重要
  - 高带宽占用

网络I/O控制

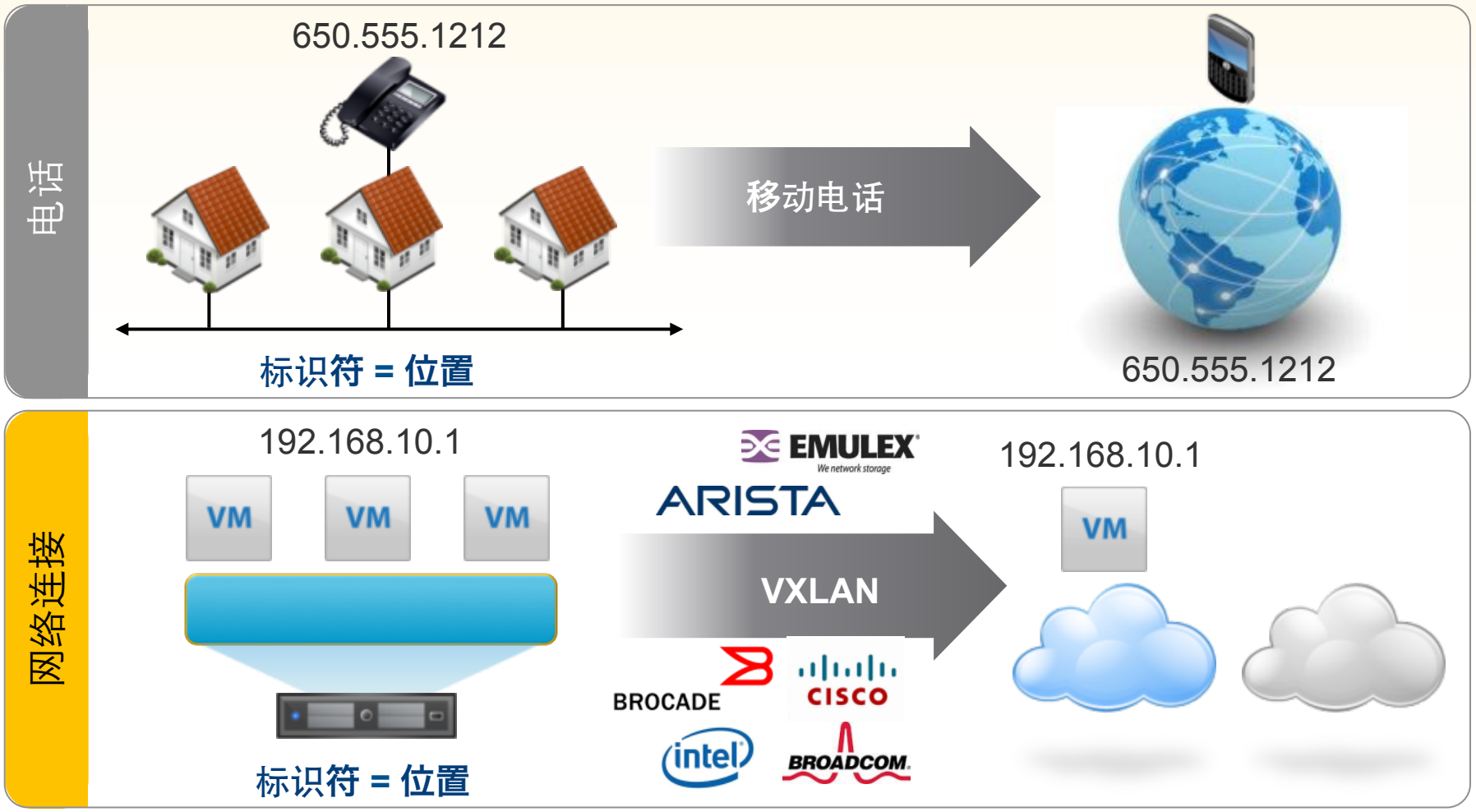

APP
OS
APP
OS
APP
OS
iSCSI
FT
vMotion
NFS
TCP/IP
Virtual Switch
10 GigE


20%
80%
VM Traffic (25)
iSCSI (100)
14%
29%
57%
VM Traffic (25)
iSCSI (100)
Vmotion (50)

需求：工作负载可任意迁移



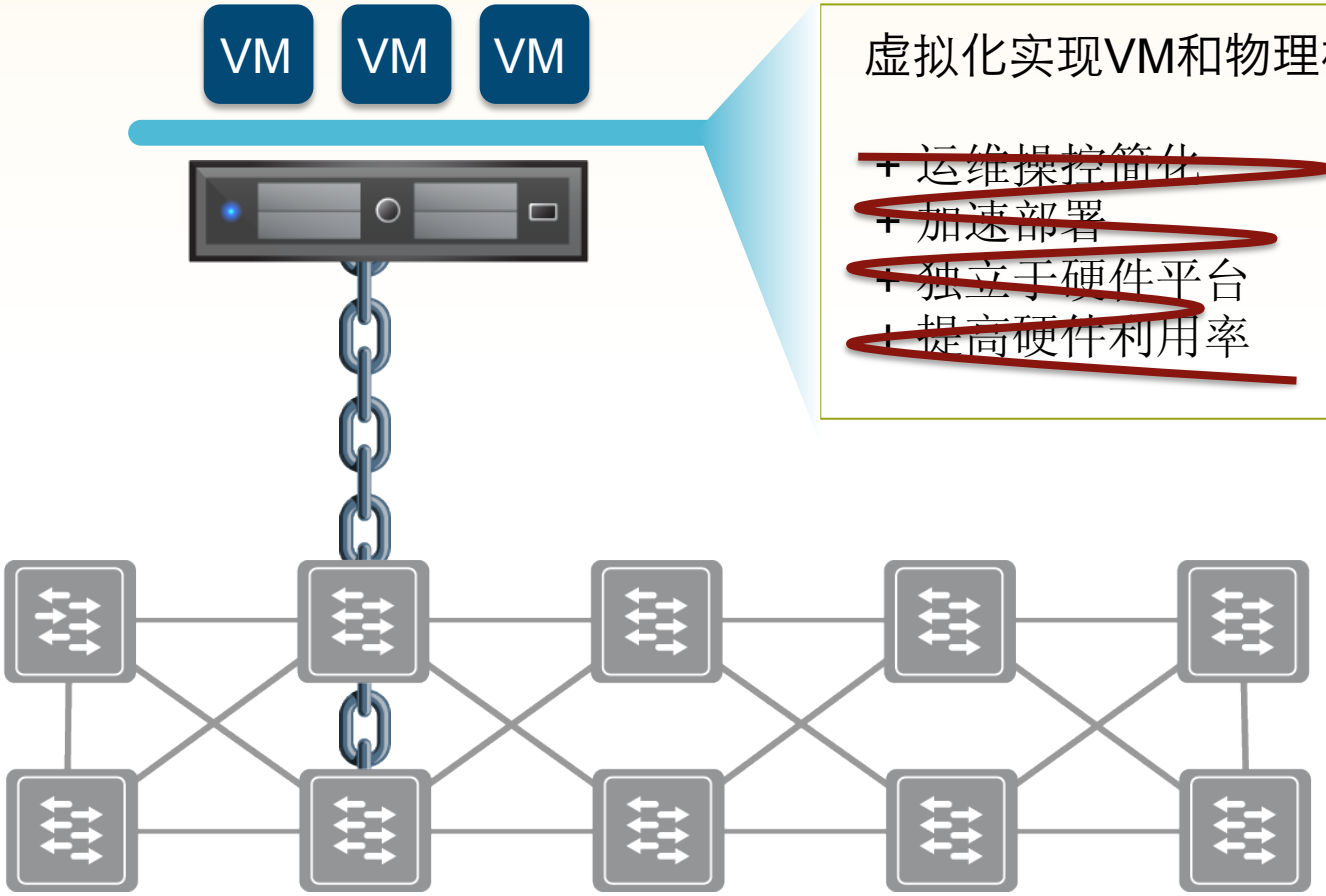
用户需要良好的扩展性与灵活性



现实没有那么完美

虚拟机

物理机



虚拟化实现VM和物理机隔离

+ 运维操控简化
+ 加速部署
+ 独立于硬件平台
+ 提高硬件利用率

网络虚拟化是解决之道

虚拟

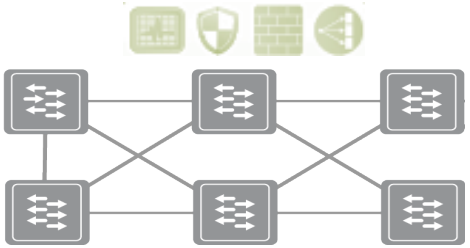
1. 解除锁定

物理

硬件无关性

虚拟

2. 灵活



物理

主机不需要
配合网络的改变

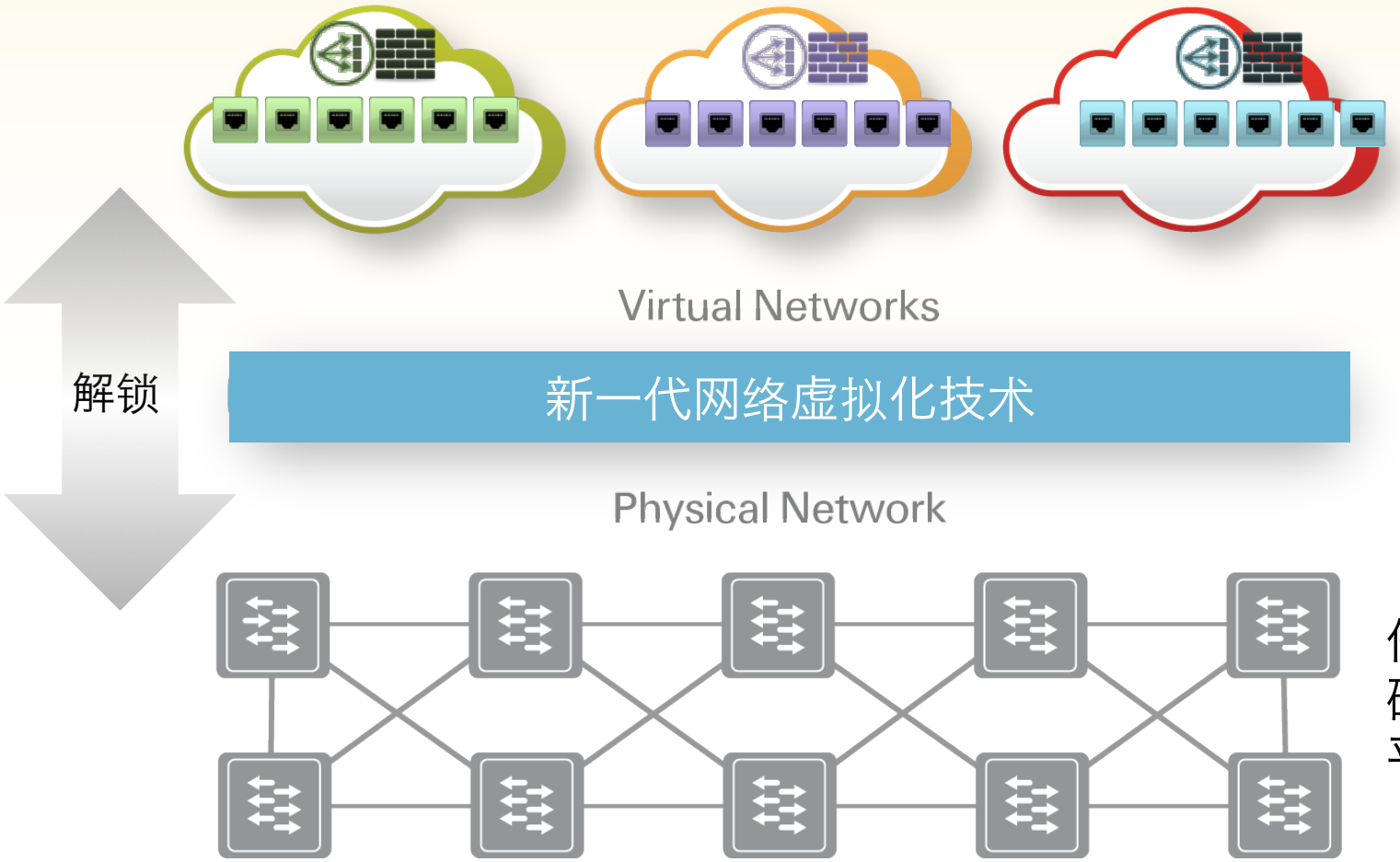
网络操作

3. 自动化

云操作

提升运维效率

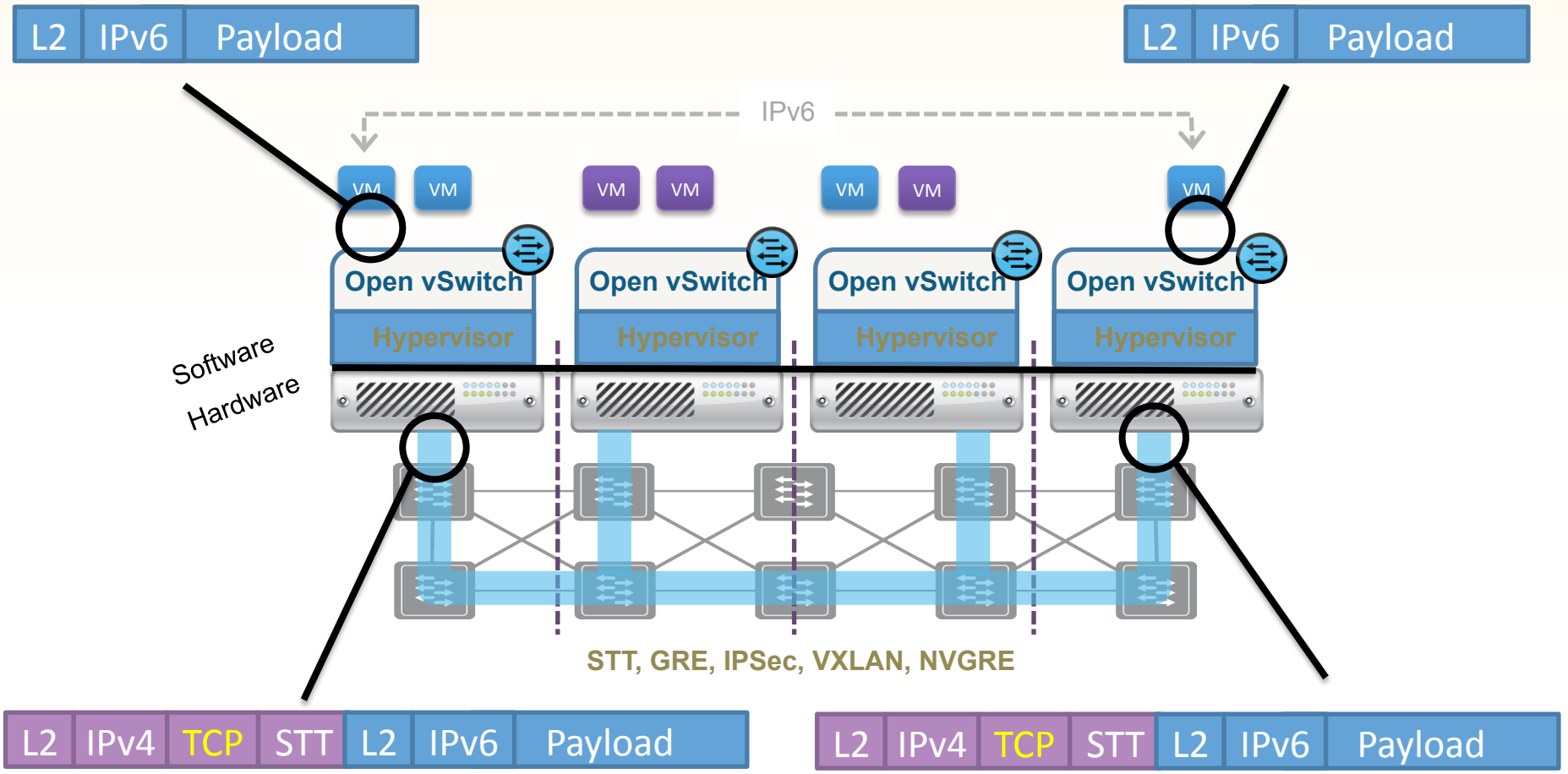
全新一代网络虚拟化技术



网络虚拟化市场发展迅猛

协议	厂商
VXLAN	VMware, Cisco, Citrix, Red Hat, Arista, Brcoade, Broadcom, Dell, Emulex, Intel
OpenFlow	Juniper, HP, IBM, NEC, Nicira, Big Switch, Brocade, Others
NVGRE	Microsoft, HP, Dell, Intel, Arista, Emulex
STT	Nicira
OTV	Cisco
LISP	Cisco
TRILL	Brocade/Cisco
Shortest Path Bridging	Avaya, Alcatel-Lucent

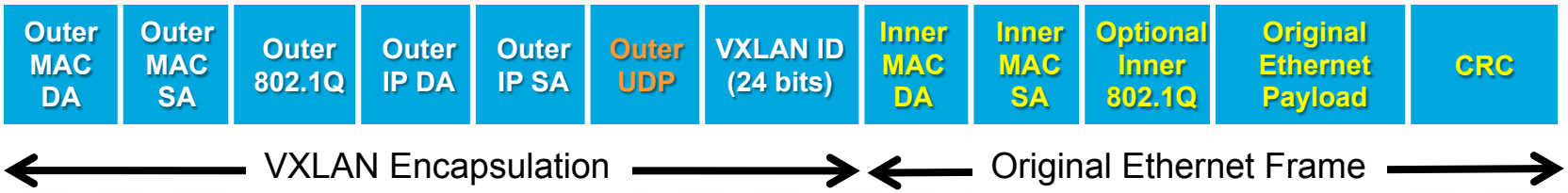
通道技术：不依赖于物理网络配置



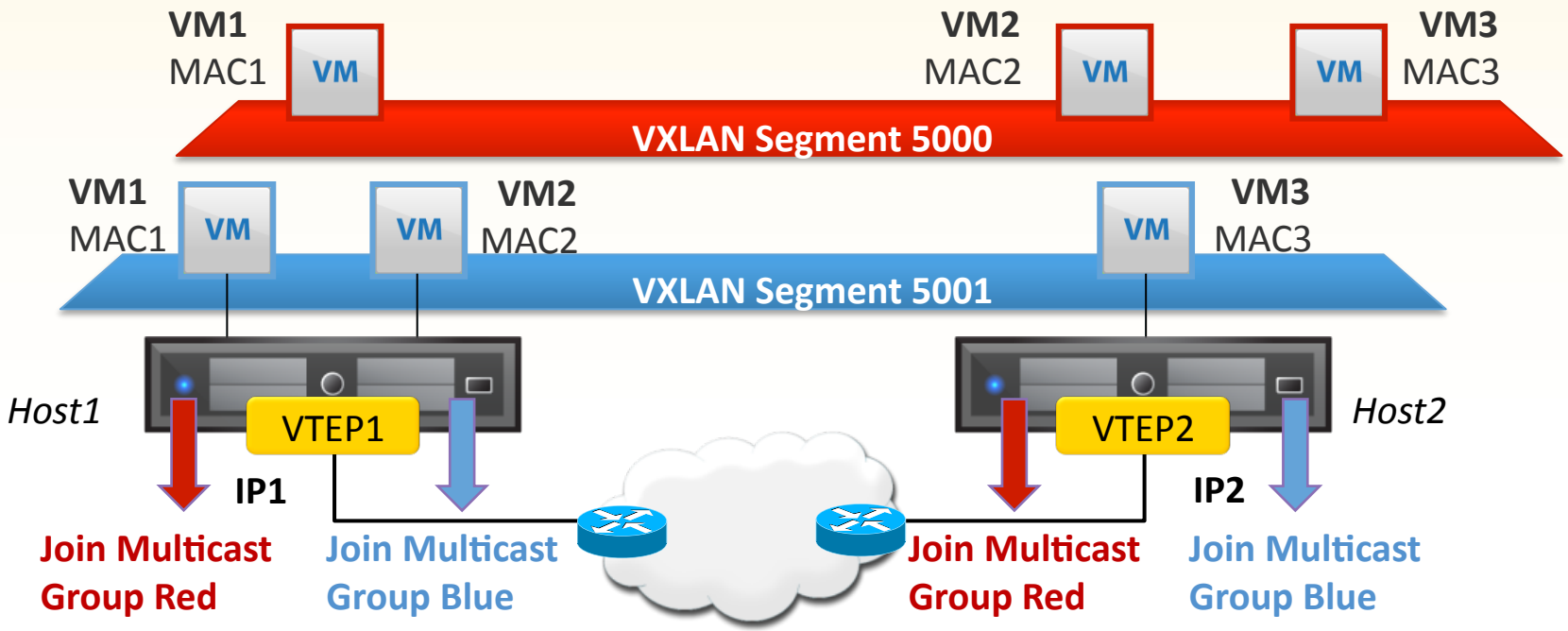
VXLAN：实现方式

主要特点

- 可工作于任何交换网络(需组播支持)
- 开放的标准



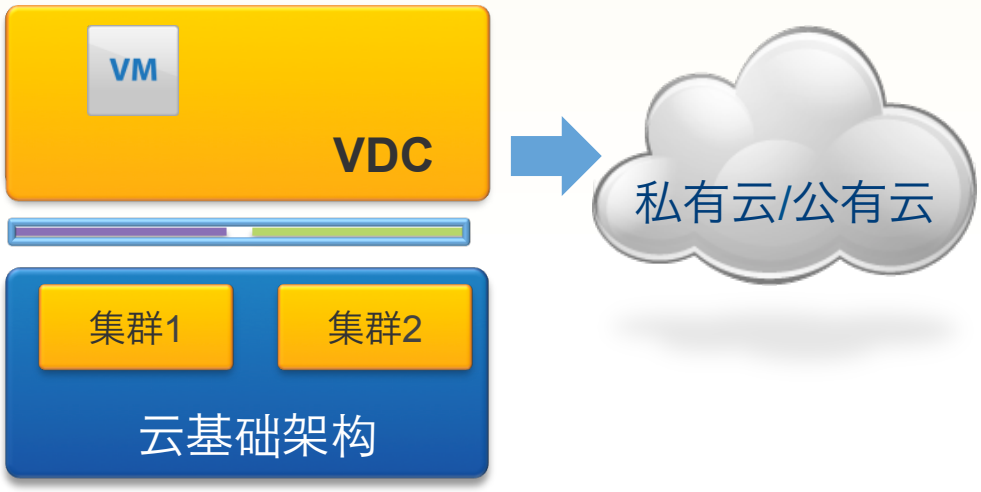
VXLAN网关与转发表



VNI	Inner MAC	Outer MAC/IP
5001	MAC1	Local
5001	MAC2	Local
5001	MAC3	**VTEP2**

VNI	Inner MAC	Outer MAC/IP
5001	MAC1	**VTEP1**
5001	MAC2	**VTEP1**
5001	MAC3	Local

VXLAN的价值



- 可跨集群、子网和站点移动资源。
- 是构建弹性*VDC*的基础。
- 可按需部署网络，不需要重构物理网络。
- 实现便携的数据中心。
- 不受限于*VLAN*，多租户环境下提供良好的扩展性。

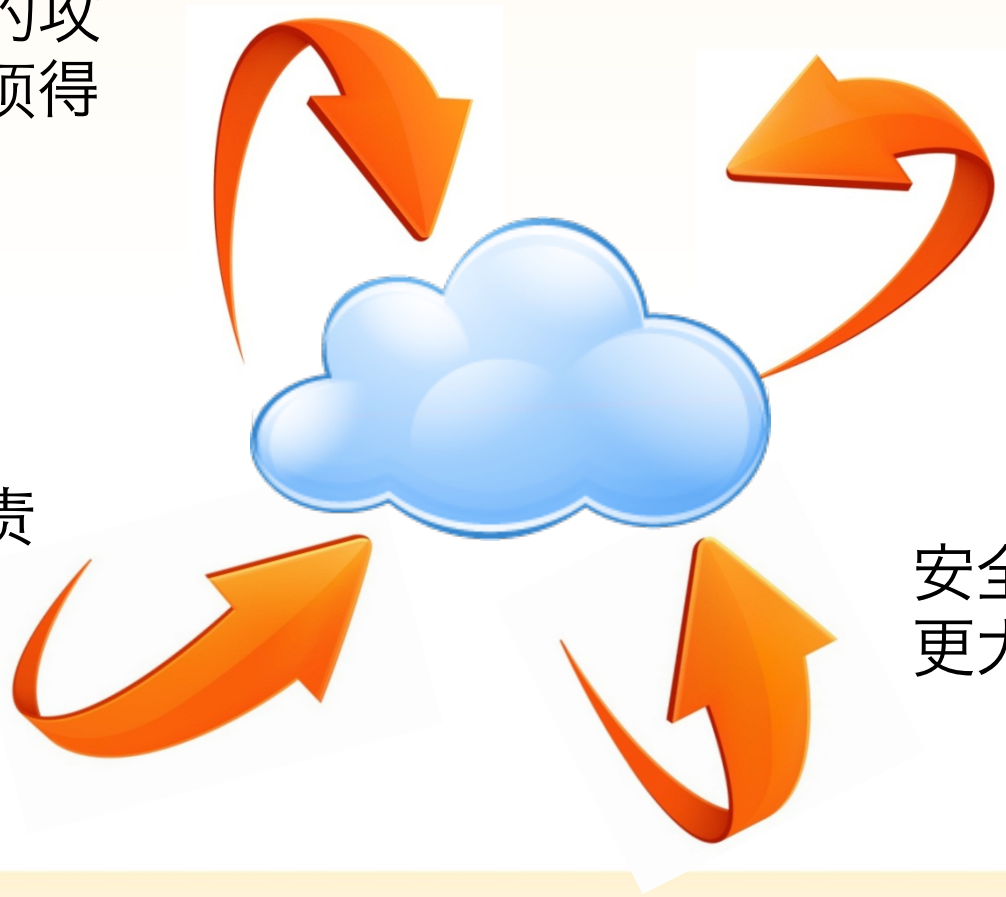
议程

- 数据中心的变革
- 软件定义的网络
  - 数据中心网络虚拟化
  - 云环境下的新一代网络虚拟化
- 软件定义的安全
  - 云环境下的安全挑战
  - 基于软件的安全性

云中安全性更具挑战

引入了新的攻击面，必须得到强化。

灵活多变，多租户环境下复杂度增加，用户的控制力减弱。



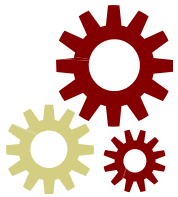
角色与职责需要明确。

安全事件的影响更大。

云安全三大要件

安全性是指为应用、数据、服务器、存储和网络提供保护，防止恶意软件和未经授权的人员对其进行访问。

遵从性是指可证明符合标准或法规要求。



可用性是指可连续保障业务运转的能力。

云安全三大要件

安全性是指为应用、数据、服务器、存储和网络提供保护，防止恶意软件和未经授权的人员对其进行访问。

遵从性是指可证明符合标准或法规要求。

可用性是指可连续保障业务运转的能力。

物理安全设备与物理隔离

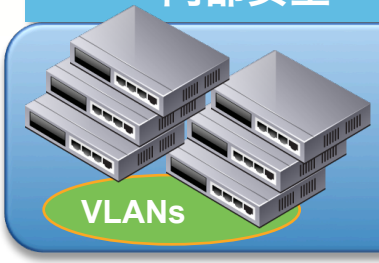
传统数据中心的纵深防御体系

边界安全

- 周边安全设备
- 防火墙, VPN, 入侵检测系统
- 负载均衡

将威胁隔绝在系统之外

内部安全



- 基于VLAN或者子网的策略
- 内部的或者Web应用防火墙
- DLP, 以应用标识为依据的策略

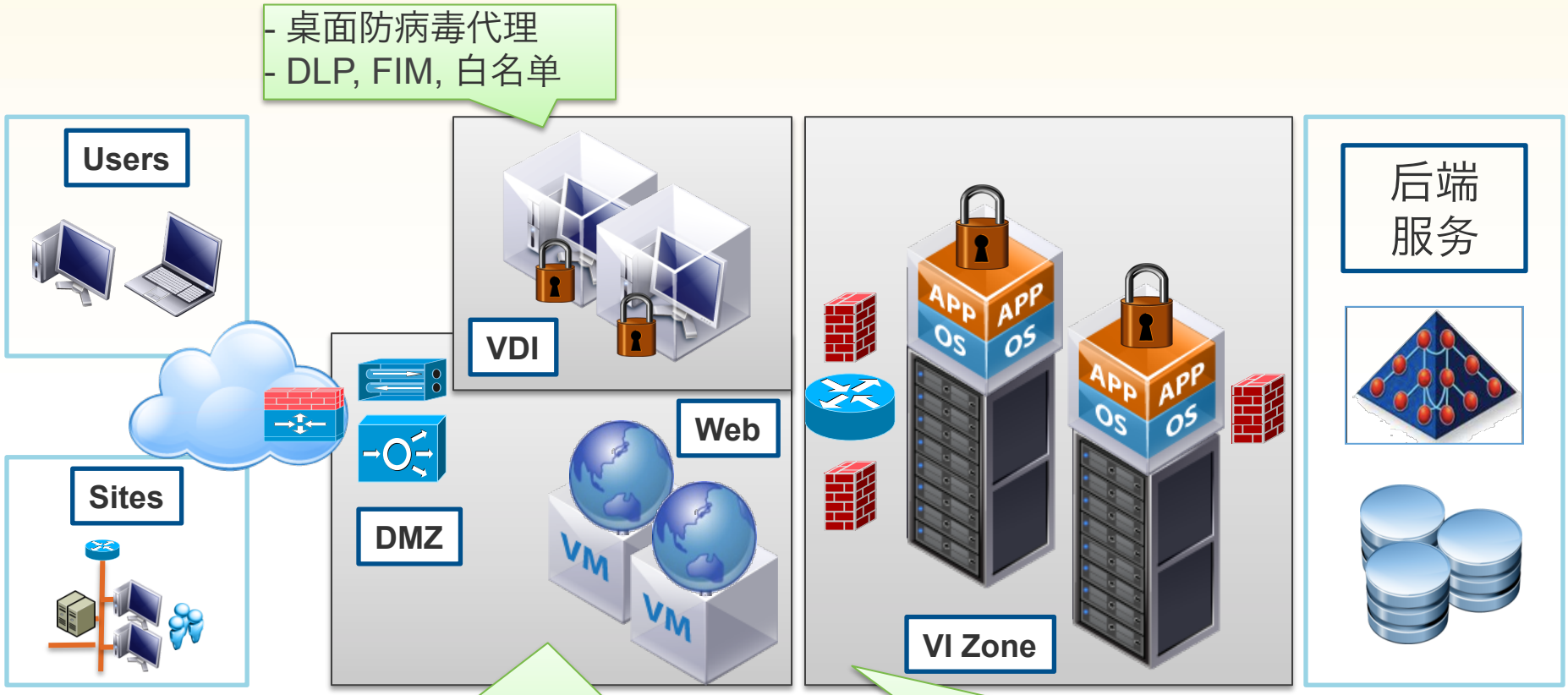
隔离内部服务和应用

端点安全

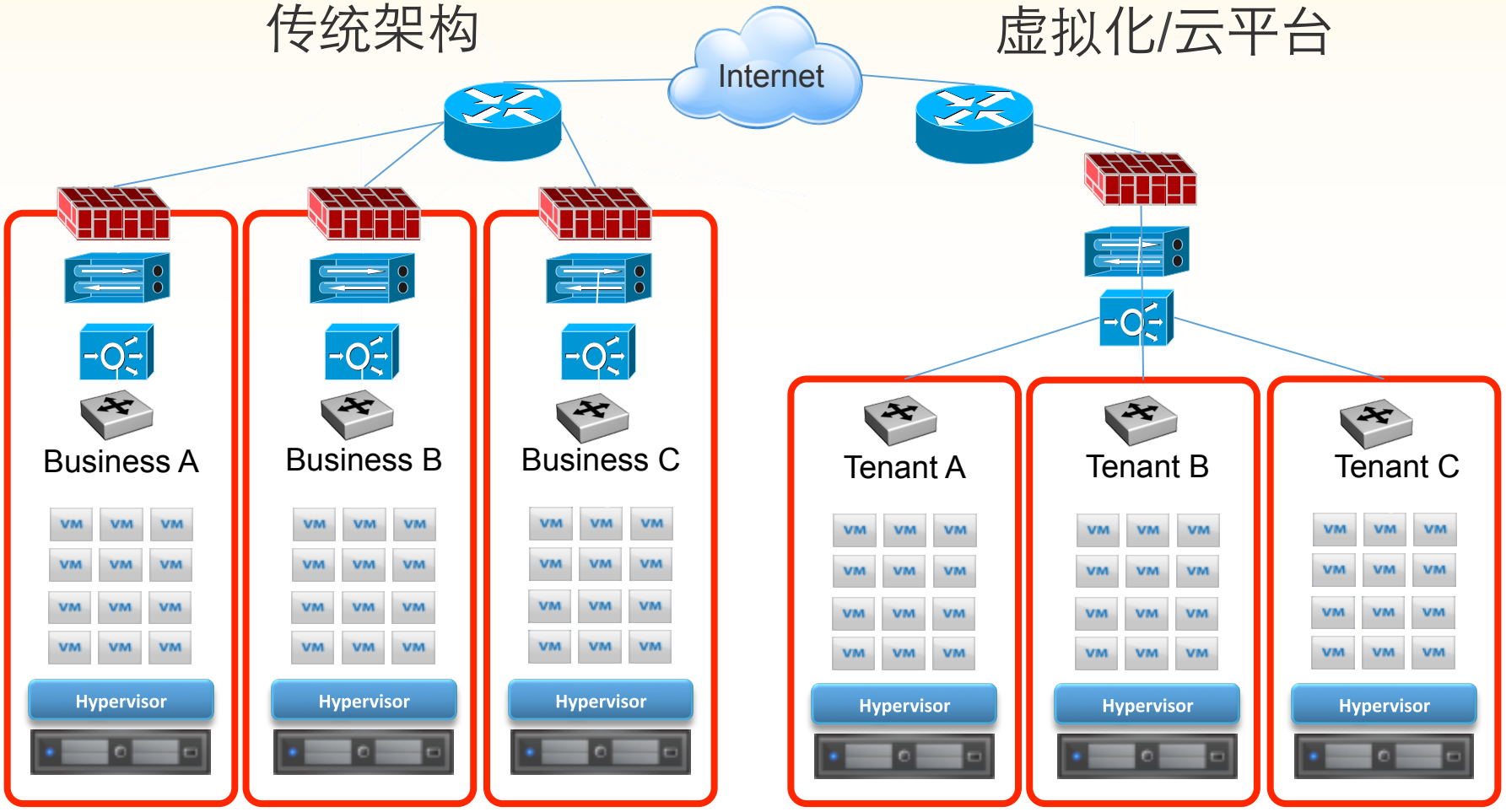
- 桌面防病毒代理,
- 基于主机的入侵检测
- 针对隐私数据的DLP代理

端点防护

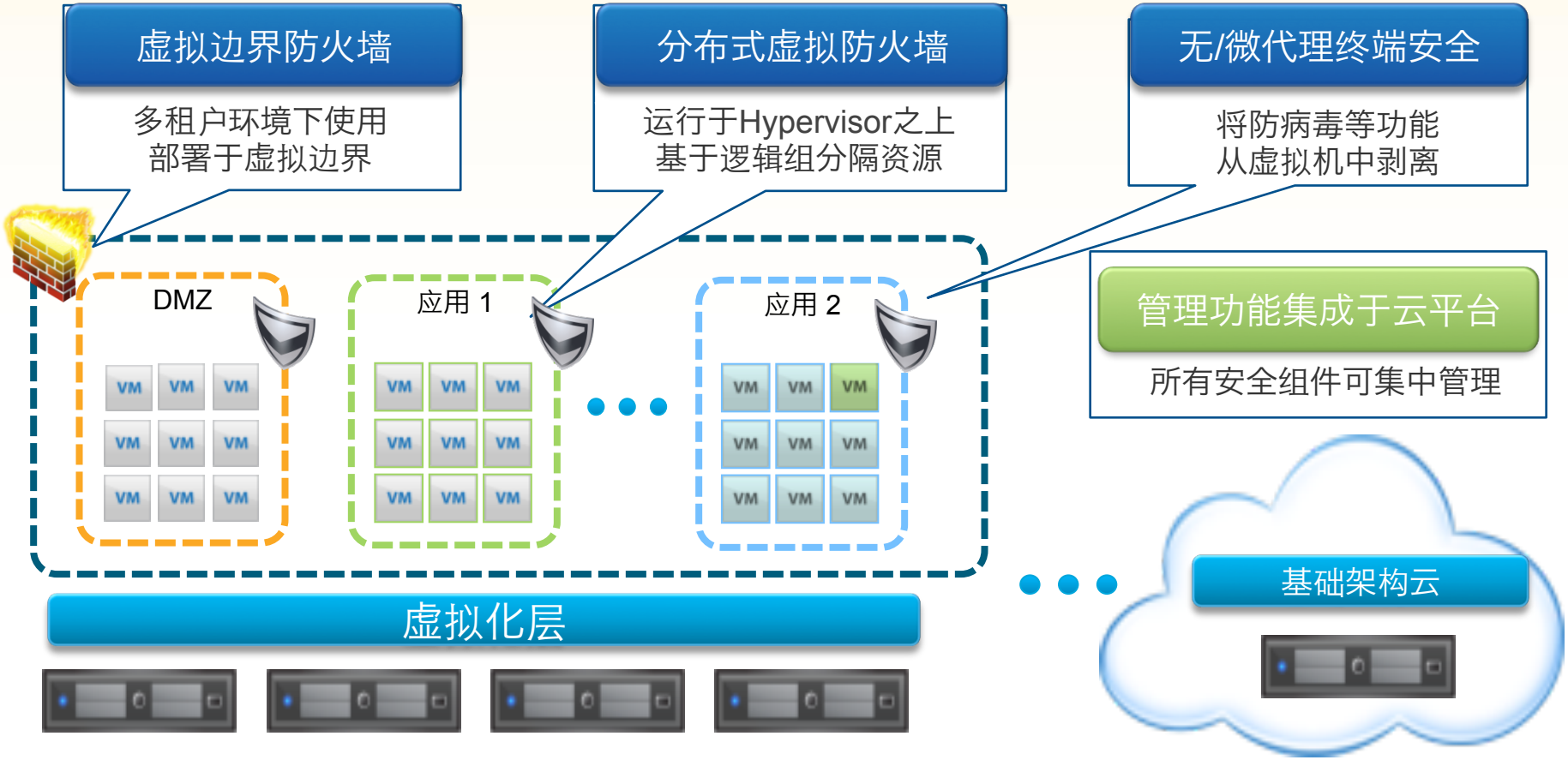
传统数据中心网络安全组件



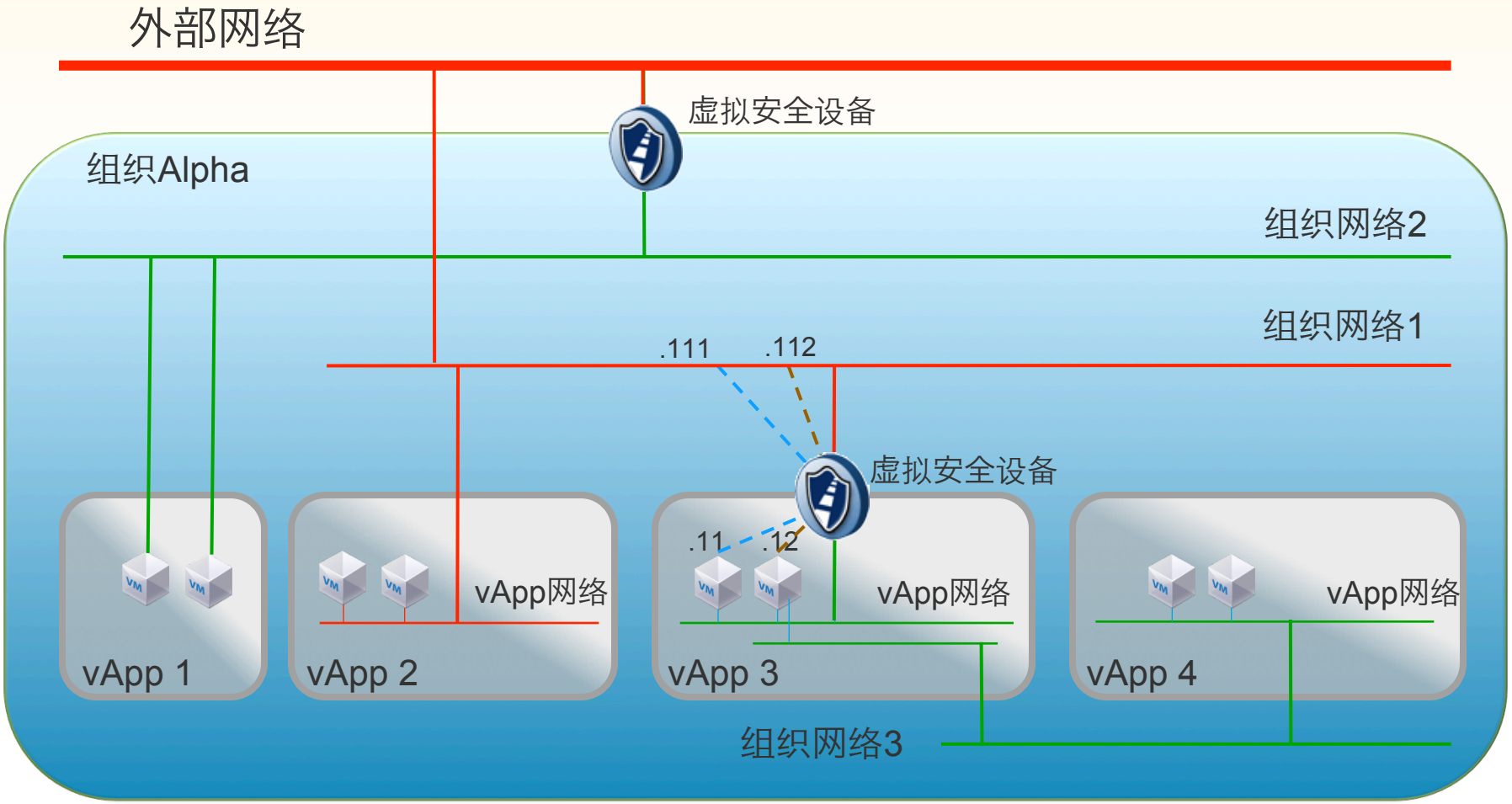
多租户环境的安全隔离


传统架构
虚拟化/云平台
Internet
Business A
Business B
Business C
Tenant A
Tenant B
Tenant C
VM
Hypervisor

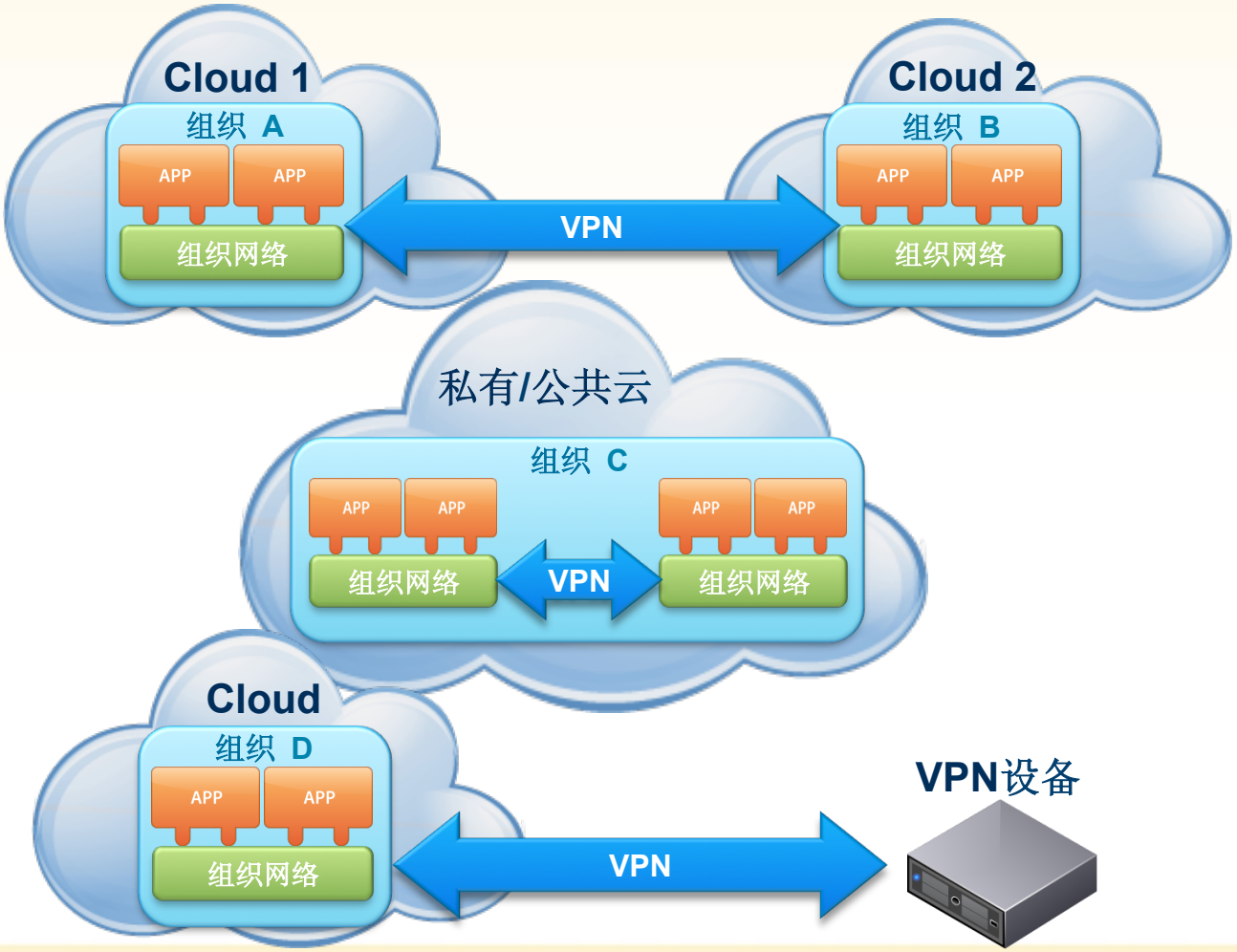
革新的防御体系


虚拟边界防火墙
多租户环境下使用
部署于虚拟边界
分布式虚拟防火墙
运行于Hypervisor之上
基于逻辑组分隔资源
无/微代理终端安全
将防病毒等功能
从虚拟机中剥离
DMZ
应用 1
应用 2
VM
管理功能集成于云平台
所有安全组件可集中管理
虚拟化层
基础架构云

多租户环境下的安全设备管理



S2S VPN网关构建可信通道

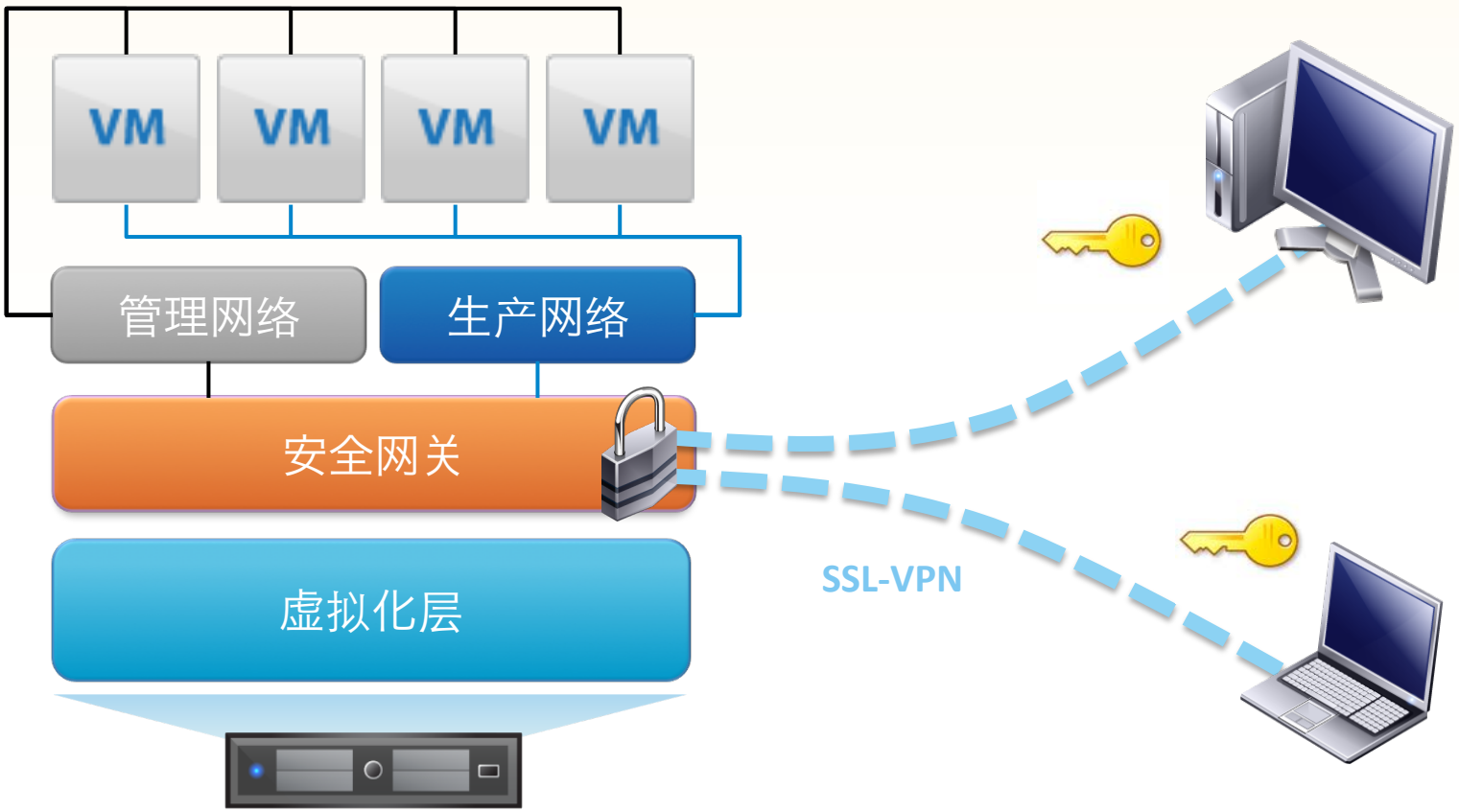


连接另一组织网络的安全加密链路

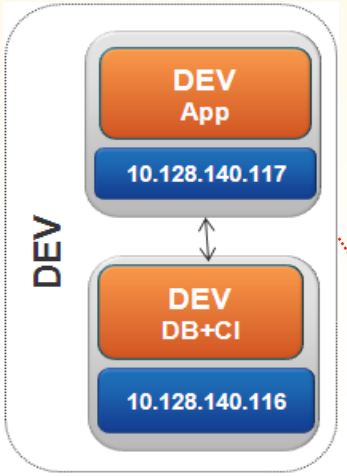
连接本组织网络的安全加密链路

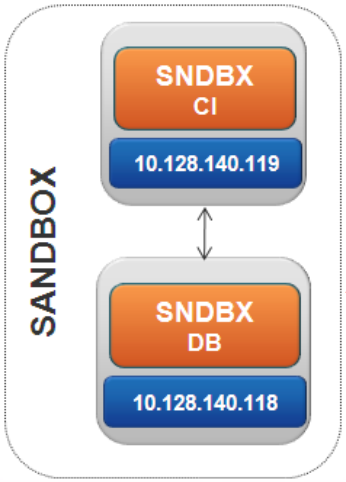
连接远程网络的安全加密链路

SSL-VPN提供管理通道

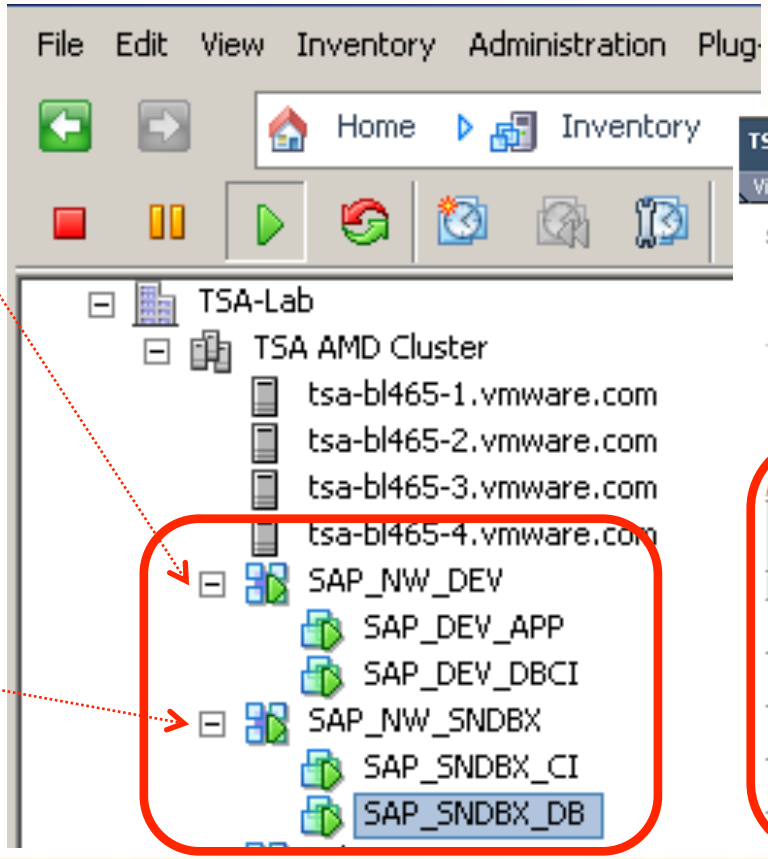


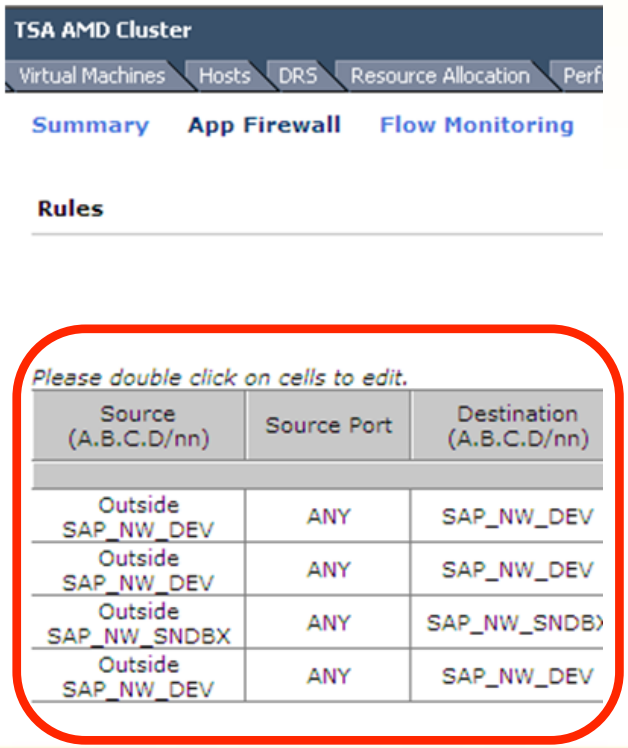
基于逻辑组的访问控制



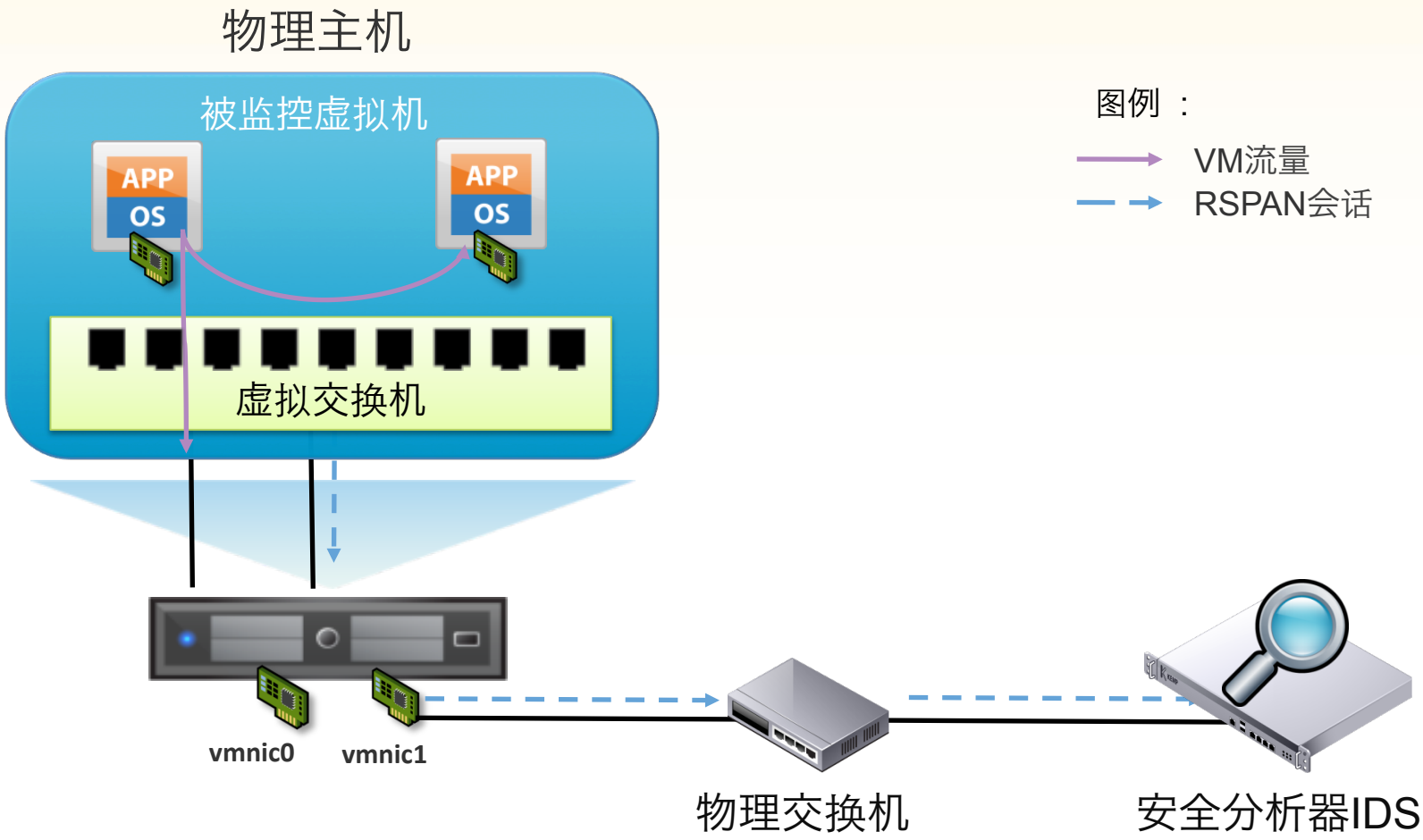


vApp：
一个或多个虚拟机的逻辑实体

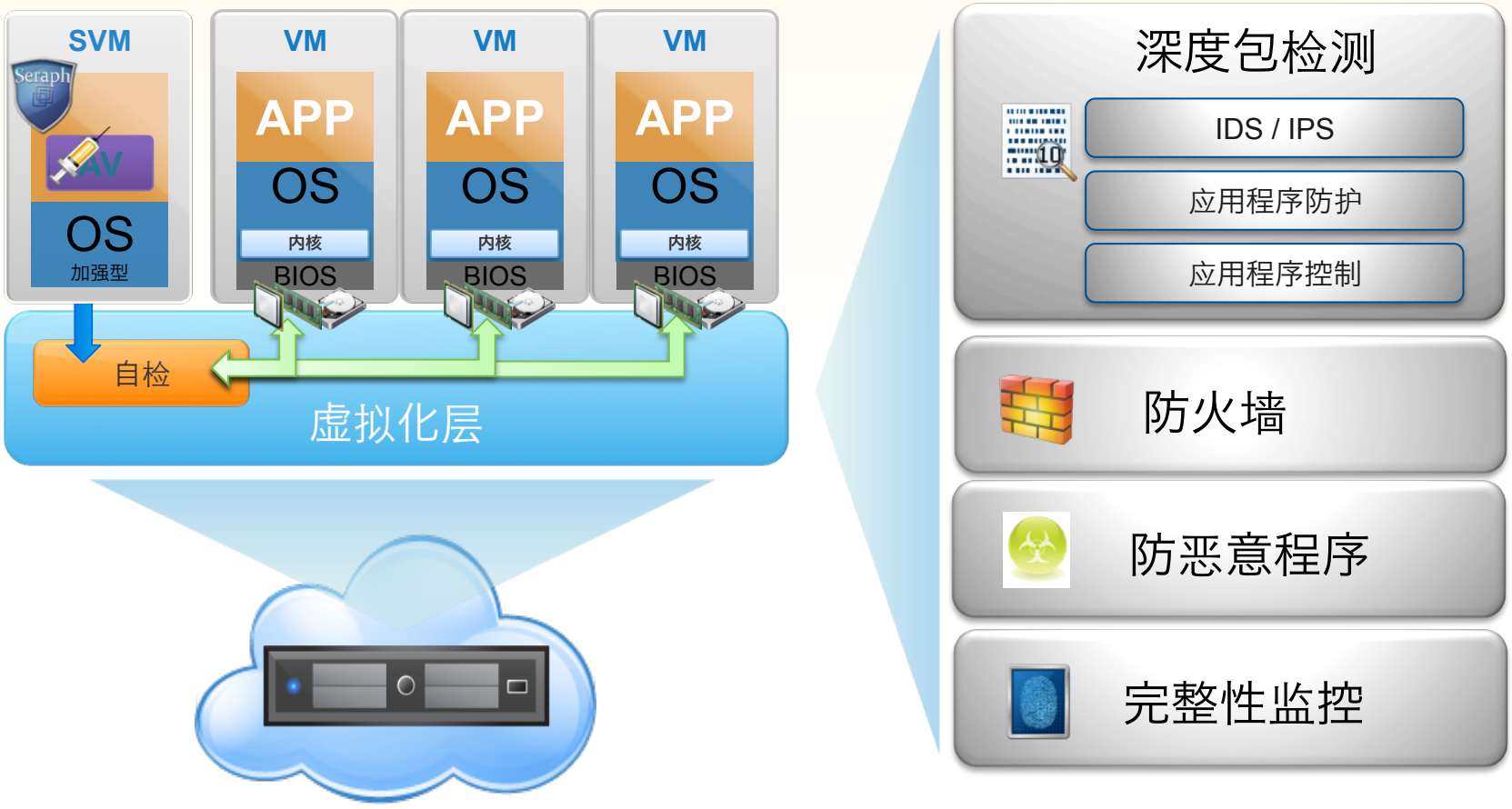




流量集中监控审计


物理主机
被监控虚拟机
APP
OS
APP
OS
虚拟交换机
图例 ：
VM流量
RSPAN会话
vmnic0
vmnic1
物理交换机
安全分析器IDS

无/微代理终端安全


SVM
Seraph
AV
OS
加强型
VM
APP
OS
内核
BIOS
VM
APP
OS
内核
BIOS
VM
APP
OS
内核
BIOS
自检
虚拟化层
深度包检测
IDS / IPS
应用程序防护
应用程序控制
防火墙
防恶意程序
完整性监控

硬件 vs. 软件

传统基于硬件安全解决方案		基于云的软件解决方案
昂贵 ▪ 需采用专用的硬件设备 ▪ 需采用多套解决方案		经济 ▪ 一个虚拟设备提供全部功能 ▪ 全部保护功能通过单一框架实现
复杂 ▪ 多个管理界面 ▪ 大量的安全策略 ▪ 安全角色存在交叉		简单 ▪ 极少的规则，VLAN与代理 ▪ 虚拟化、网络与安全团队统一界面 ▪ 简化了遵从性管理
死板 ▪ 策略与硬件绑定 ▪ 对虚拟化和配置改变没有感知		灵活 ▪ 策略随虚拟机一起迁移 ▪ 可感知虚拟化与配置改变

云安全是一个生态系统


云管理
性能监控
容量规划
配置管理
数据保护
灾难恢复
云架构
自助式门户和目录
请求实现 过程工作流
安全的多租户
虚拟数据中心的创建与管理
软件定义的存储
软件定义的网络
软件定义的安全性
软件定义的可用性
虚拟化
负载平衡和自动置备
资源抽象化和池化
物理基础架构
（服务器、存储、网络）


BROCADE
SOPHOS
WWW.SOPHOS.COM
BROADCOM
catbird
ARISTA
loglogic
intel
TREND MICRO
KASPERSKY
ANTI VIRUS
Bitdefender
RSA
McAfee
ca
RAPID7
EMULEX
We network storage
CISCO
JUNIPER NETWORKS
Check Point
SOFTWARE TECHNOLOGIES LTD.
Lumension SECURITY
symantec.
SOURCEfire
hp

谢谢

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012