

**RSA[®]CONFERENCE
C H I N A 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**



云数据中心的网络安全

王钟
Hillstone Networks

Session ID:

Session Classification: 云安全



RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012

议题

1

动态变化中的数据中心

2

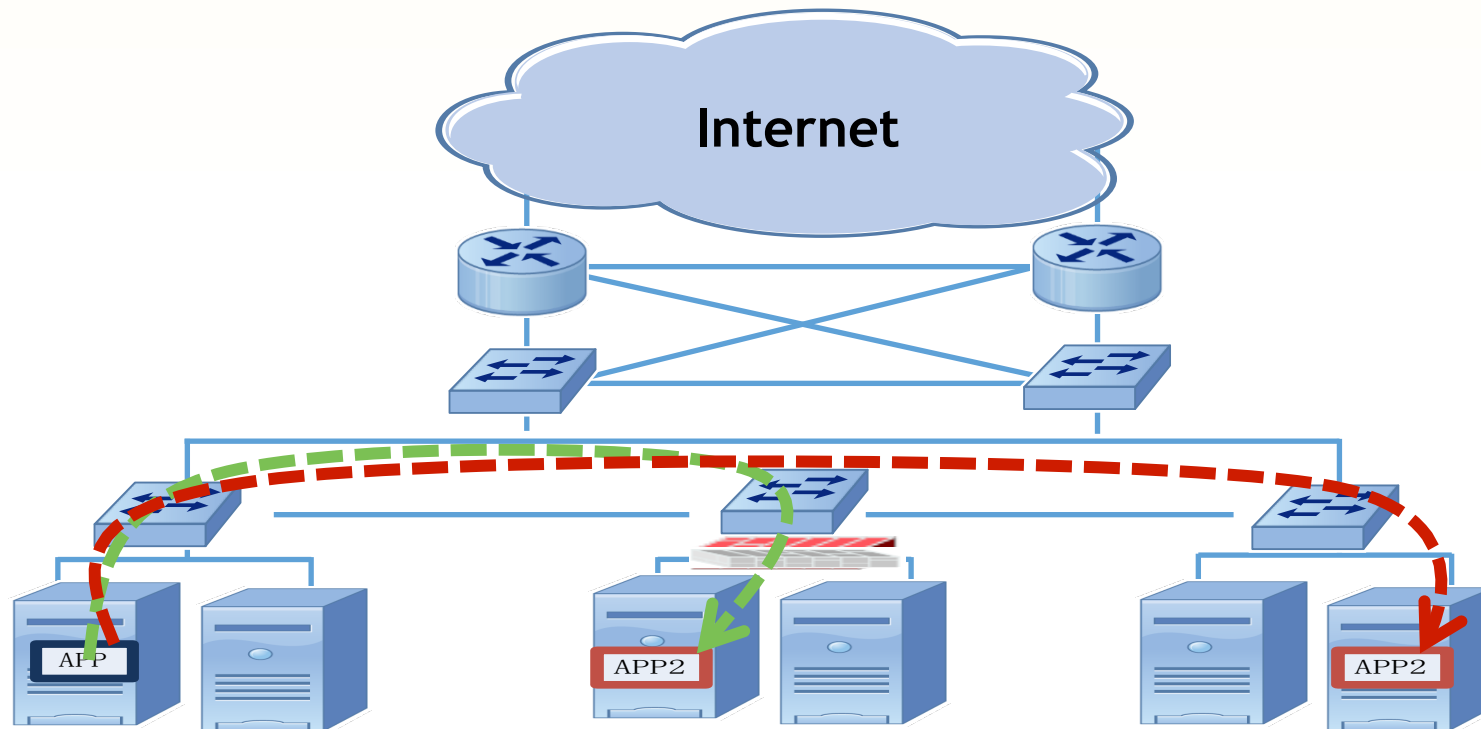
当前数据中心面临的安全挑战

3

数据中心网络安全解决方案

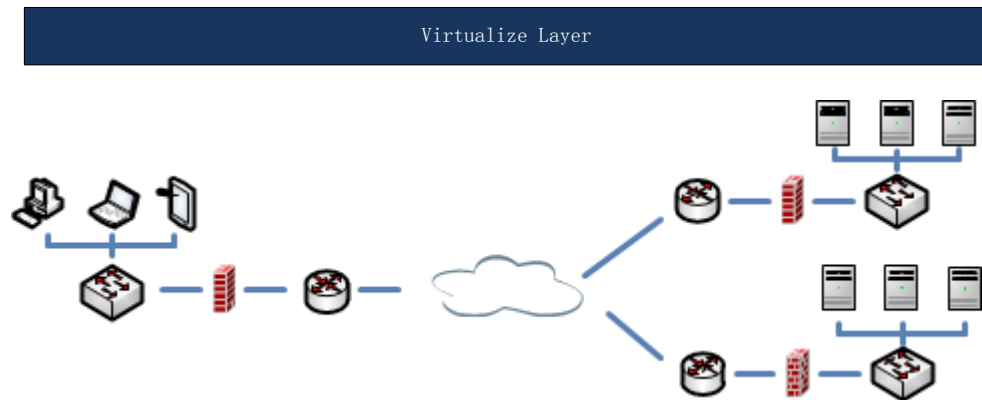
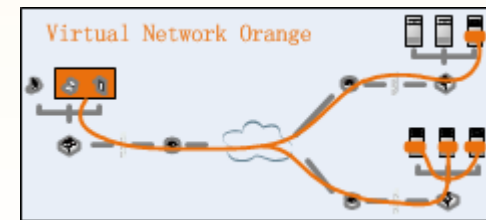
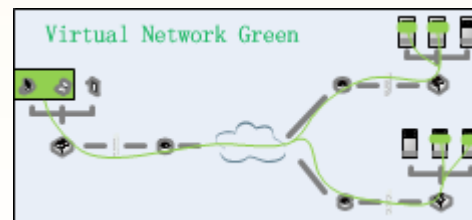
服务器虚拟化

- 服务器虚拟化在数据中心的广泛采用所带来的安全问题亟待解决。
- 多数的识别和安全控制措施基于固定位置、静态网络或固定IP，难以应付虚拟机迁移带来的安全问题。
- 虚拟化环境的动态特性意味着新的安全威胁和漏洞。



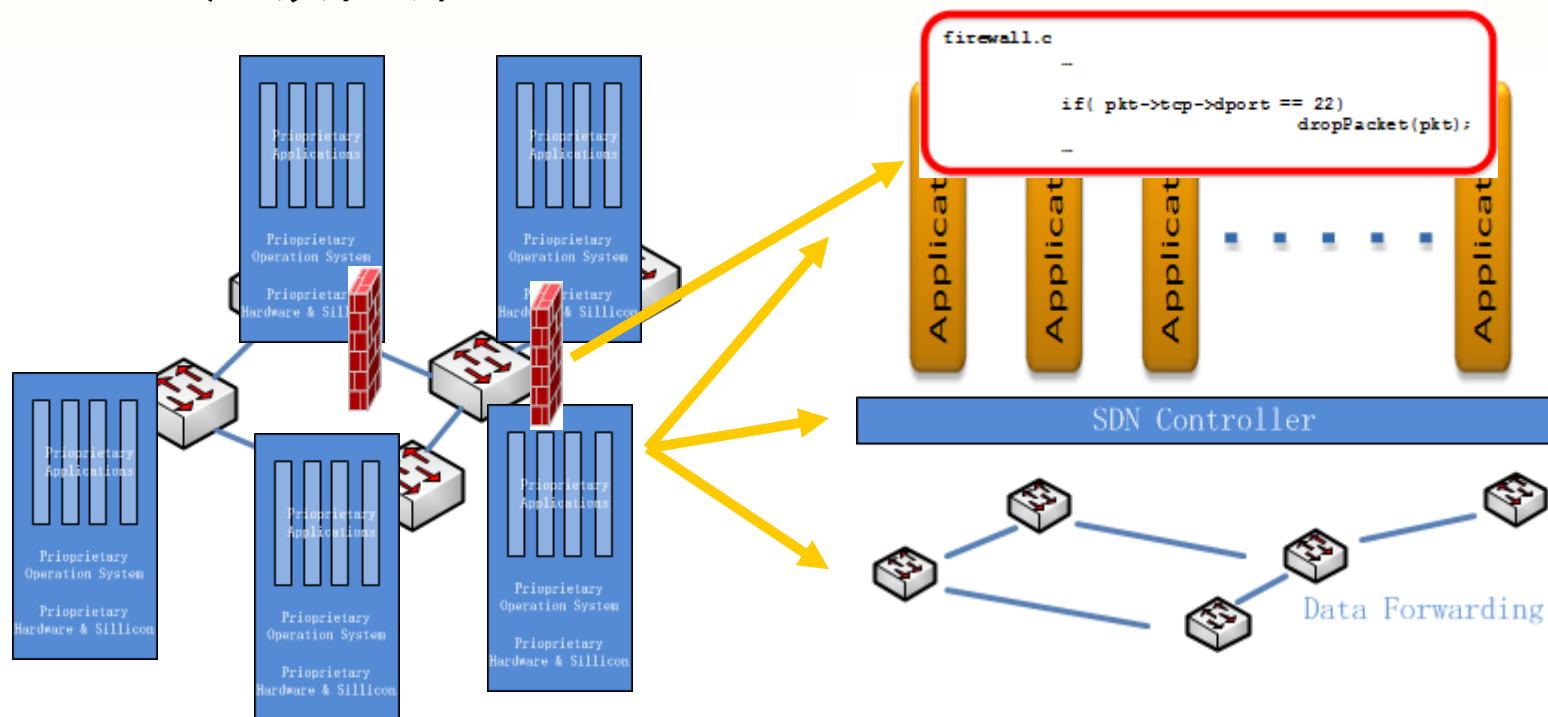
网络虚拟化

- 网络虚拟化将网络服务和物理网络设备分离。
- 网络部署方式的改变：从设备的手工单独配置方式变为可编程的自动部署；同时网络也可以按需而动。
- 基于固定物理网络设备环境的安全技术面临着动态变化的网络虚拟化的挑战。

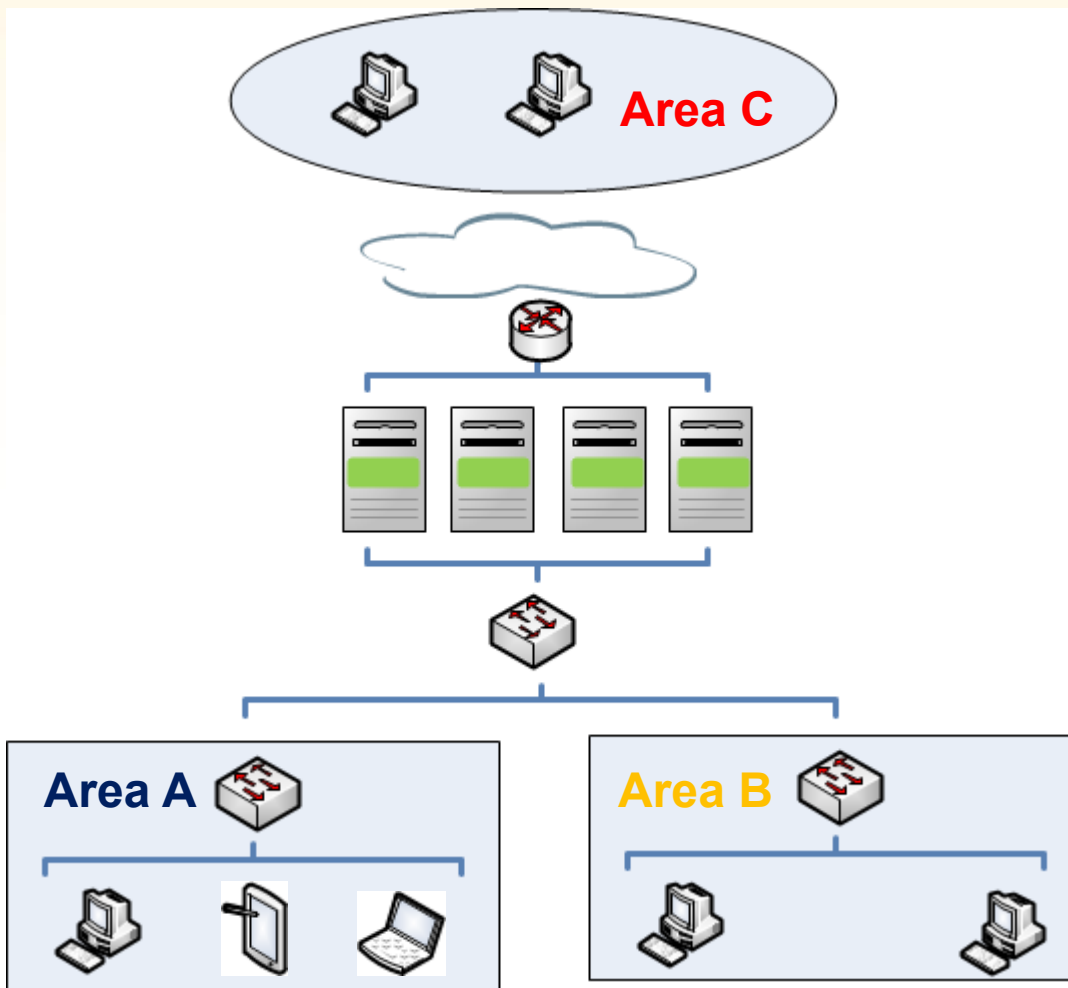


SDN - 软件定义网络

- SDN将网络控制平面和网络的物理拓扑分开。
- 当网络变为可编程实现的时候，网络安全应该怎么做？
- 当网络的控制和管理被虚拟化、集中化后，安全的管理应该在哪里？



BYOD



- 动态的IP和变动的位置
- 你在哪里？
- 你是谁？

议题

1

动态变化中的数据中心

2

当前数据中心面临的安全挑战

3

数据中心网路安全解决方案

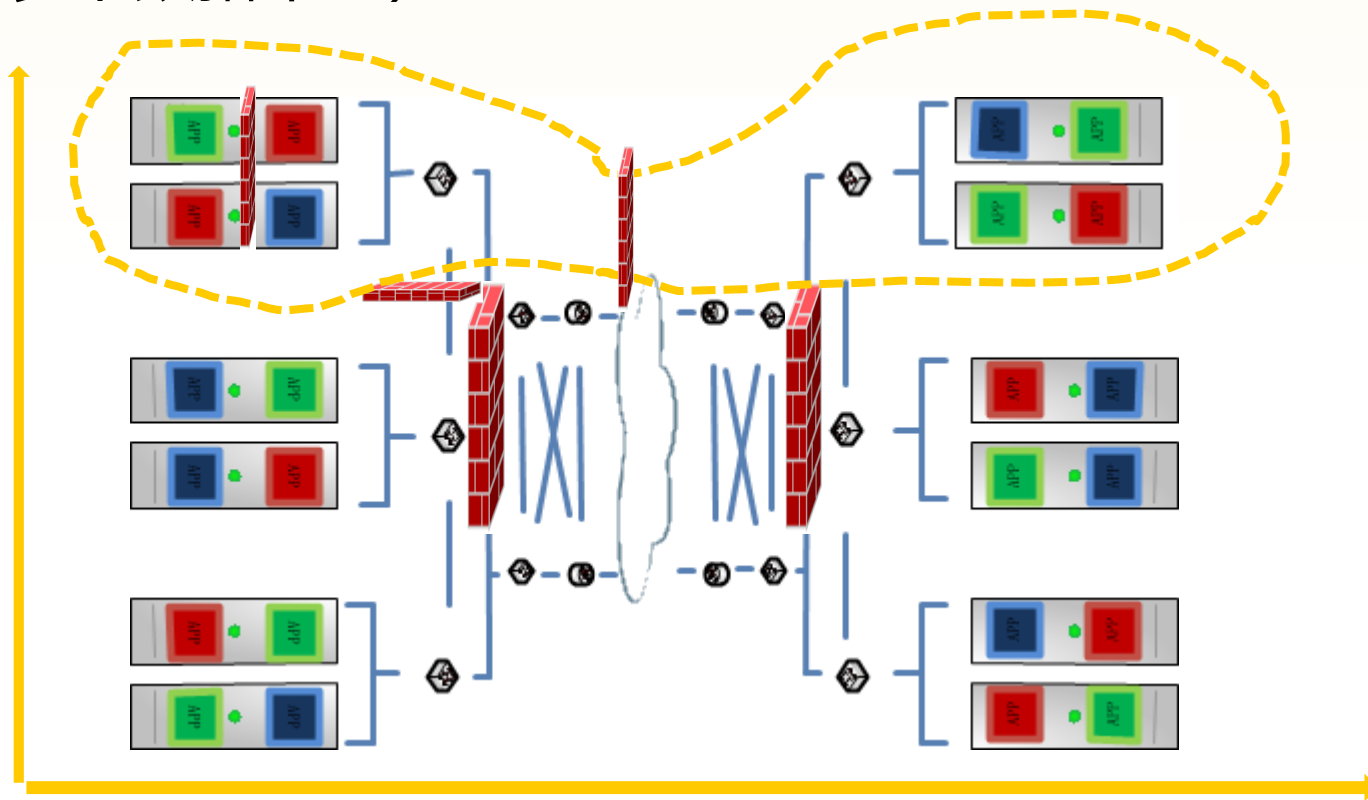
2012 Gartner分析的IT问题排名

- Poor threat and vulnerability management/targeted attack prevention
- Consumerization of IT
- Cloud security
- Legal and regulatory compliance
- Lack of effective, mature governance/standards for IT systems and infrastructure
- Not having a flexible organizational structure to support new drivers, constraints
- Vendor risk management — third-party connections, service providers, supply chain
- Poor understanding of which data and systems are business-critical
- Poor project management
- Lack of skilled workforce
- Poor reporting and lack of metrics to demonstrate value
- Lack of proper security "culture"
- Lack of mature BCM/DR program
- Lack of mature identity and access management program
- Lack of mature backup/recovery management

Gartner.

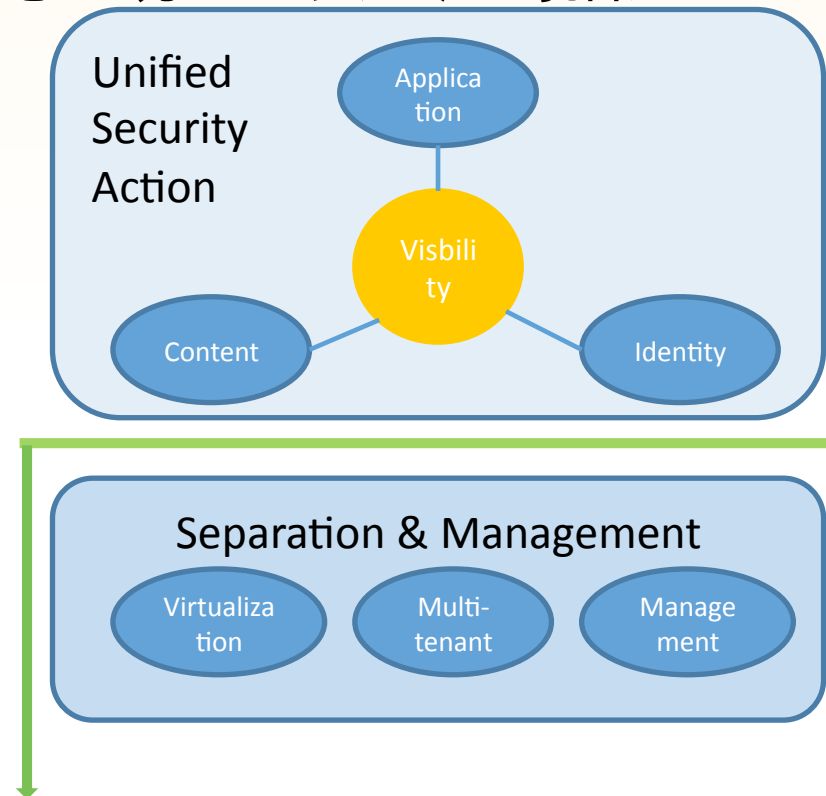
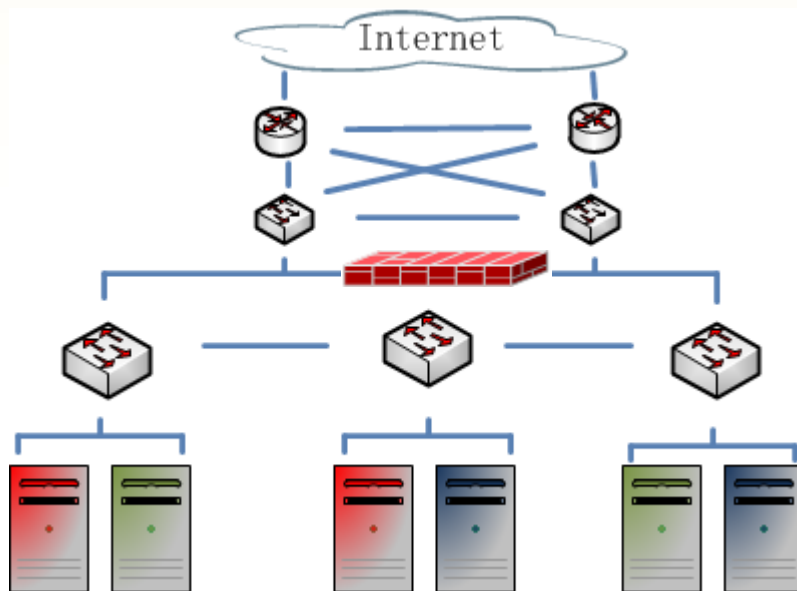
两个维度上的网络安全

- 维度1：传统的数据中心边界
- 维度2：数据中心内部（一个数据中心内部和跨越不同地域的多个数据中心）



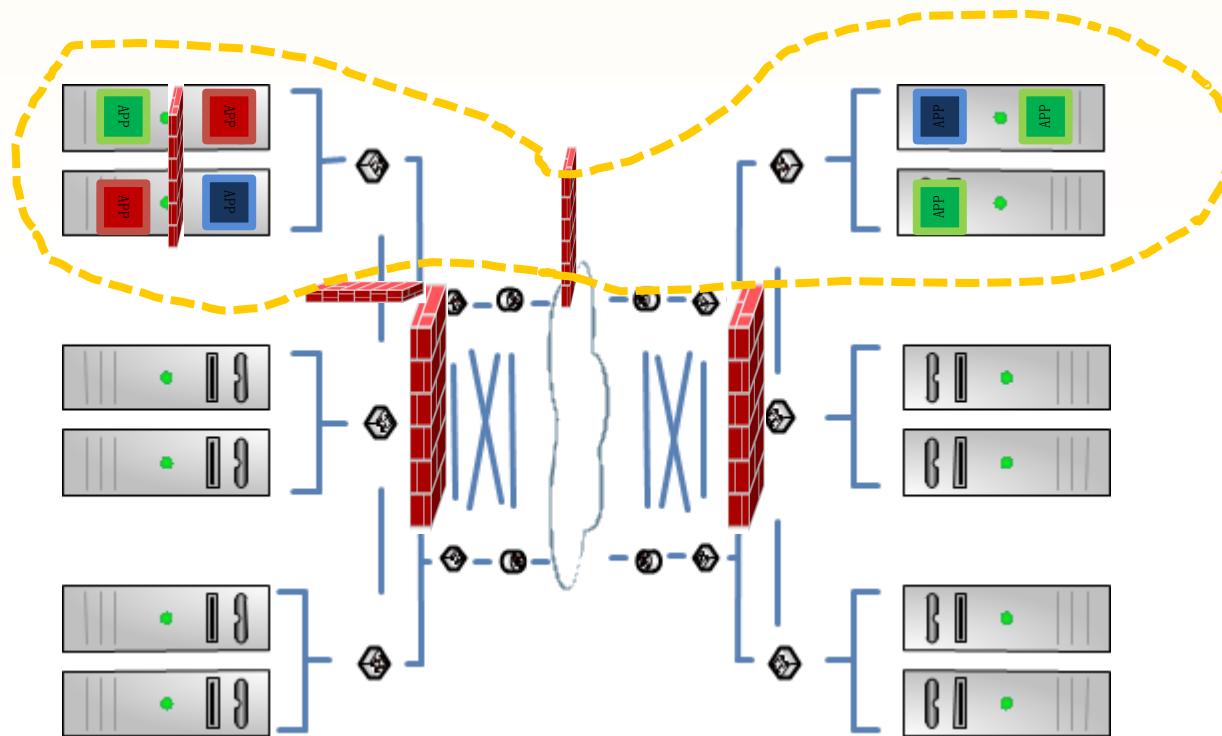
另一个视角

- 虚拟化数据中心多租户环境的管理和隔离
- 对内容、应用、身份提供可见且统一的安全应对措施



虚拟化带来新挑战

- 网络的边界在哪里？
- 被保护的對象在哪里？



议题

1

动态变化中的数据中心

2

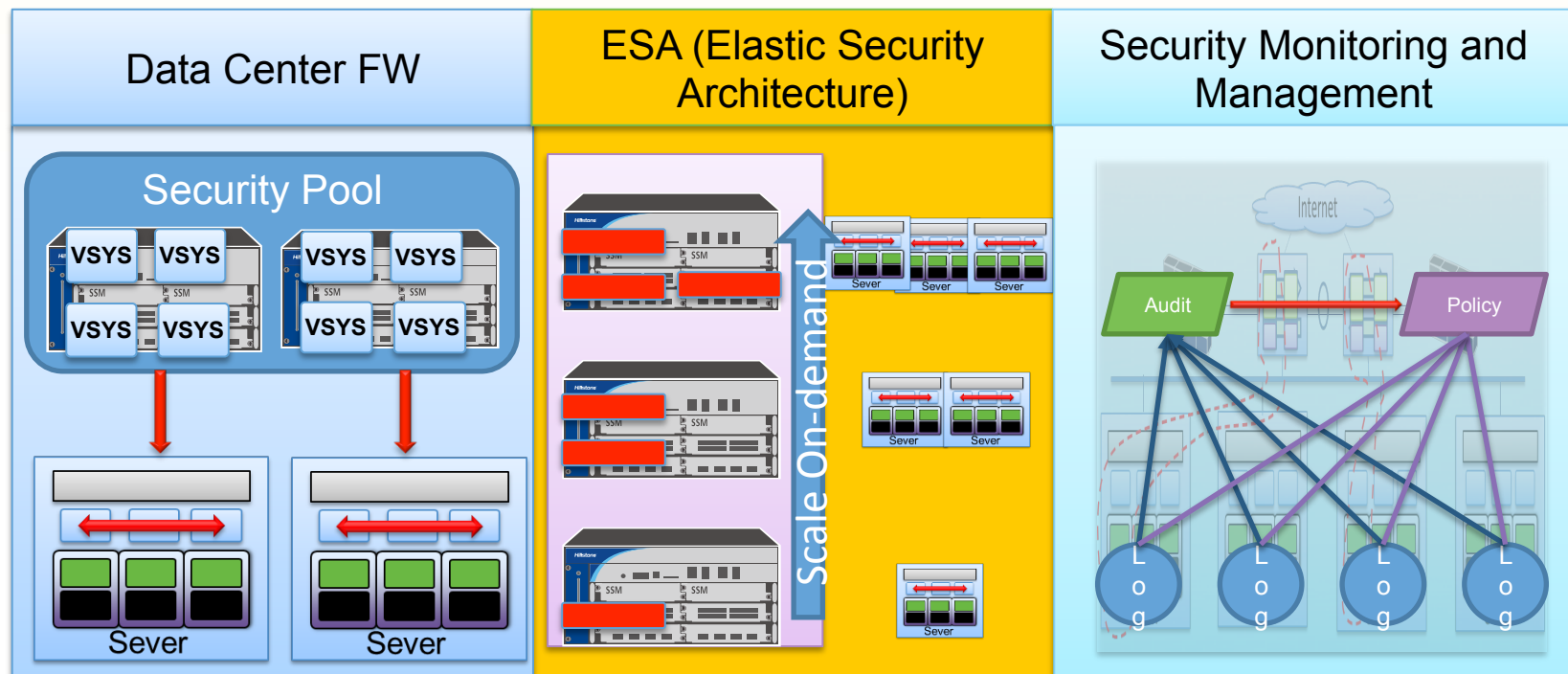
当前数据中心面临的安全挑战

3

数据中心网络安全解决方案

不仅是一个设备

- 基础架构层面的网络安全
- 数据中心防火墙+ 弹性安全架构+ 安全监控和管理

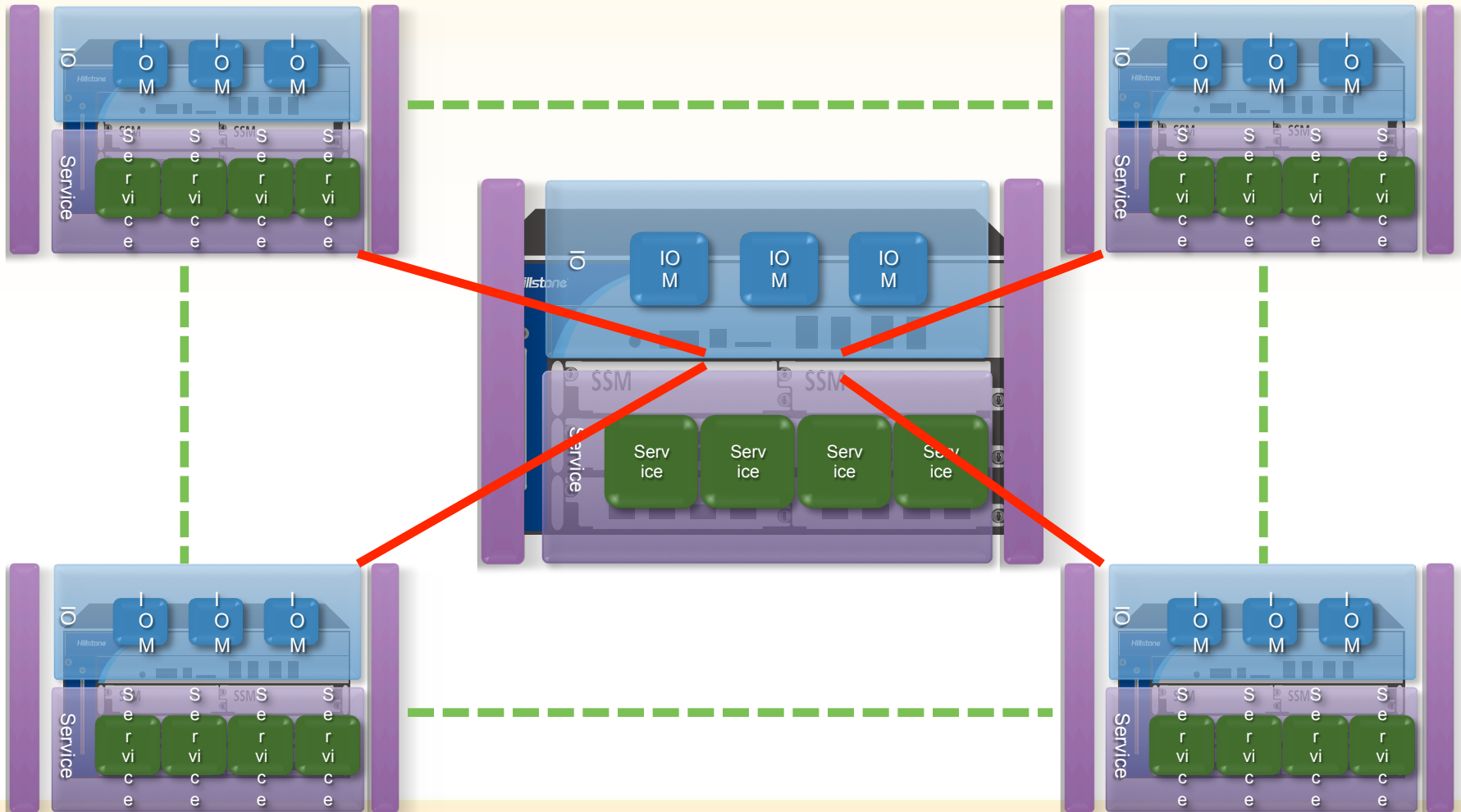


数据中心防火墙的关键特性

- 安全即服务 Security as a Service
- 安全即资源 Security as a Resource
- 开放可定义 Open and Definable
- 冗余高可靠 Redundant
- 分布可扩展 Distributed scalable
- 绿色节能 Green

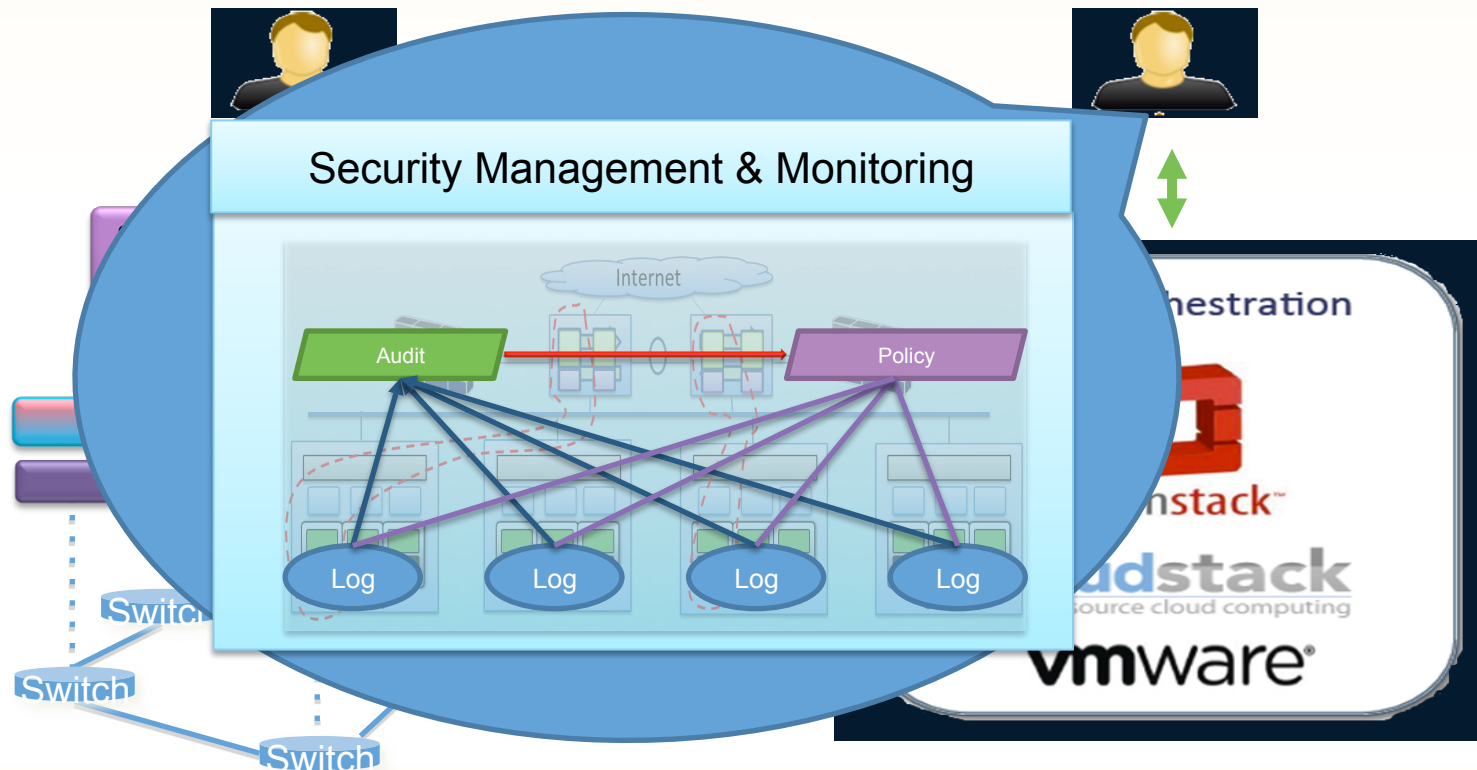
弹性安全架构(Elastic Security Architecture)

RSA CONFERENCE
C H I N A 2012



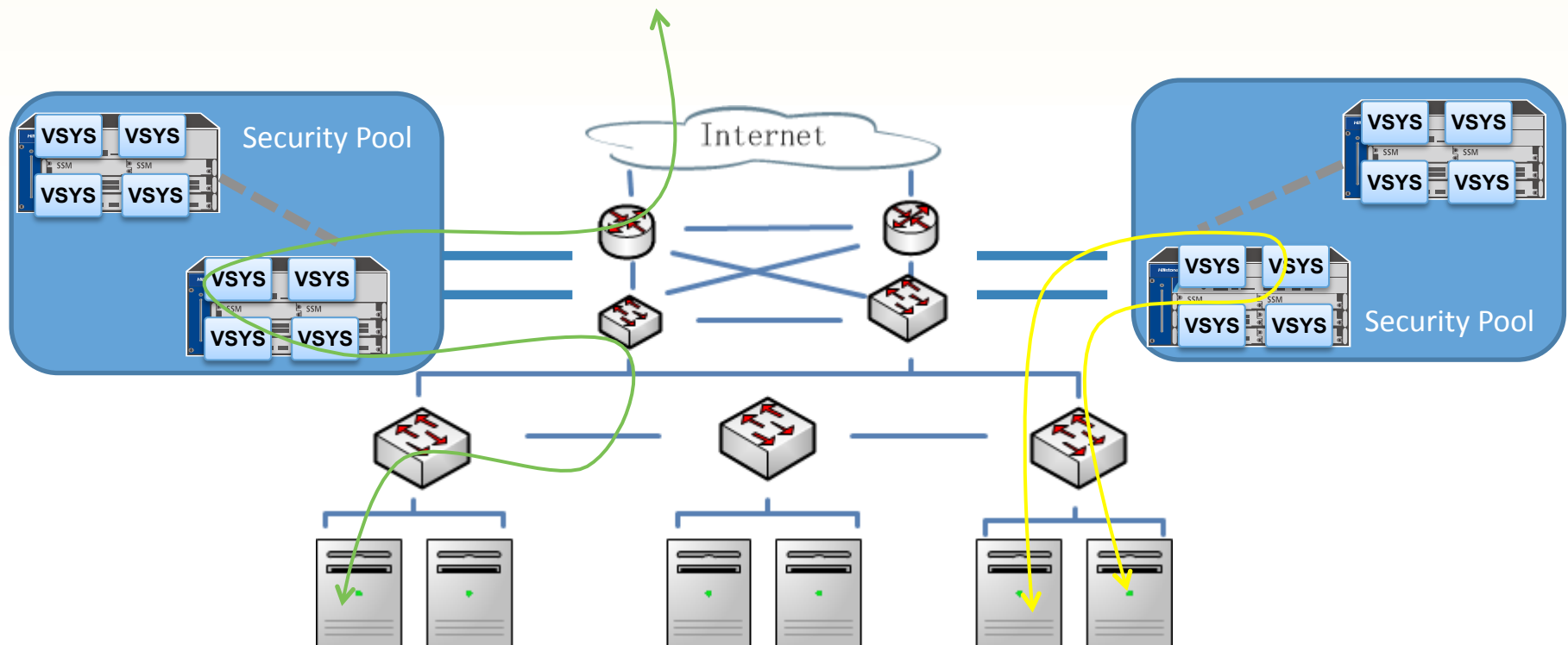
安全监控和管理

- 分布环境中，集中管理是安全的关键。
- 对付随机的、具有欺骗性的安全威胁，全局的相关可见性是关键。

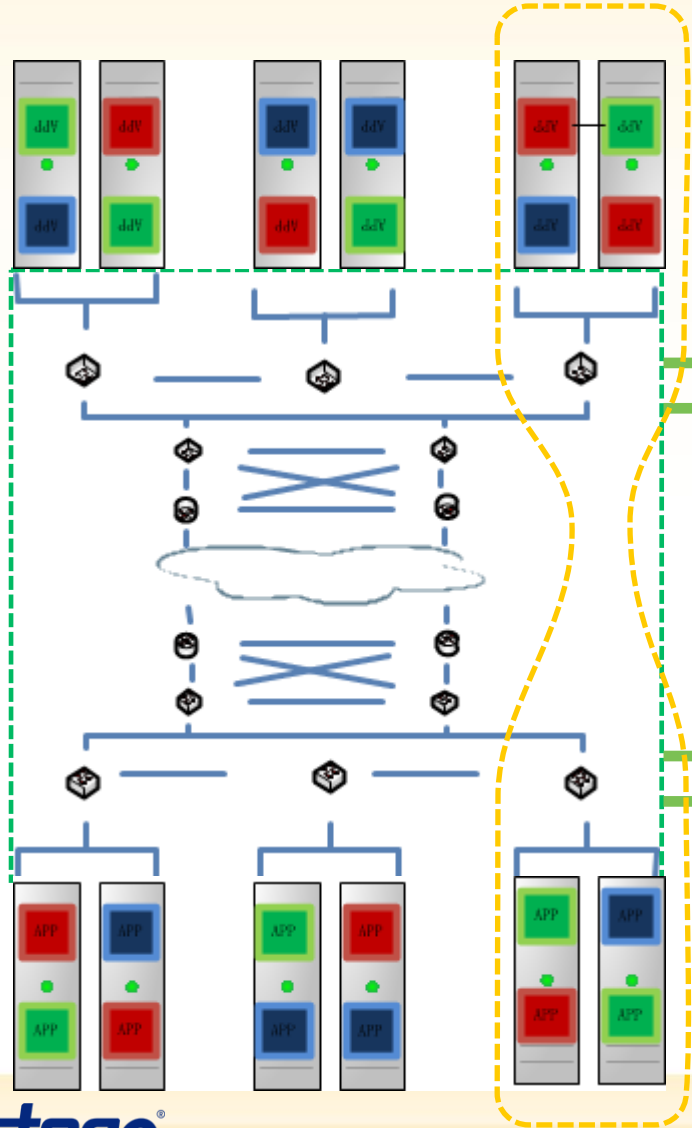


安全数据中心部署方案

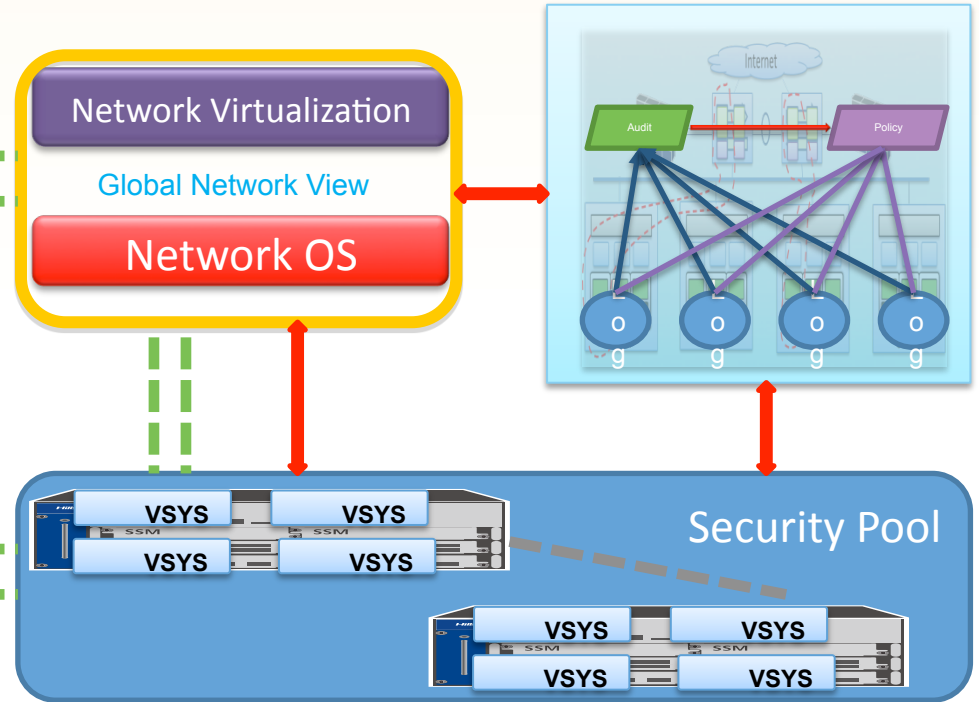
- 数据中心边界的安全池部署



安全数据中心部署方案



虚拟化数据中心内部的安全资源池部署



Thank You



RSA CONFERENCE
C H I N A 2012
RSA信息安全大会2012