大型企业私有云的安全规划探索分享

吕鹏啸

北京江南天安科技有限公司

RSA CONFERENCE CHINA 2012

标题

- 企业云安全的出发点
  - 哪些应用适合云计算
  - 企业云安全的业务目标是什么
  - 企业云安全的技术目标是什么
  - 合规
- 云安全建设的开始和重要点
- 云数据中心的安全建设
  - 纵深防御.
  - 虚拟化的新增威胁
  - 阿喀琉斯之踵:门卫守则
  - 云环境下的加密技术

业务先行还是安全先行？

@思科那些事：【思科致歉隐私"混乱"云连接降为可选项】【CNW.com.cn独家译稿】在收到大量客户关于自动固件升级和服务条款的的投诉后，思科公司做出了让步，将其Connect Cloudservice(云连接服务)从Lin...http://t.cn/zWcCmSj

今天 12:22 来自定时8 转发(5) | 评论

云计算是否适合大型企业

- 云计算对企业带来的价值是什么
- 业务角度
  - 业务的重要性
- 技术角度
- 成本角度

云安全的业务目标是什么

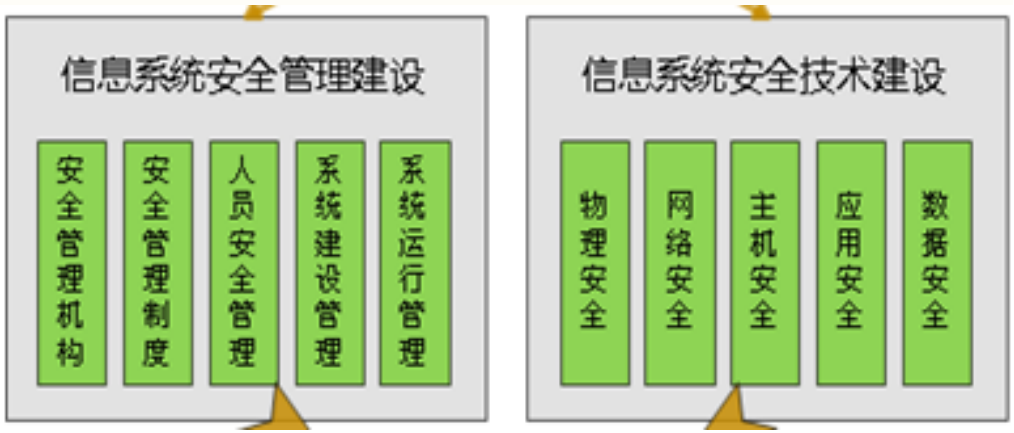
- 保障应用的可靠运行
- 数据的防护
- 高效安全协作

云安全的技术目标是什么

- 集成化 （例如： 2001:0DB8:0000:AB2C:DD98:BB02:1428:0036 ）
- 虚拟化
- 自动化
- 弹性化

合规

- CSA
- 等级保护

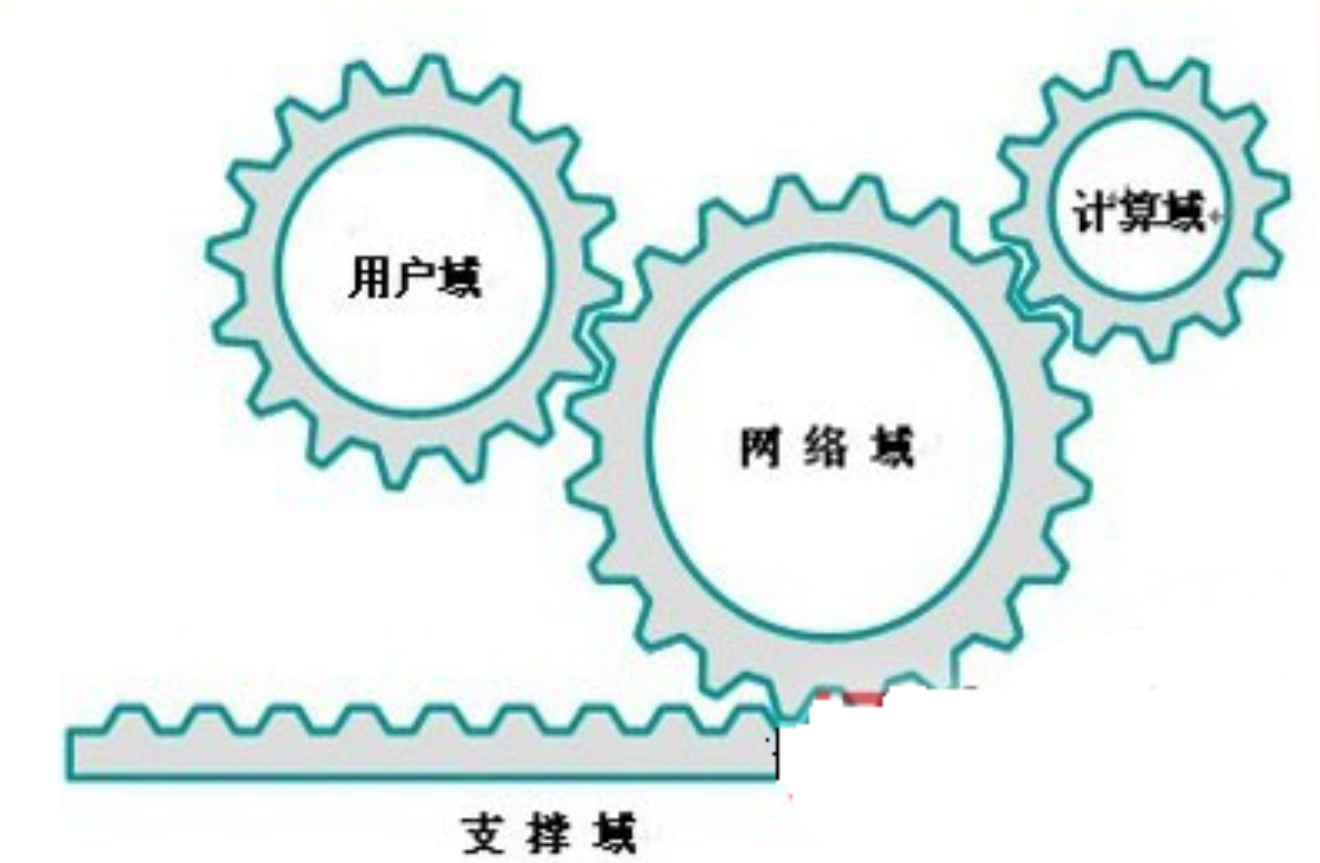

信息系统安全管理建设
安全管理机构
安全管理制度
人员安全管理
系统建设管理
系统运行管理
信息系统安全技术建设
物理安全
网络安全
主机安全
应用安全
数据安全


云的治理
安全治理、风险管理
法律和电子证据
数据生命周期管理
合规与审计
云的运行
信息泄露防护
加密和密钥管理
应用安全
边界安全与安全域
VM安全
Hypervisor安全
虚拟网络安全
身份识别和访问管理
安全事件管理与响应
业务连续性
基础设施安全管理

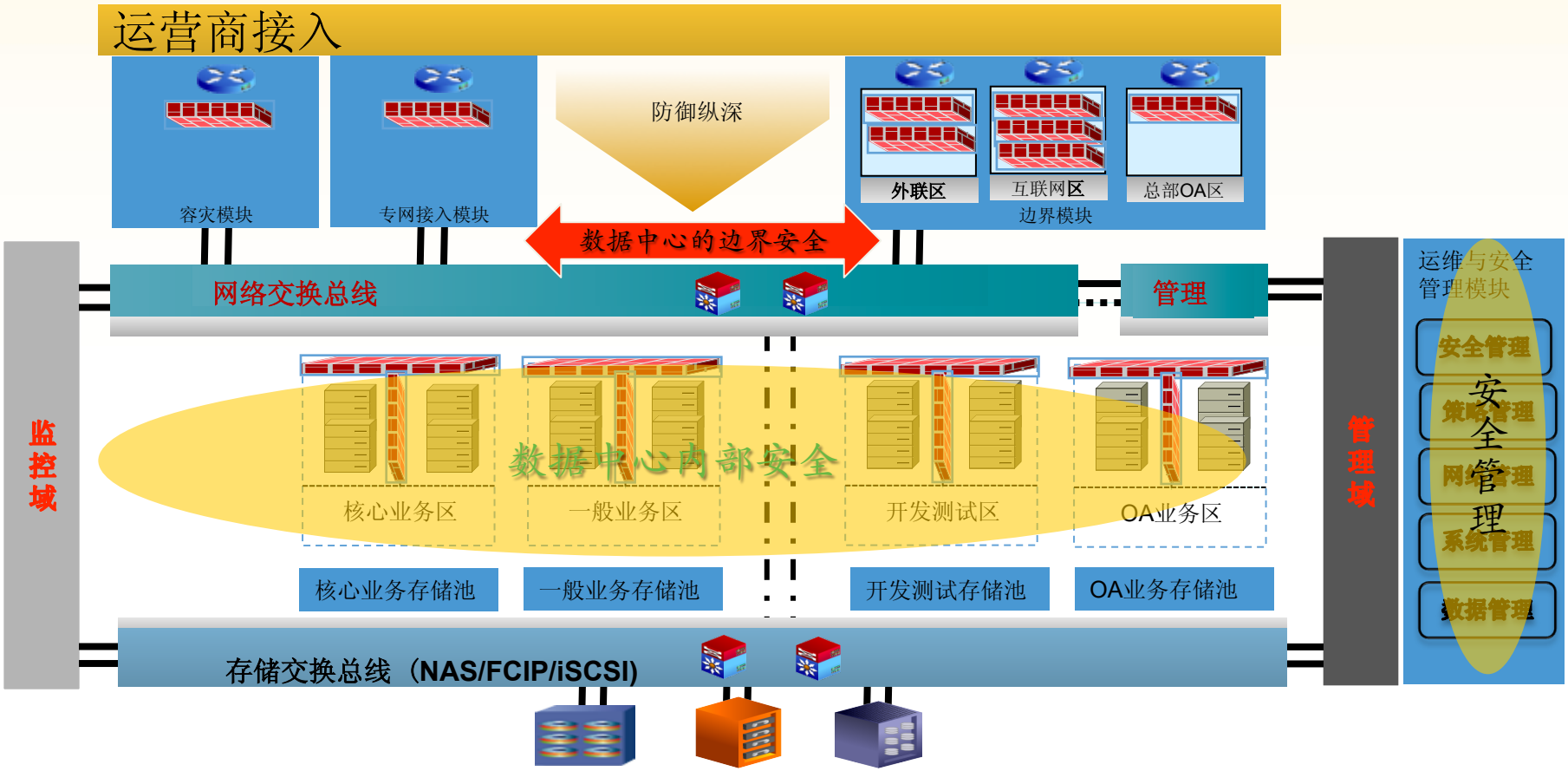
云安全建设的开始和重要点

- 数据中心安全的建设原则
  - 业务为中心，流程为驱动，风险为导向
  - 架构简单，符合规范
  - 纵深防御，水平分区

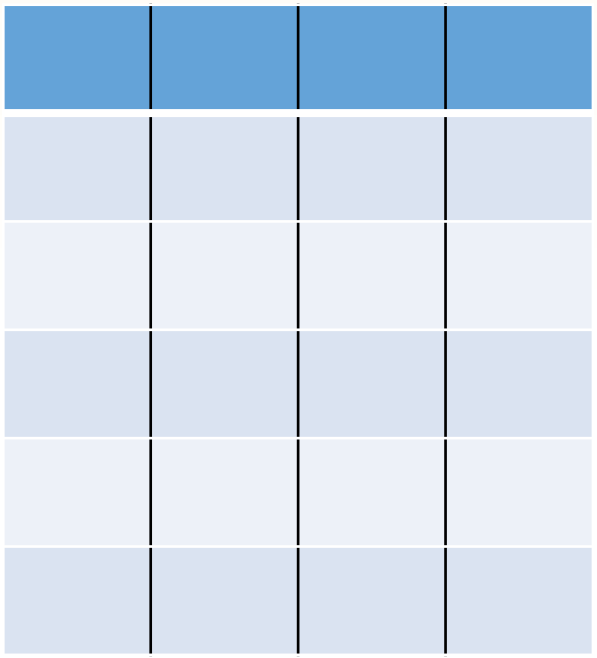
分区分域模型

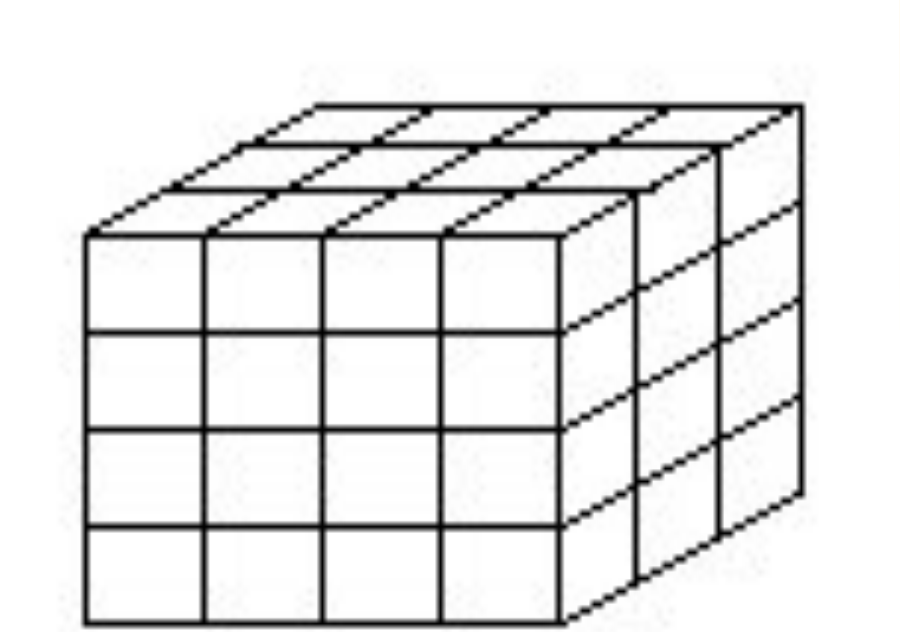


数据中心的安全域举例

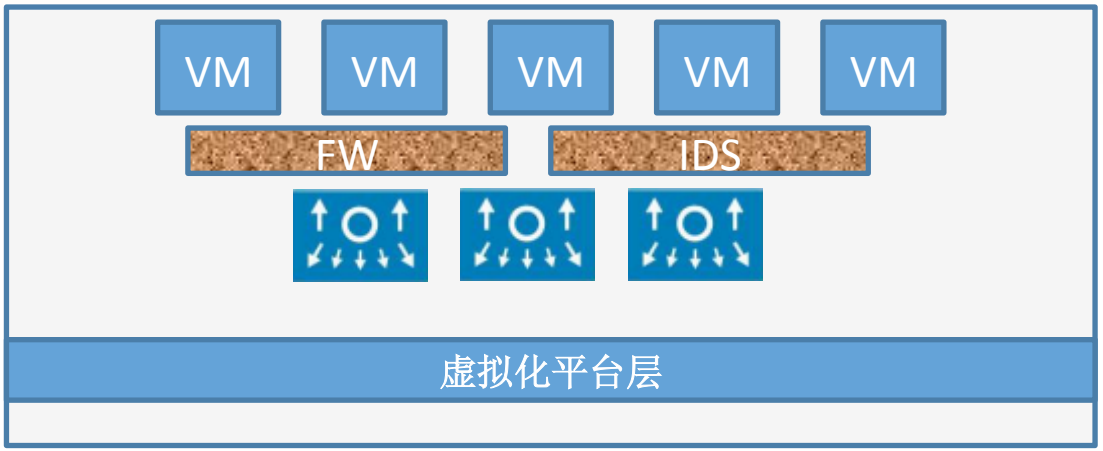

运营商接入
容灾模块
专网接入模块
防御纵深
外联区
互联网区
总部OA区
边界模块
数据中心的边界安全
网络交换总线
管理
监控域
数据中心内部安全
核心业务区
一般业务区
开发测试区
OA业务区
核心业务存储池
一般业务存储池
开发测试存储池
OA业务存储池
存储交换总线（NAS/FCIP/iSCSI）
管理域
运维与安全管理模块
安全管理
策略管理
网络管理
系统管理
数据管理
安全管理

虚拟化：应对水平攻击



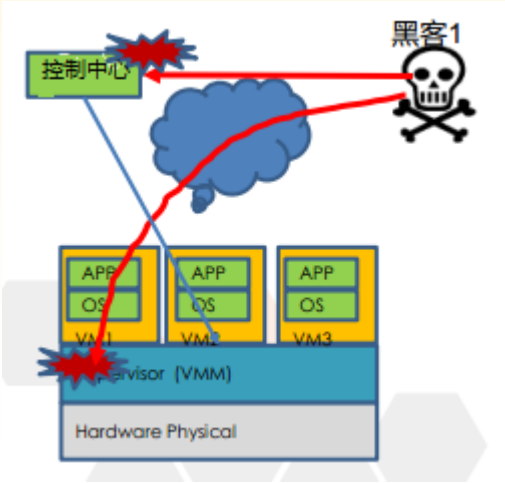


虚拟化的困扰: 边界不清晰, 管理不清晰



威胁一: 虚拟化底层的安全

- 服务器虚拟化增加的Hypervisor层的漏洞.
- 平台管理中心的漏洞.
- 硬件虚拟化技术的漏洞.



Intel CPU漏洞导致64位操作系统、虚拟化软件易受黑客攻击 - 湖北...
2012年6月17日 - Intel CPU 漏洞导致 64 位操作系统、虚拟化软件易受黑客攻击[责任编辑：Admin]拟化软件程序在 Intel 处理器上运行时，容易受到本地特权扩（来自：湖北教
www.edu-hb.com/Html/201206/17/20120617125 ... 2012-6-17 - 百度快照

Intel处理器运行64位操作系统易受本地提权攻击--中国计算机安全--...
一些64位操作系统和虚拟化软件程序在Intel处理器上运行时，容易受到本地特权扩大攻击（ local privilege escalation）。该漏洞可能被利用来获取本地特权扩大或是guest-...
www.infosec.org.cn/news/news_view.php?new ... 2012-6-20 - 百度快照

CPU漏洞导致64位操作系统易受黑客攻击 虚拟化子站 IT专家网
一些64位操作系统和虚拟化软件程序在Intel处理器上运行时，容易受到本地特权扩大... 专家表示，用大数据技术分析过去威胁... CPU漏洞导致64位操作系统易受黑客攻击 美国
virtualization.ctocio.com.cn/255/12359755 ... 2012-6-16 - 百度快照

CPU漏洞导致64位操作系统、虚拟化易受黑客攻击 安全子站 IT专家网
2012年6月19日 - 一些64位操作系统和虚拟化软件程序在Intel处理器上运行时，容易受到本地特权扩大攻击(local privilege escalation)。该漏洞可能被利用来获取本地特权扩大...
security.ctocio.com.cn/486/12360486.shtml 2012-6-19 - 百度快照

VMware紧急公布hypervisor程序重大漏洞
2009年5月12日 - 核心提示： VMware昨天宣布其最新的hypervisor升级程序中存在一个重大漏洞，使得用户无法启动虚拟机，而这些虚拟机在数据中心的虚拟环境中运行着业务应用...
www.abc188.com/info/html/xingyezixun/yeji ... 2009-5-12 - 百度快照

Microsoft Virtual PC Hypervisor虚拟机监视安全绕过漏洞 - 启明...
2010年3月18日 - Virtual PC hypervisor存在漏洞可使这种假设无效，使DEP、SafeSEH、ASLR等反漏洞利用机制无效。Virtual PC使用的VMM没有实现正确的内存管理，允许运行...
www.venustech.com.cn/NewsInfo/124/6883.Html 2010-3-18 - 百度快照

Linux Kernel Xen Hypervisor实现拒绝服务漏洞,电脑病毒,杀毒软件...
当运行的系统支持无EPT的Intel CPU时，Xen hypervisor实现中存在漏洞。在试图dump有关崩溃的完全虚拟化guest信息时，拥有配置完全虚拟化guest系统权限的用户可以利用...
www.china-antivirus.com/Html/ldgg/xtld/19 ... 2012-6-4 - 百度快照

Xen hypervisor_callback函数中本地拒绝服务漏洞--瑞星反病毒资讯...
Xen hypervisor_callback函数中本地拒绝服务漏洞来源：绿盟科技 时间：2009-05-19 10:05:42 受影响系统：XenSource Xen 3.x 描述：Xen是可用于Linux内核的一种...
it.rising.com.cn/new2008/Safety/NewsInfo/ ... 2012-6-10 - 百度快照

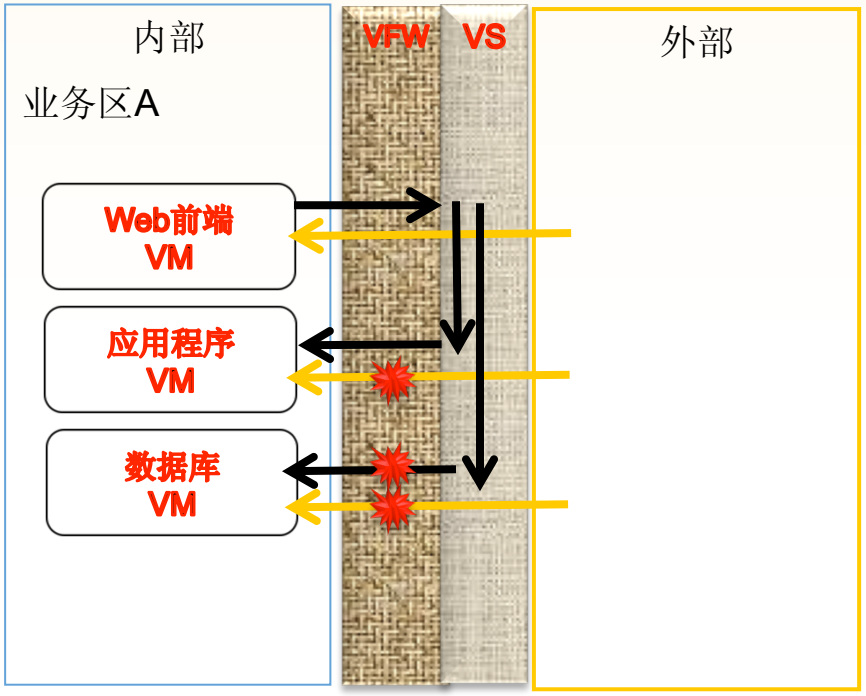
威胁二: 物理安全做到了吗?

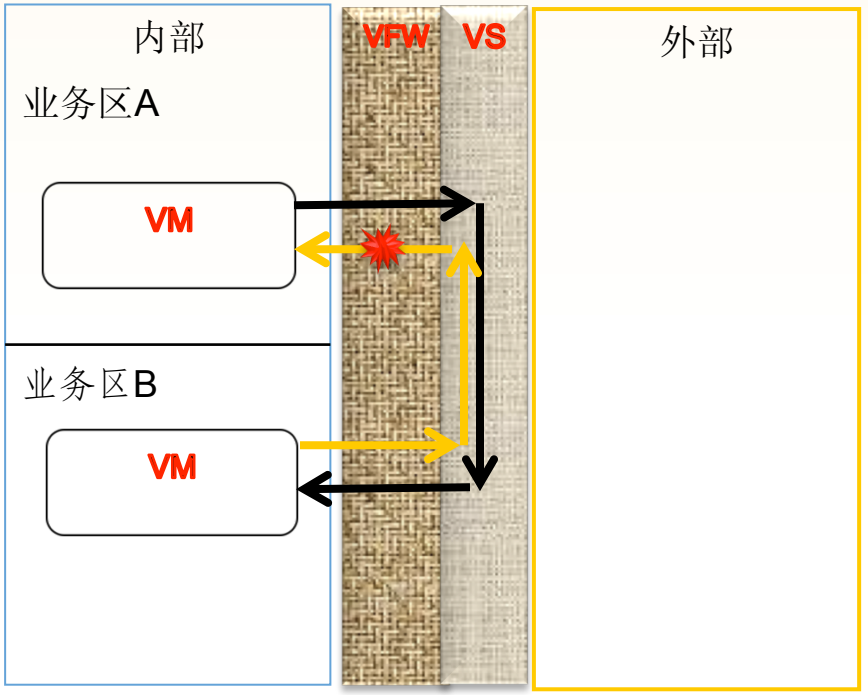
Amazon Data Center Loses Power During Storm

By: Rich Miller
June 30th, 2012

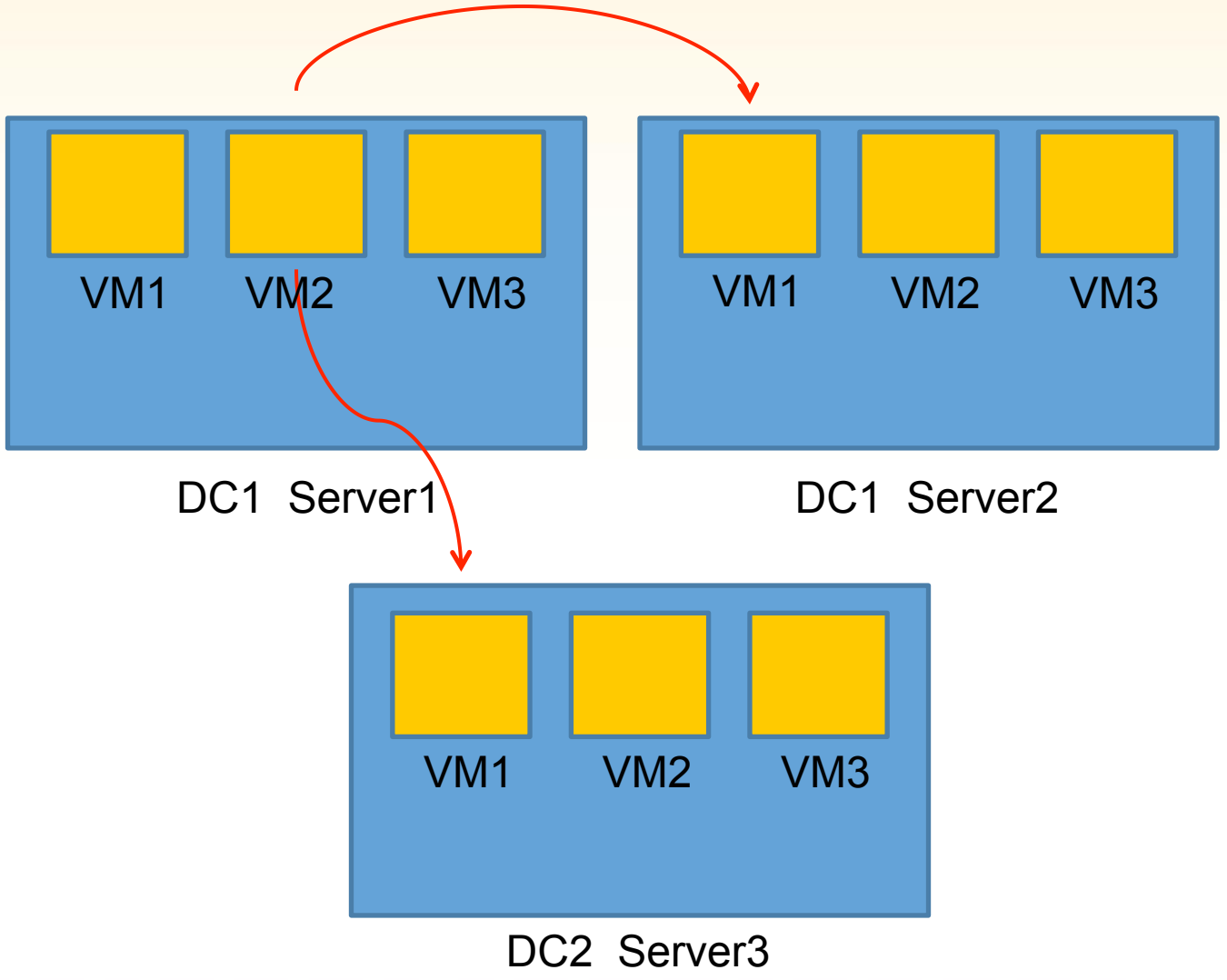
Amazon Web Services says an electrical storm caused a service outage Friday night at a data center in northern Virginia. (Lightning Photo via NOAA).

威胁三: 虚拟机之间的流量安全吗?

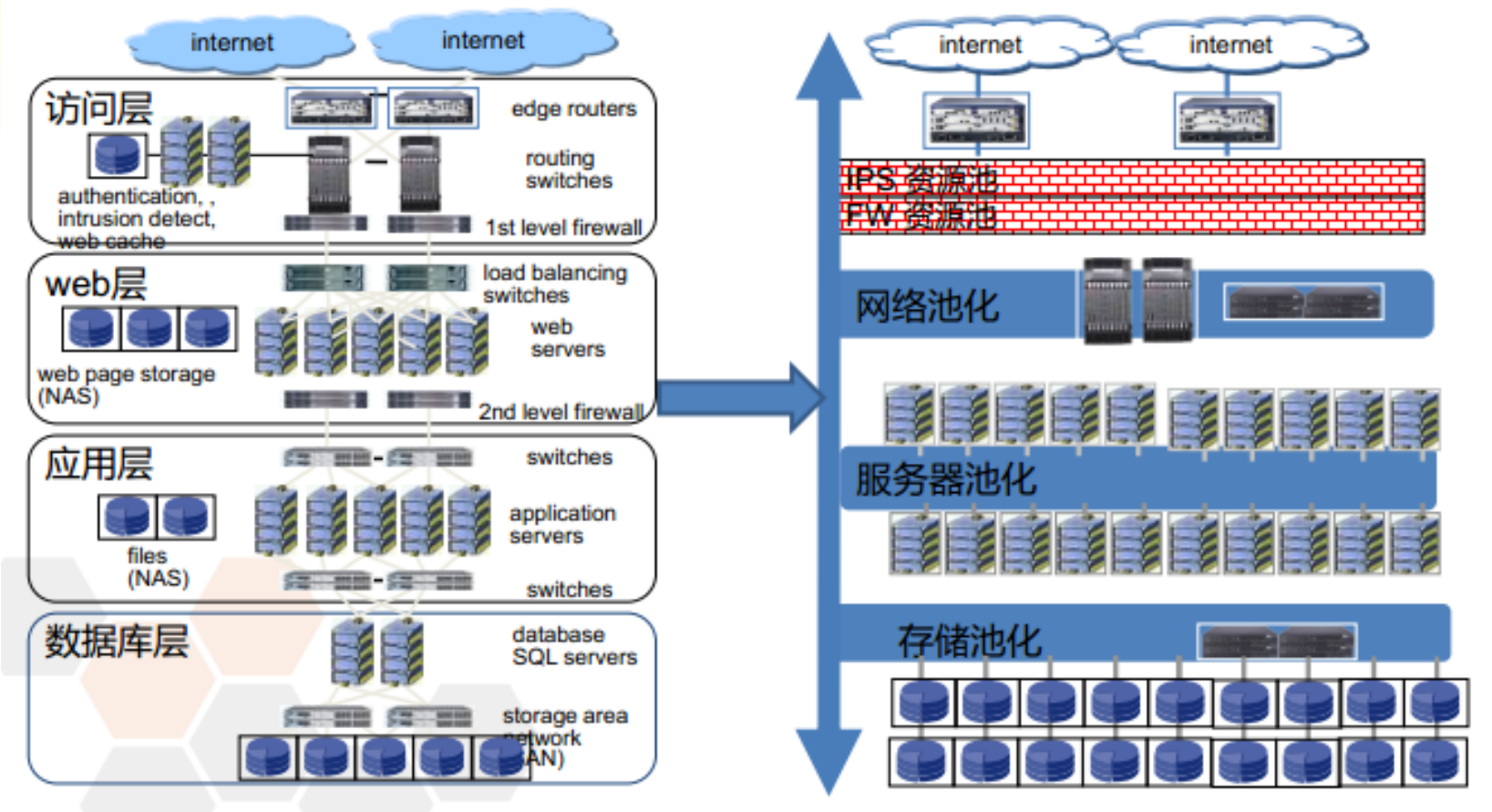




威胁四: 迁移后的安全策略能同步吗?



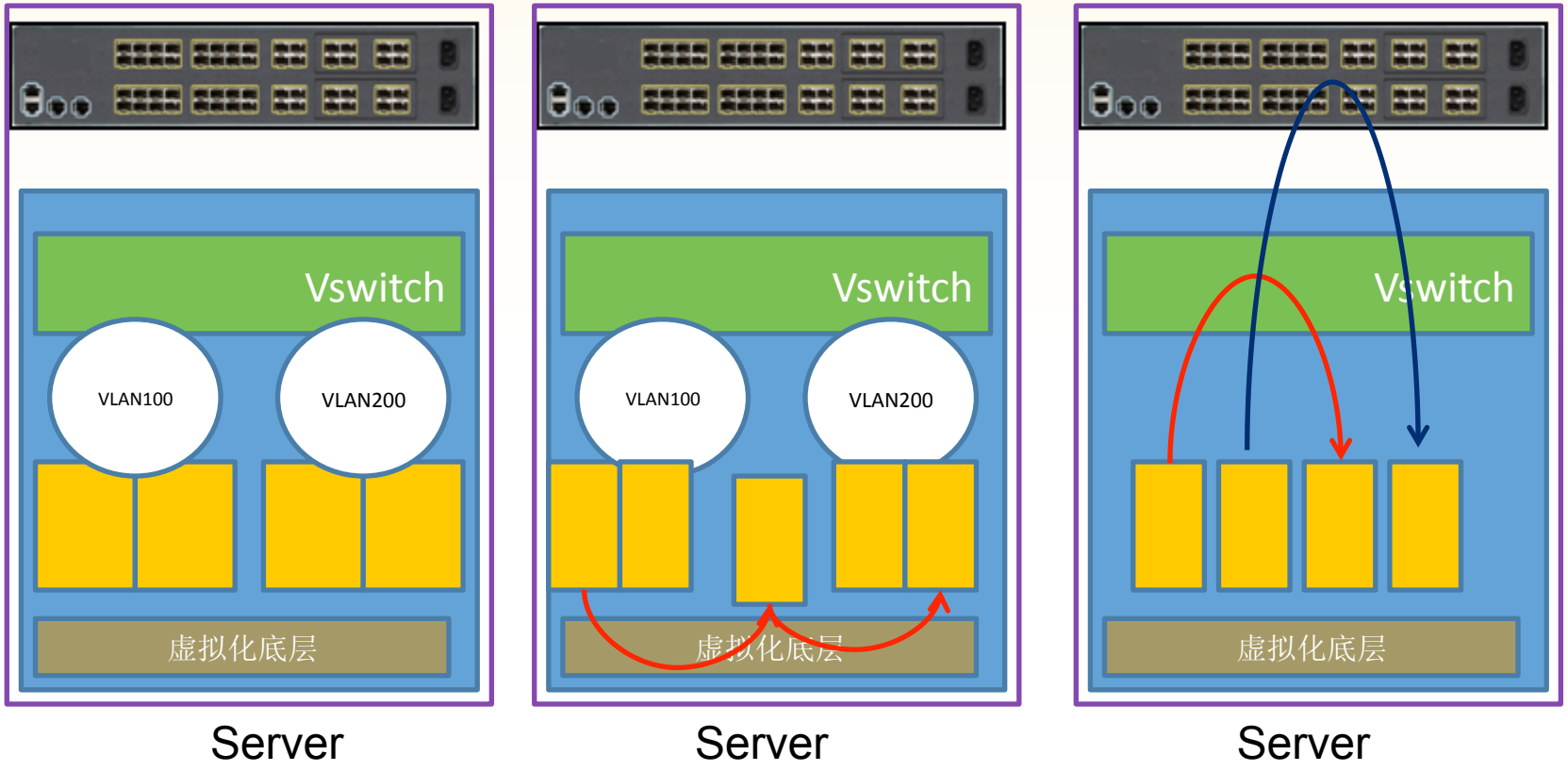
威胁5: 池化后可靠吗?性能足够吗?



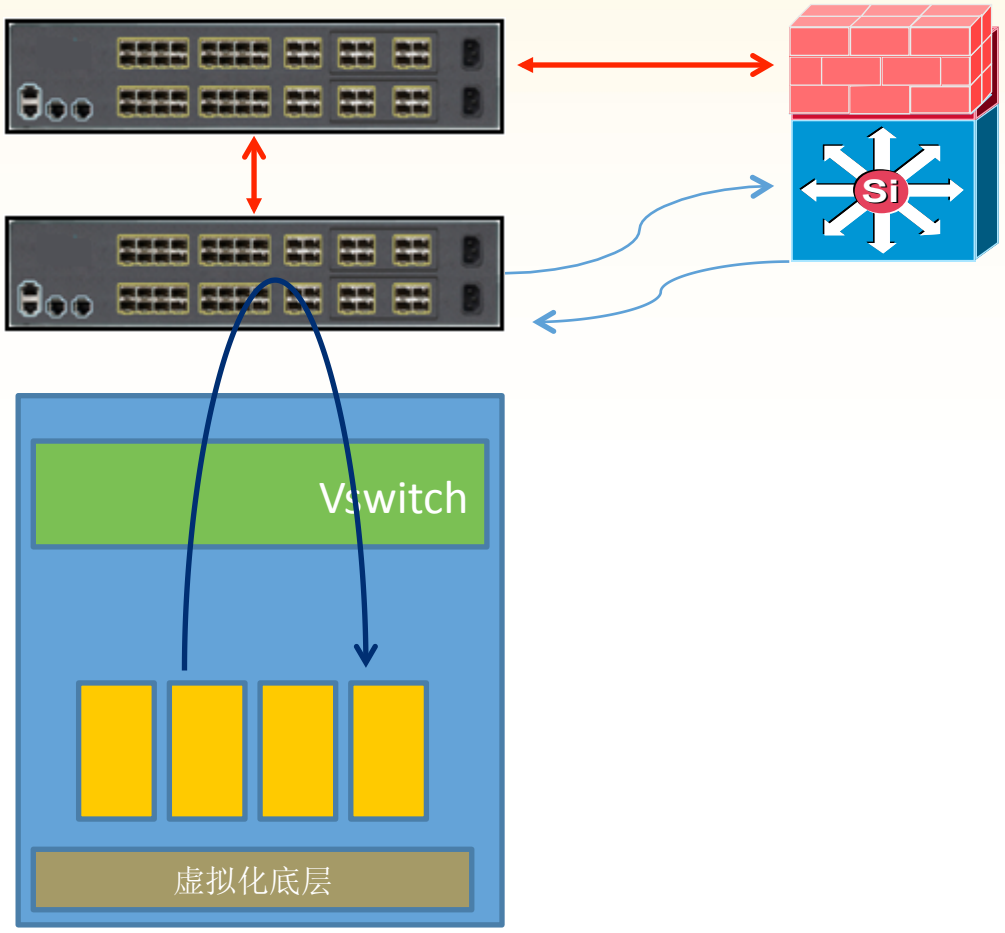
威胁6：了解这些吗？

- 启动风暴、登录风暴、 关闭风暴。
- 杀毒风暴。
- 文件碎片。
- 个性化需求。
- 专用外设。
- 延迟导致的应用崩溃、数据库崩溃
- 大集中的大集中。

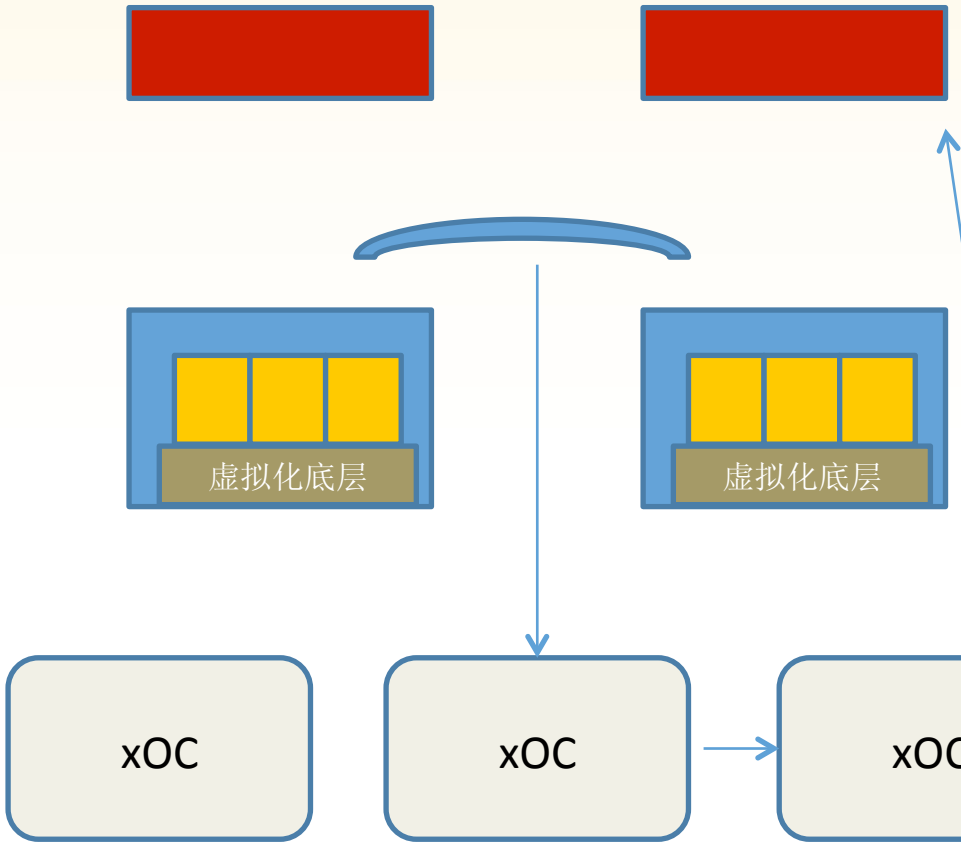
解决方案: VM之间的流量控制



解决方案: 水平攻击的防御(二层)



解决方案: 安全管理策略迁移



安全设备部署在哪里?
虚拟安全设备?

如何发现VM发生迁移

各个管理中心如何
分配任务和通讯

解决方案：风暴

- 存储阵列 +SSD ？
- 服务器 + SSD？
- 关闭病毒扫描？ 分段 ？
- 所谓的底层查杀 ？
- 分段开机 ？
- 快照也许并不适合虚拟化
- 成本 ！

门卫守则

- 对进入边界的访问进行各种安全管控
- 对出去的访问几乎不进行安全管控
- 至少对出口流量进行源IP地址校验 RFC2267 . (评估对路由器性能的影响)
- 最好添加一道水印

- DDos的源也许就在你的旁边

云环境下的身份认证

- 推荐使用双因子认证
- 公有云发生的泄密事件已经敲响警钟。

- 中国标准的云身份认证
- 国际标准的云身份认证

谢谢

RSA CONFERENCE
CHINA 2012