确保云环境中的应用安全
Application Safety in Cloud Computing

陆永康
日本及亚太区技术总监
SonicWALL, Inc.

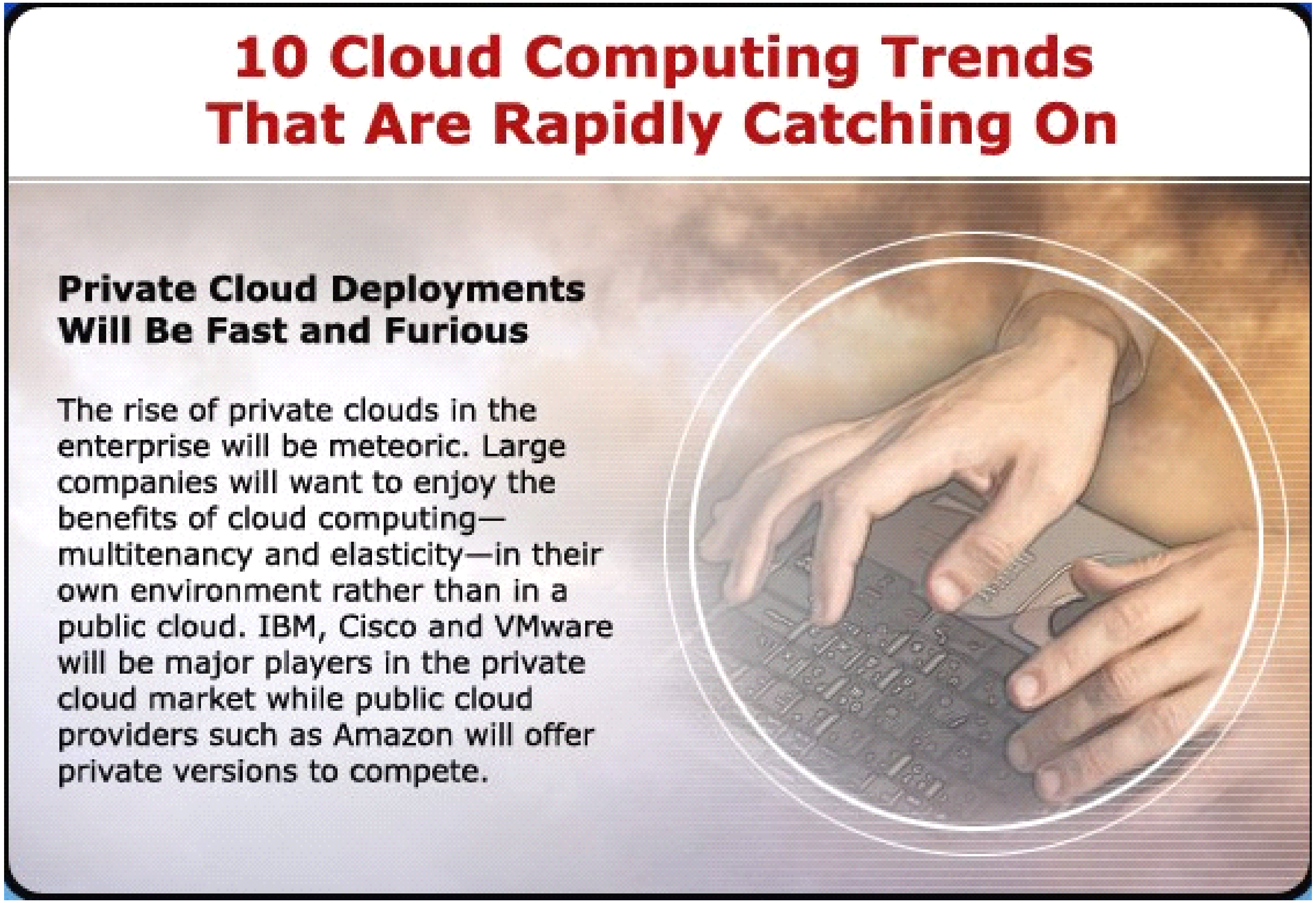
云计算推动力

- 节省成本
  - 不用投资软件和硬件
  - 不用花费在技术支持和设备维护
    - 操作系统打补丁
    - 升级
    - 数据备份
- 迅速部署
  - 简单定制 (Customization) 便马上可用

云计算推动力

- 可测量性
  - 自动资源分派
    - CPU 周期 (cycle)
    - 记忆
    - 存贮
    - 带宽
    - 连接数
- 用多少算多少

云计算趋势



10 Cloud Computing Trends That Are Rapidly Catching On

Private Cloud Deployments Will Be Fast and Furious

The rise of private clouds in the enterprise will be meteoric. Large companies will want to enjoy the benefits of cloud computing—multitenancy and elasticity—in their own environment rather than in a public cloud. IBM, Cisco and VMware will be major players in the private cloud market while public cloud providers such as Amazon will offer private versions to compete.

来源: eWEEK.com 2010年2月16日

云计算趋势

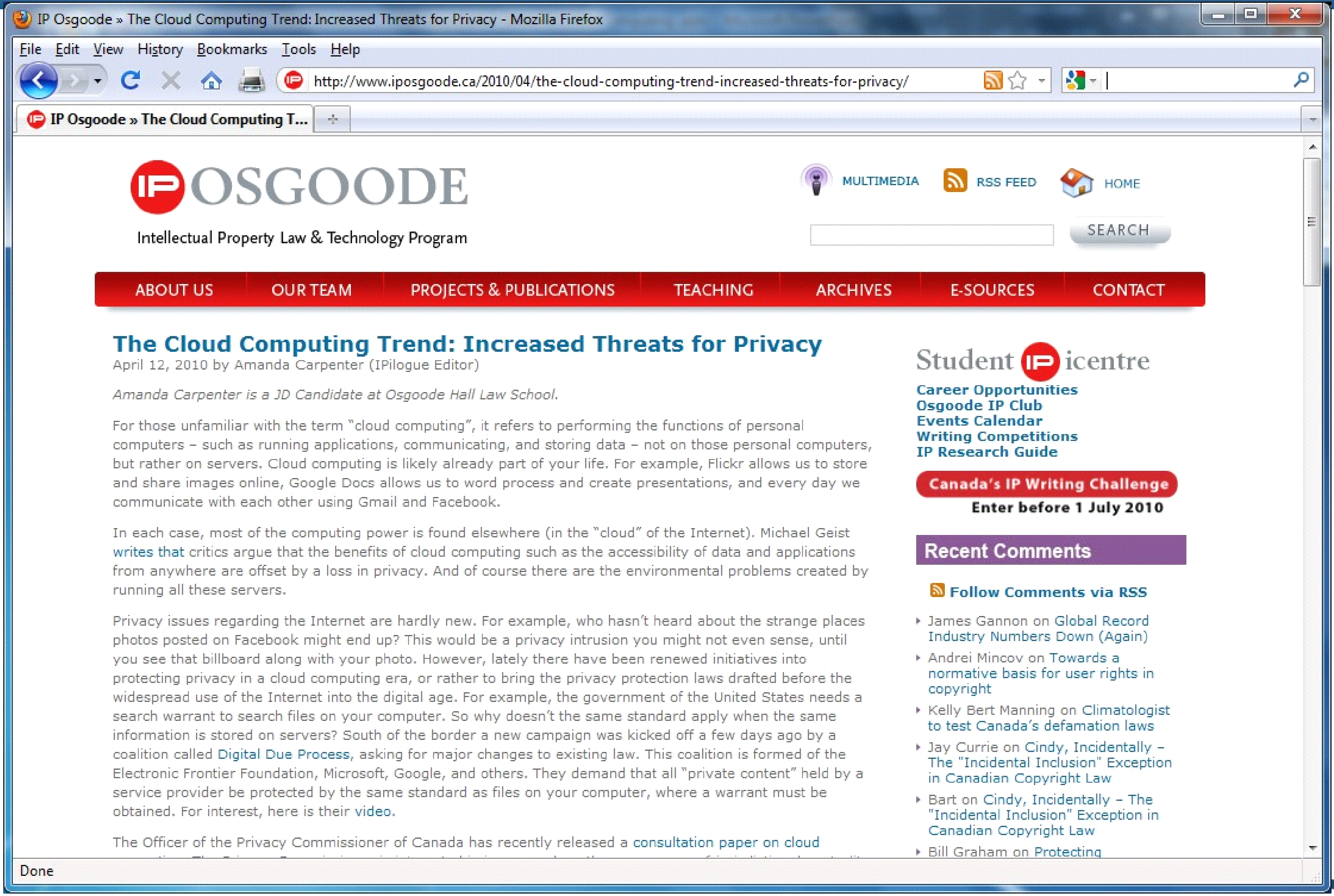
10 Cloud Computing Trends That Are Rapidly Catching On

HR, Collaboration Will Get Large in the Cloud

CRM will be joined by human capital management and collaboration in driving cloud application adoption. While Salesforce.com and Oracle CRM will continue to drive the adoption of cloud-based CRM, Taleo and Success Factors will drive the adoption of HCM. In addition, Google Apps and Cisco WebEx will drive the adoption of messaging and collaboration apps by midsize and large enterprises.

来源: eWEEK.com 2010年2月16日

云计算威胁


IP Osgoode » The Cloud Computing Trend: Increased Threats for Privacy - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.iposgoode.ca/2010/04/the-cloud-computing-trend-increased-threats-for-privacy/
IP Osgoode » The Cloud Computing T...
IP OSGOODE
Intellectual Property Law & Technology Program
MULTIMEDIA
RSS FEED
HOME
SEARCH
ABOUT US
OUR TEAM
PROJECTS & PUBLICATIONS
TEACHING
ARCHIVES
E-SOURCES
CONTACT
Done

The Cloud Computing Trend: Increased Threats for Privacy

April 12, 2010 by Amanda Carpenter (IPilogue Editor)

Amanda Carpenter is a JD Candidate at Osgoode Hall Law School.

For those unfamiliar with the term "cloud computing", it refers to performing the functions of personal computers – such as running applications, communicating, and storing data – not on those personal computers, but rather on servers. Cloud computing is likely already part of your life. For example, Flickr allows us to store and share images online, Google Docs allows us to word process and create presentations, and every day we communicate with each other using Gmail and Facebook.

In each case, most of the computing power is found elsewhere (in the "cloud" of the Internet). Michael Geist writes that critics argue that the benefits of cloud computing such as the accessibility of data and applications from anywhere are offset by a loss in privacy. And of course there are the environmental problems created by running all these servers.

Privacy issues regarding the Internet are hardly new. For example, who hasn't heard about the strange places photos posted on Facebook might end up? This would be a privacy intrusion you might not even sense, until you see that billboard along with your photo. However, lately there have been renewed initiatives into protecting privacy in a cloud computing era, or rather to bring the privacy protection laws drafted before the widespread use of the Internet into the digital age. For example, the government of the United States needs a search warrant to search files on your computer. So why doesn't the same standard apply when the same information is stored on servers? South of the border a new campaign was kicked off a few days ago by a coalition called Digital Due Process, asking for major changes to existing law. This coalition is formed of the Electronic Frontier Foundation, Microsoft, Google, and others. They demand that all "private content" held by a service provider be protected by the same standard as files on your computer, where a warrant must be obtained. For interest, here is their video.

The Officer of the Privacy Commissioner of Canada has recently released a consultation paper on cloud

Student IP icentre

Career Opportunities
Osgoode IP Club
Events Calendar
Writing Competitions
IP Research Guide

Canada's IP Writing Challenge
Enter before 1 July 2010

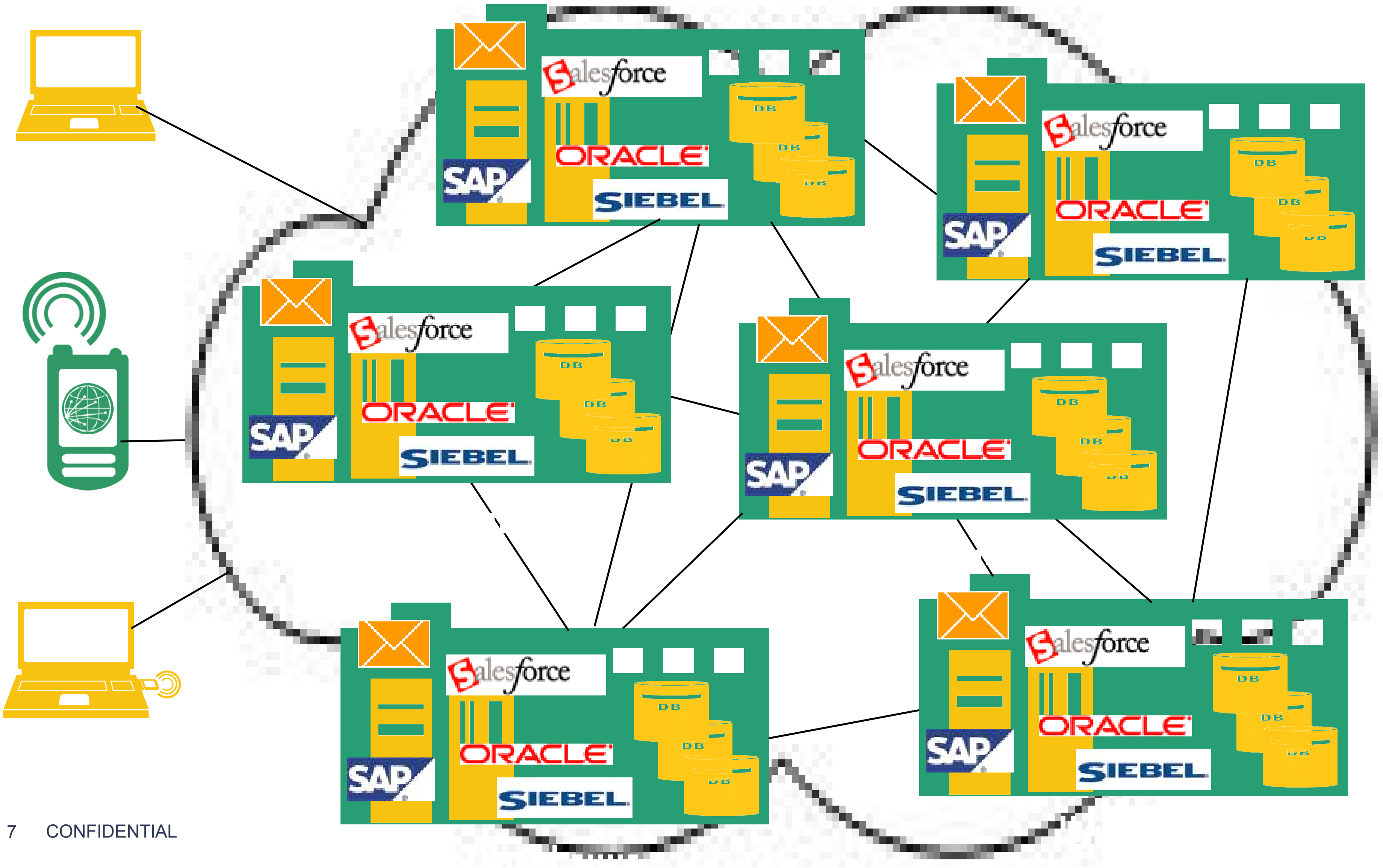
Recent Comments

Follow Comments via RSS

- James Gannon on Global Record Industry Numbers Down (Again)
- Andrei Mincov on Towards a normative basis for user rights in copyright
- Kelly Bert Manning on Climatologist to test Canada's defamation laws
- Jay Currie on Cindy, Incidentally – The "Incidental Inclusion" Exception in Canadian Copyright Law
- Bart on Cindy, Incidentally – The "Incidental Inclusion" Exception in Canadian Copyright Law
- Bill Graham on Protecting

来源：IP SOGOODE 2010年4月12日

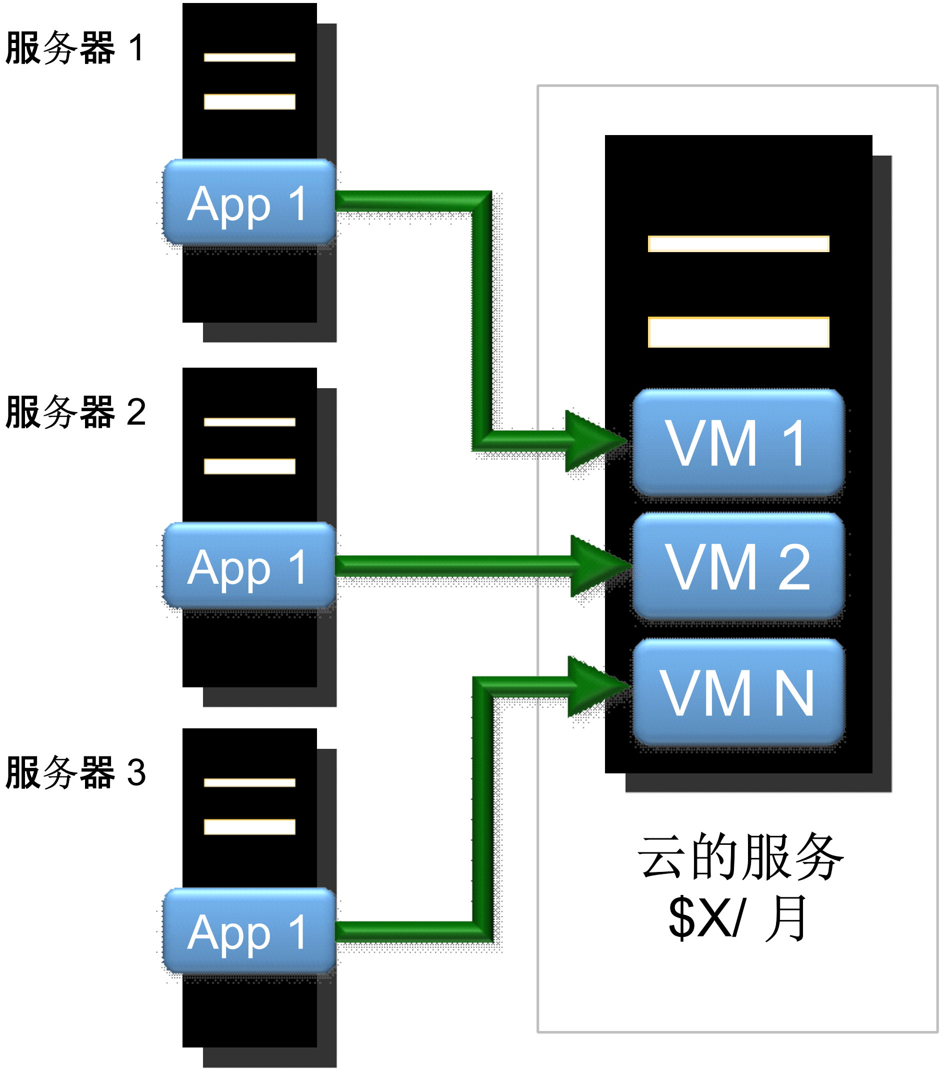
云



云的结构

- 互联网连接
- 多个数据中心
- 资源分享 (多租户 Multi-tenancy)
  - 服务器
  - 软件
    - 应用软件
  - 存贮
  - 网络

基于云的服务例子



好处

- 提供迅速可测量性 (scalability), 冗余 (redundancy)
- 减少资本费用 (cap-ex)

涵义

- 数据和应用已移离你可控制的范围 -- 流动用户直接存取数据
- 对延误和带宽敏感的应用会有一定影响

转移到云（公众云 public cloud)

- 推动力
  - 节省成本
  - 迅速部署
- 把你的应用看成基于云的服务
- 你的应用转移到云后你将会失去基础设施（Infrastructure)的控制权
  - 依赖云供应商

你的应用在云上安全吗?

- 应用软件的隔离
  - 租户之间的隔离
  - 避免死机的影响 – 其他租户应用出问题时不构成影响
  - 记忆，存贮，网络
- 存取控制 (Access control)
  - 认证和授权 (Authentication and authorization)
  - 时间的限制
- 威胁
  - 病毒, 木马, Malware, 间谍软件
  - DoS 和 DDoS 攻击
  - 网 (Web) 和数据库的攻击

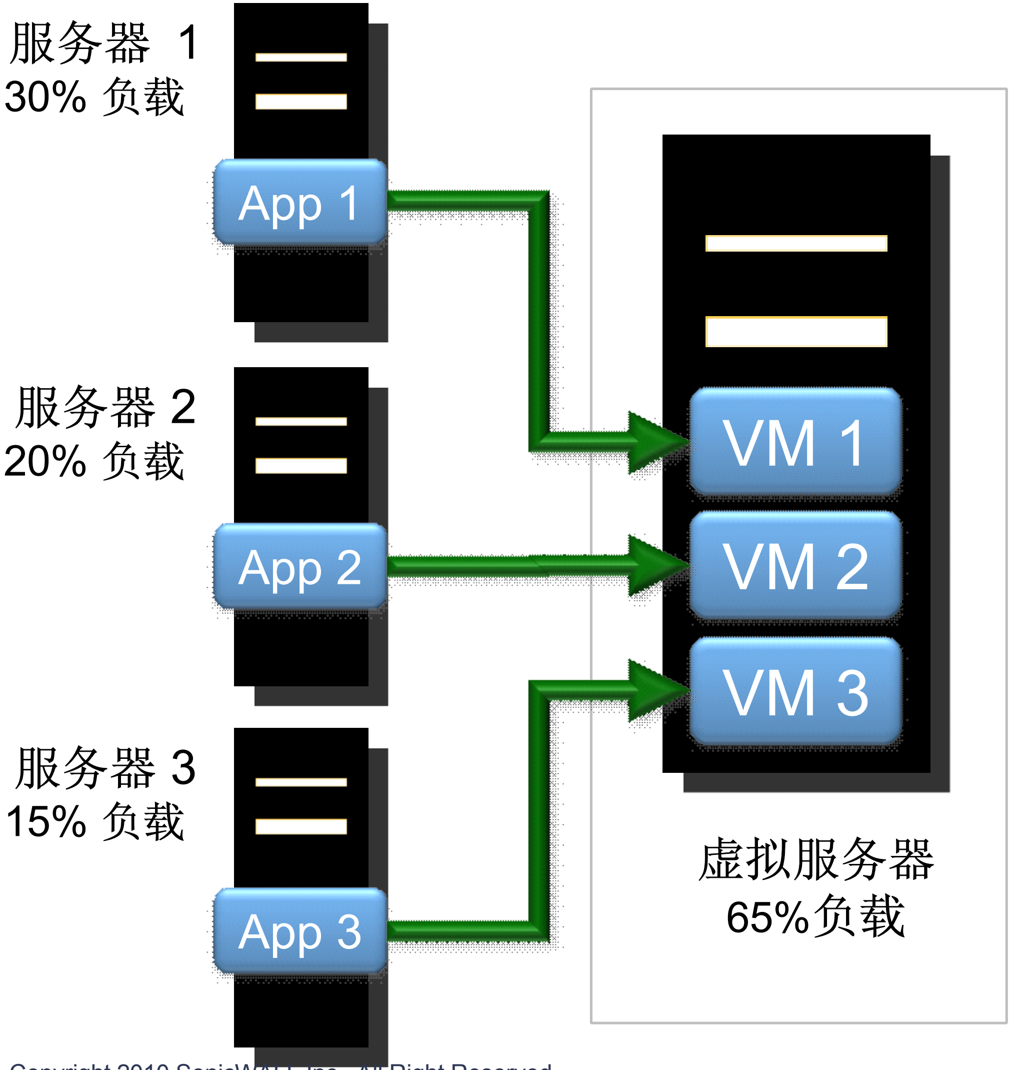
你的应用在云上安全吗?

- 数据的保护
  - 存贮
    - 备份和恢复
    - 加密
    - 在互联网的传送
  - 数据泄漏
    - 机密数据
  - 传输风险
    - 在数据中心里
    - 数据中心之间
    - 在互联网上
    - 机密性 (加密)
    - 完整性 (认证)

公众云 vs 企业云

- 你可以百分百控制企业云(enterprise cloud) 的安全
- 至于公众云 (public cloud)
  - 要看云供应商能提供什么
  - 需要制定安全政策
    - 数据完整性
    - 数据泄漏
    - 不死机证明 (proof)
    - 灾害恢复 (Disaster recovery)
    - 存取控制
    - Forensics
    - 服务水准协议 (Service level agreement)
      - Down time

云里面的虚拟服务器



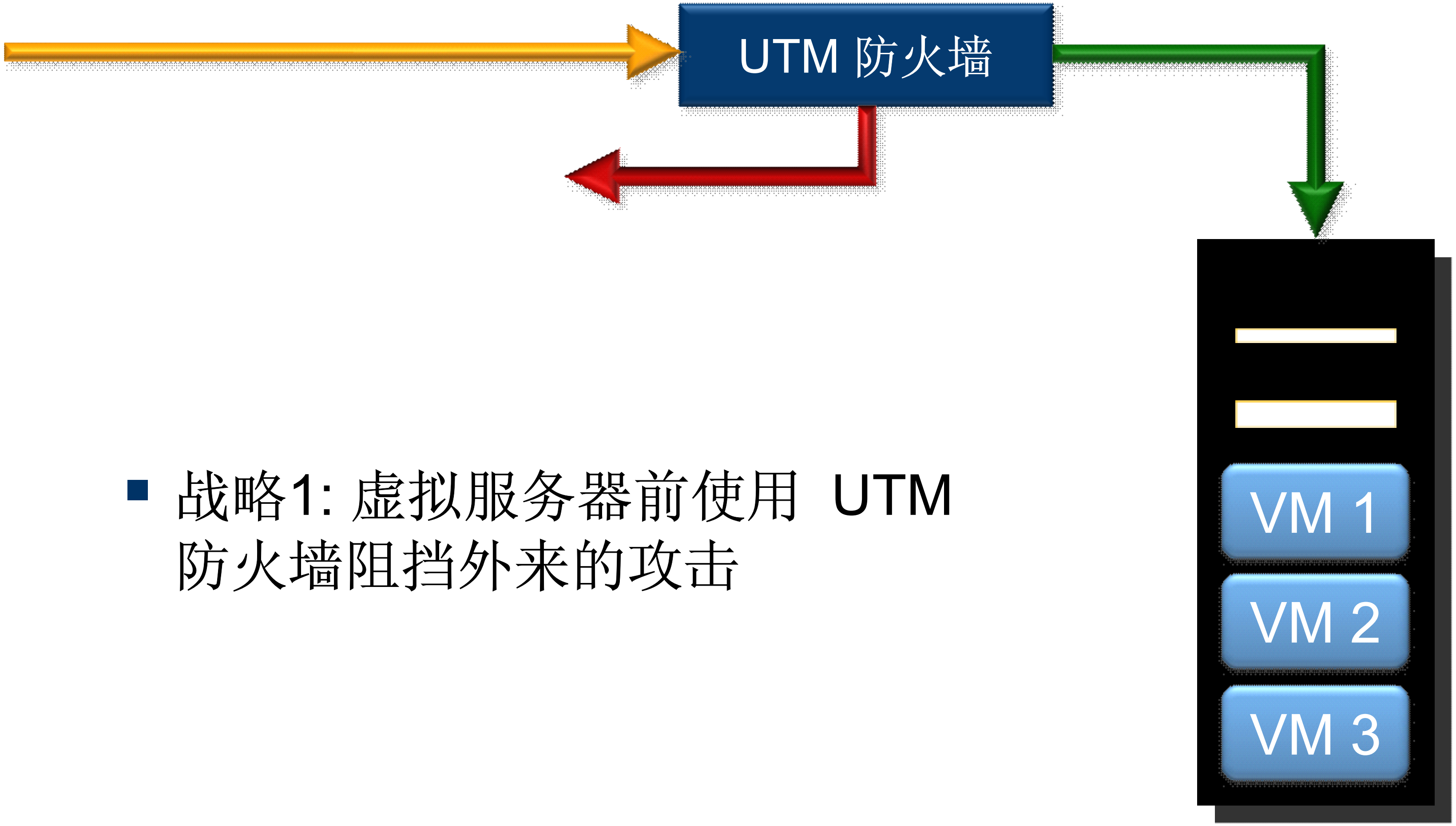
好处

- 高效率
- 好表现 (Performance)

涵义

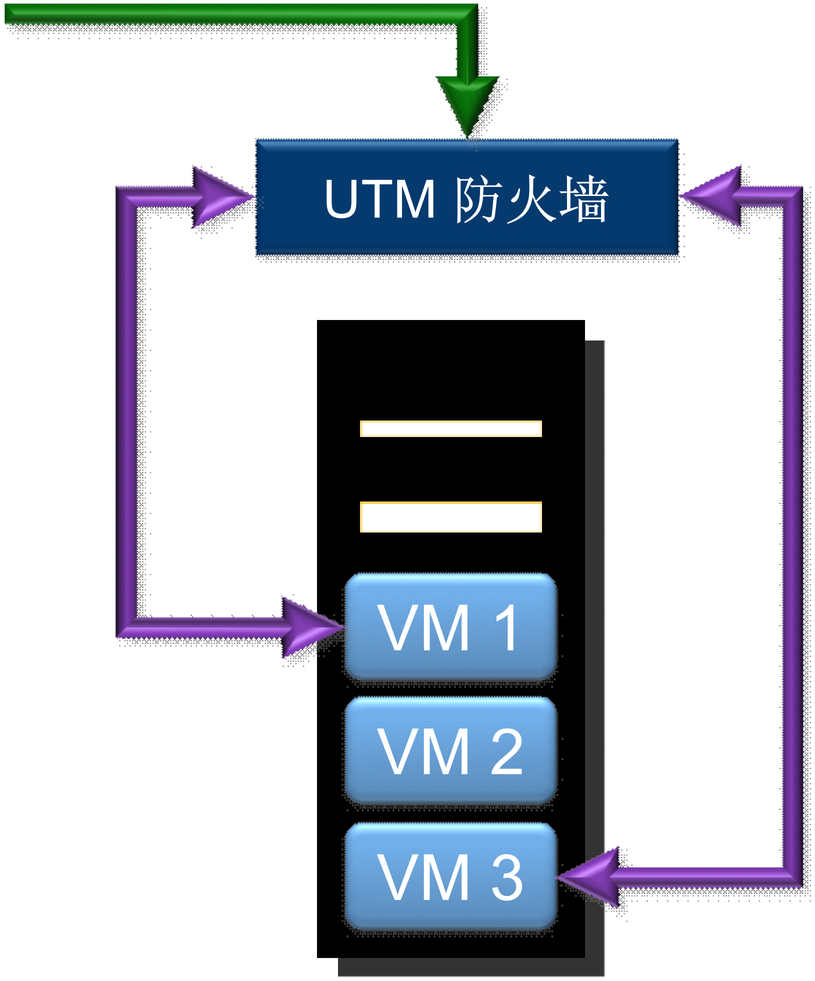
- Hypervisor 威胁
- 应用之间的安全

保护云里面的虚拟服务器



- 战略1: 虚拟服务器前使用 UTM 防火墙阻挡外来的攻击

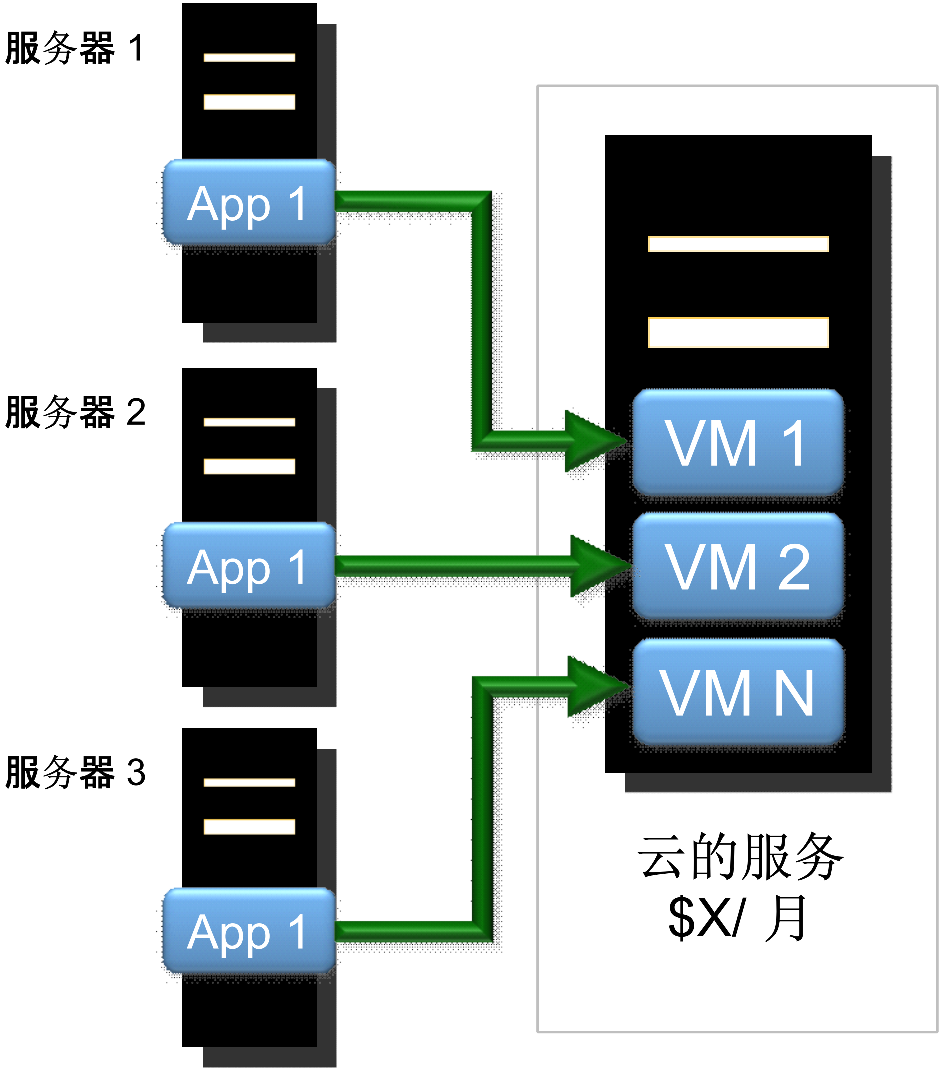
保护云里面的虚拟服务器



干净虚拟服务器网络（**Clean VM Networking)**

- 战略2：在多个虚拟服务器之间提供安全保护
- UTM 防火墙保护：
  - 虚拟服务器1和3
  - 外来攻击

基于云的服务例子



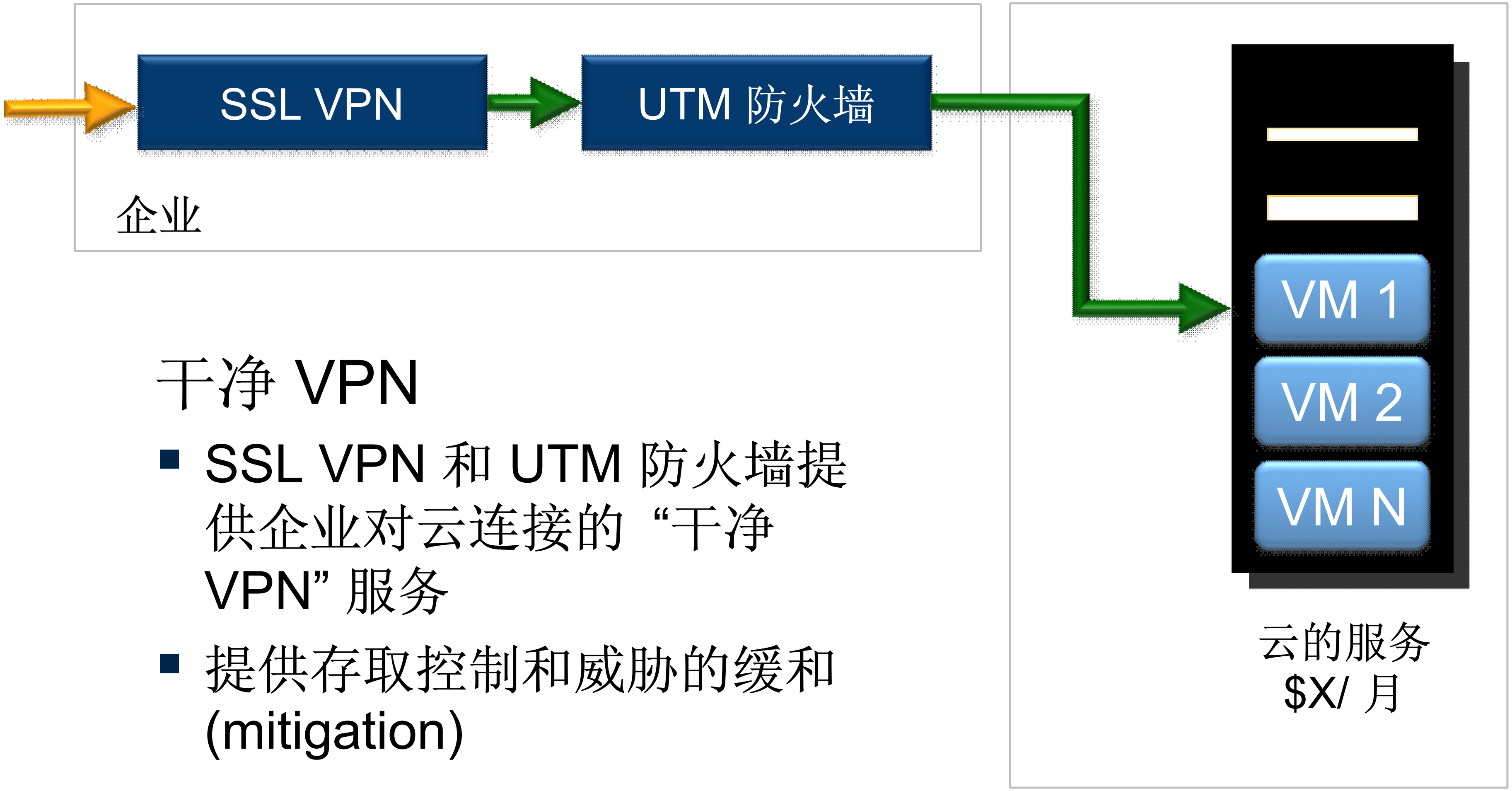
好处

- 提供迅速可测量性 (scalability), 冗余 (redundancy)
- 减少资本费用 (cap-ex)

涵义

- 数据和应用已移离你可控制的范围 -- 流动用户直接存取数据
- 对延误和带宽敏感的应用会有一定影响

基于云的服务



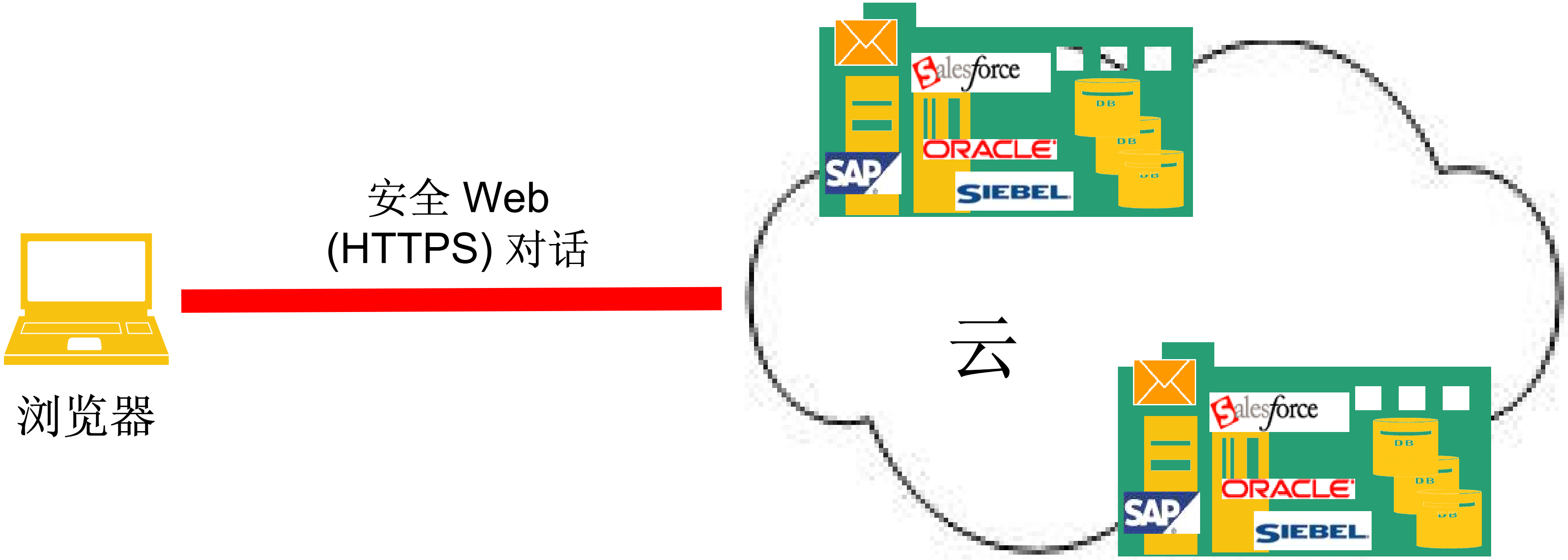
干净 VPN

- SSL VPN 和 UTM 防火墙提供企业对云连接的 “干净 VPN” 服务
- 提供存取控制和威胁的缓和 (mitigation)

云安全措施

客户端

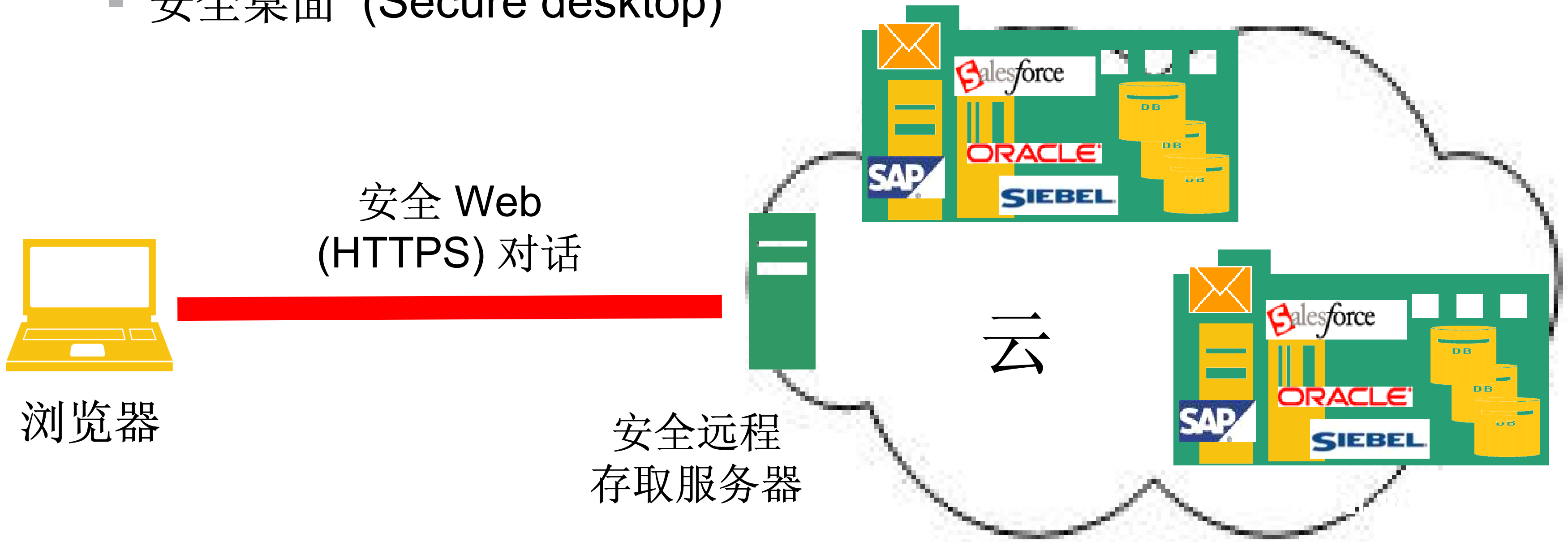
- 安全 web (HTTPS) 对话
- 切勿使用公共电脑



云安全措施 (1)

云接入点

- 安全远程存取服务器 (Secure Remote Access Server)
- 远点控制 (End point control)
  - 设备查询（Device interrogation – 病毒软件，操作系统 …)
  - 检疫区 (Quarantine zone)
  - 安全桌面 (Secure desktop)



安全 Web
(HTTPS) 对话

浏览器

安全远程
存取服务器

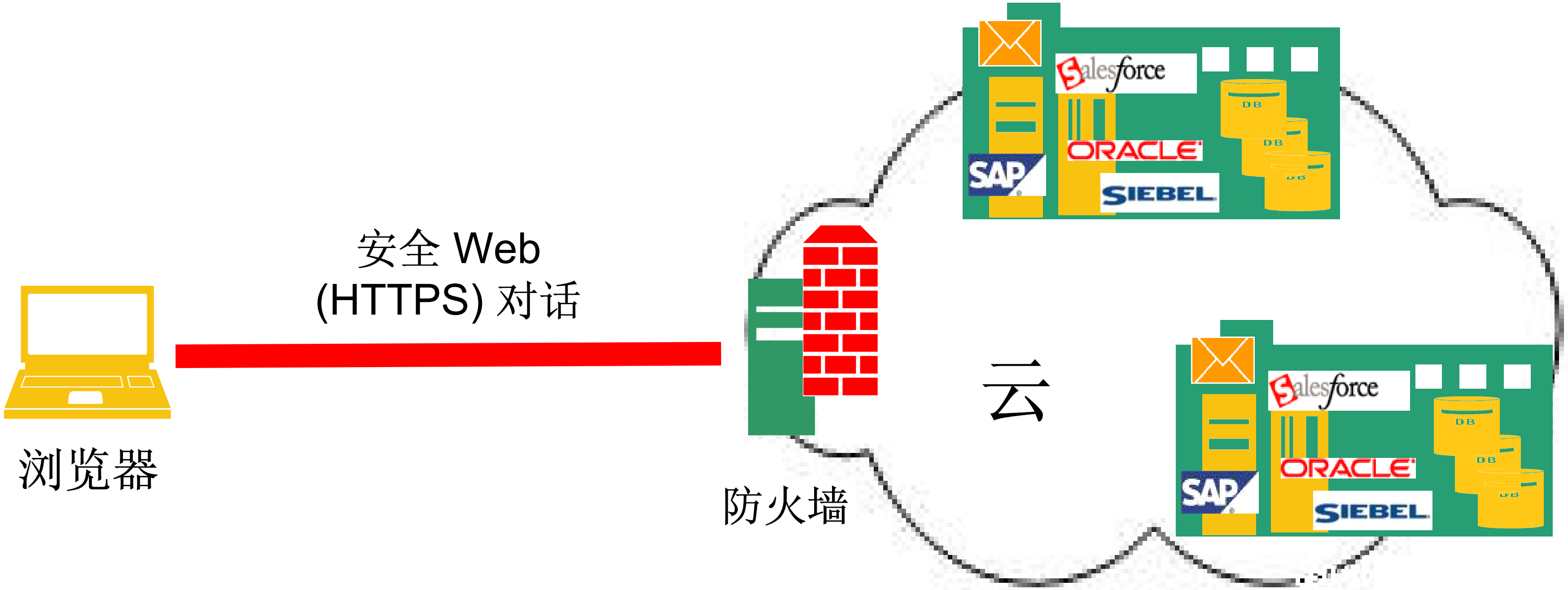
云

SONICWALL

云安全措施 (2)

云接入点

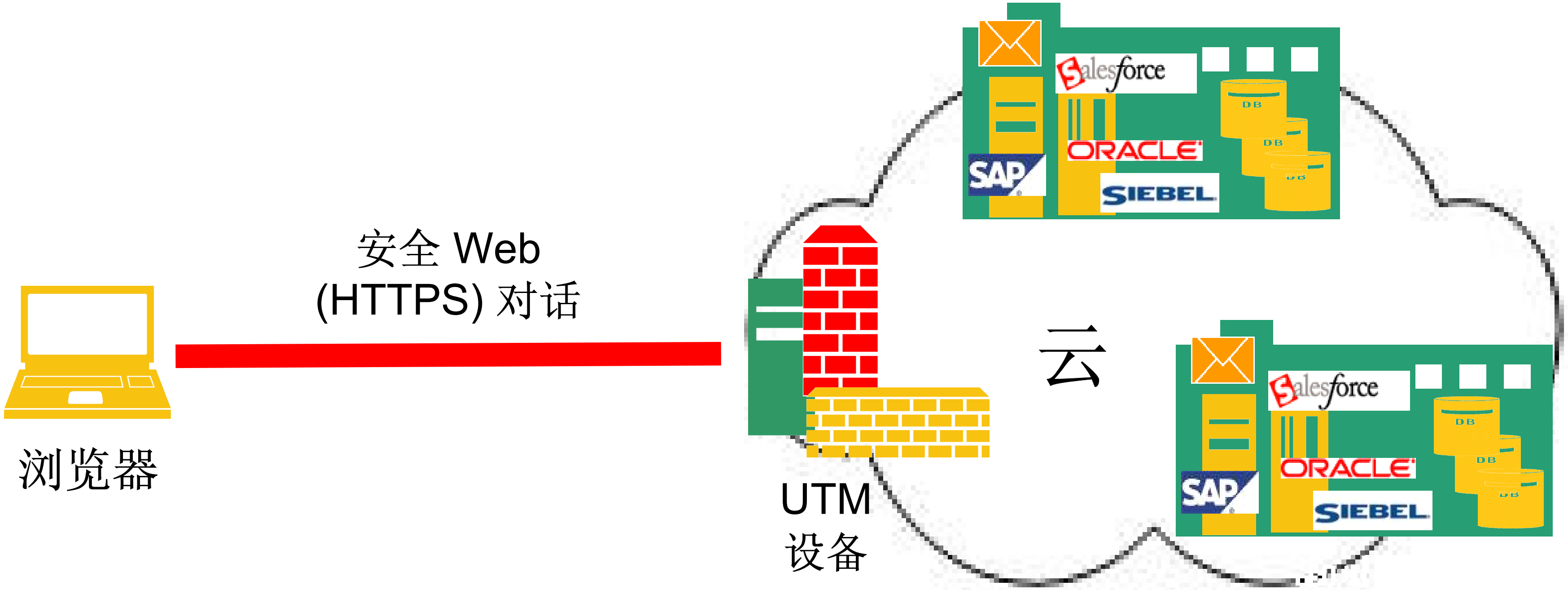
- 防火墙
  - DoS 和 DDoS
  - 防火墙策略



云安全措施 (3)

云接入点

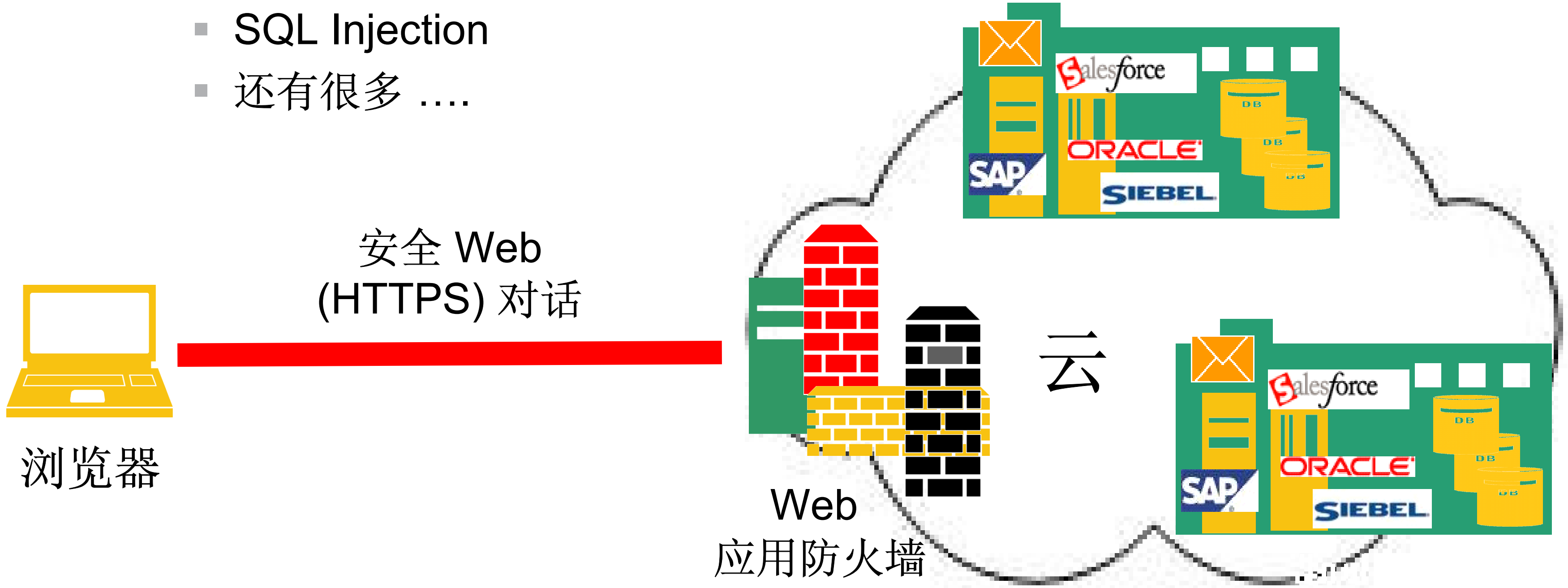
- UTM 设备
  - 网关防病毒 (Gateway Anti-Virus)
  - 入侵阻止 (Intrusion Prevention)
  - 反间谍软件 (Anti-Spyware)



云安全措施 (4)

云接入点

- Web 应用防火墙 (Web Application Firewall)
  - 阻止 web 的攻击
  - OWASP 和 PCI compliant
    - Cross Site Scripting (XSS)
    - SQL Injection
    - 还有很多 ....



安全 Web
(HTTPS) 对话

浏览器

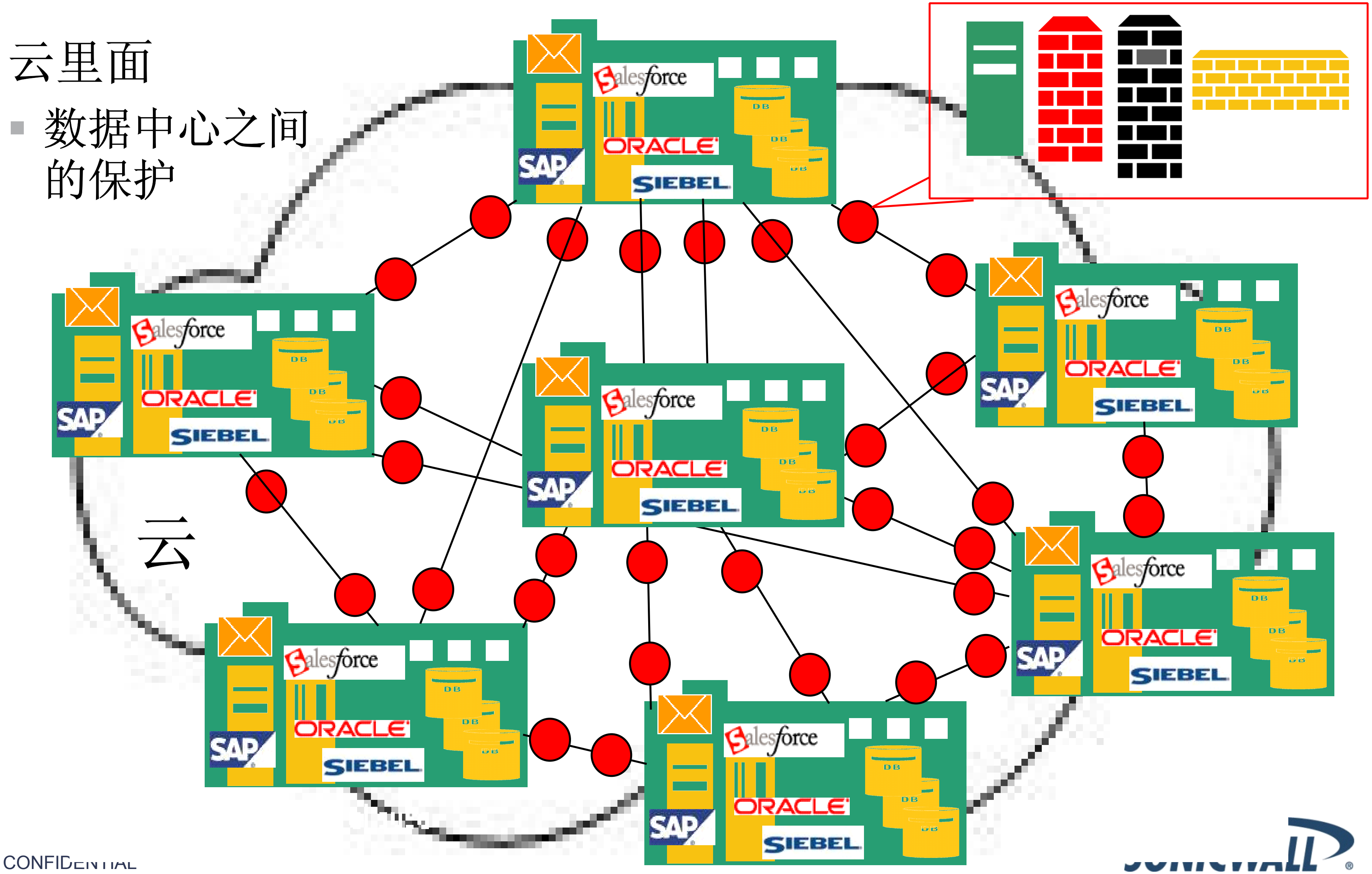
Web
应用防火墙

云

云安全措施 (5)

云里面

- 数据中心之间的保护



云安全措施 (6)

数据中心里面

- 补丁和升级
  - 操作系统
  - 应用软件
  - 存贮系统
  - 网络装置
- 数据的保护
  - 泄漏
  - 加密
  - 隔离

云安全措施 (7)

数据中心里面

- 密码保证 (Password Assurance)
  - 密码破解 (Password cracking)
  - 暴力入侵的防止 (Brute force defense)
- 日志, 监控, 报表
  - 审计试验 (Auditing Trail)
  - 表现 (Performance)
  - 资源运用 (Resources utilization)

谢谢

www.sonicwall.com

SONICWALL®