PaloAlto Networks—企业解决方案及成功客户案例分享

Palo Alto Networks

paloalto NETWORKS
the network security company™

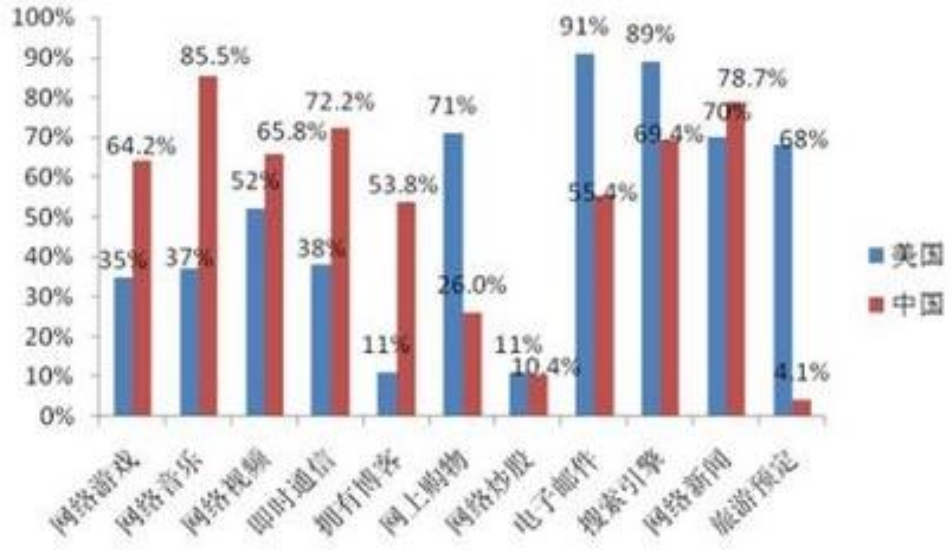
企业互联网接入网关

paloalto NETWORKS
the network security company™

企业客户互联网需求

- 趋势
  - 互联网应用大量增加；
  - 互联网带宽不断增加；
  - 网络威胁数量增多，针对性加强；
  - 企业分支数量多，成本压力大；
  - 管理层对报告要求高；

- 问题
  - 对网络中的应用没有探测能力；
  - 缺乏对网络的有效安全防御措施；
  - 管理成本太高；
  - 对用户的网络访问行为缺乏管控；
  - 对分支机构和移动用户，无法形成有效的统一安全策略。



PaloAlto Networks解决方案

App-ID

识别应用

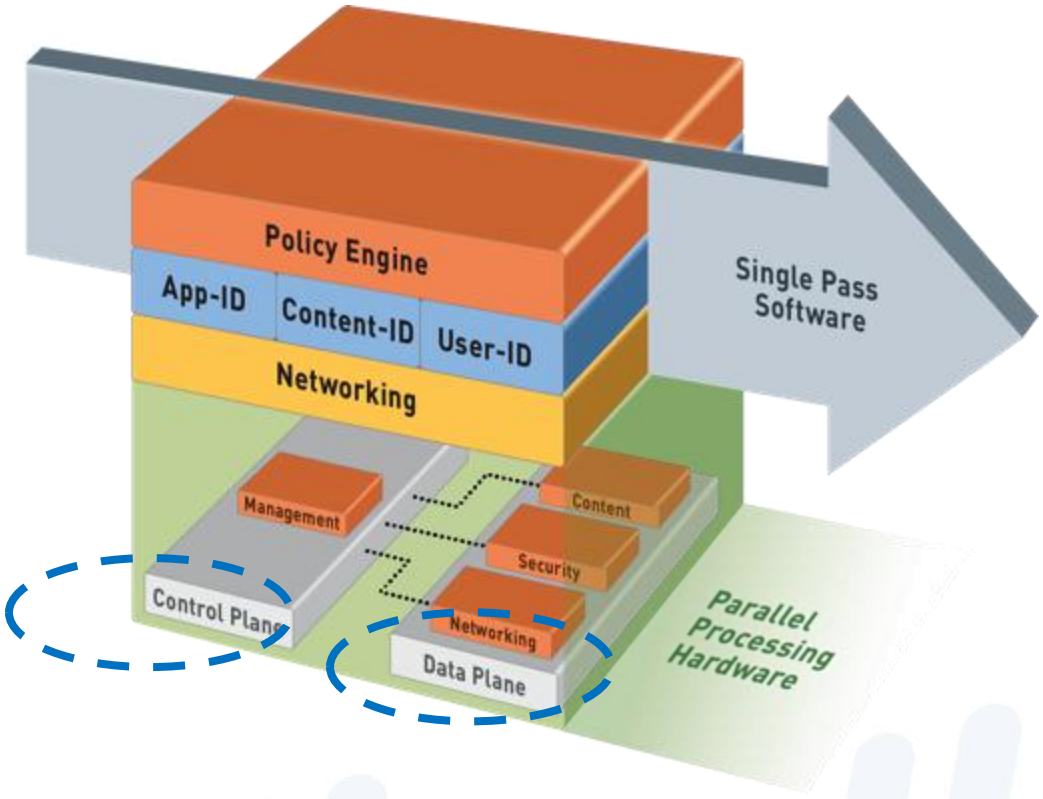
Content-ID

扫描内容

User-ID

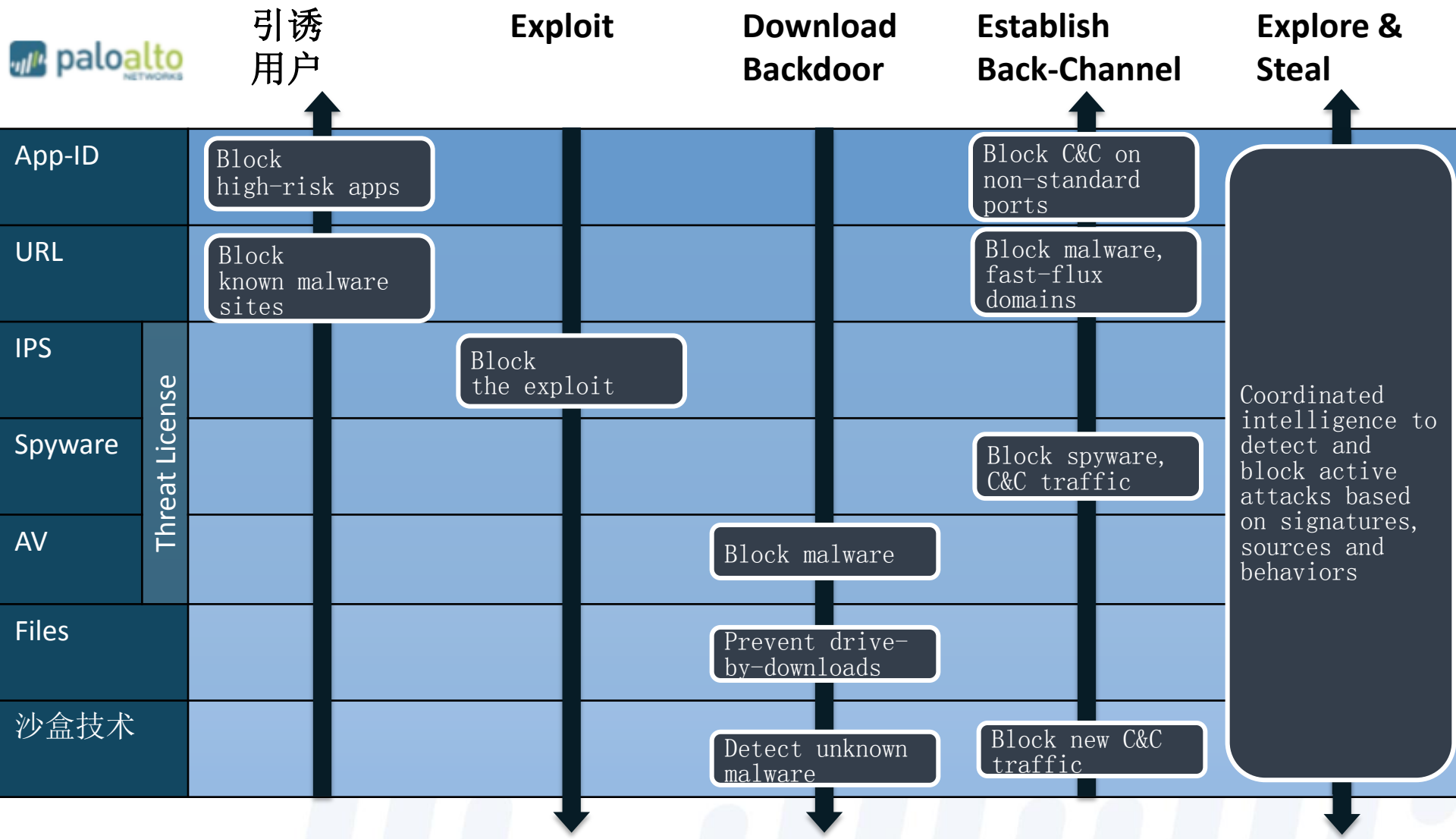
识别用户

Palo Alto Networks Platform



高达20Gbps(App-ID), 低延时

综合安全防御


引诱用户
Exploit
Download Backdoor
Establish Back-Channel
Explore & Steal
App-ID
URL
IPS
Spyware
AV
Files
沙盒技术
Threat License
Block high-risk apps
Block known malware sites
Block the exploit
Block malware
Prevent drive-by-downloads
Detect unknown malware
Block C&C on non-standard ports
Block malware, fast-flux domains
Block spyware, C&C traffic
Block new C&C traffic
Coordinated intelligence to detect and block active attacks based on signatures, sources and behaviors

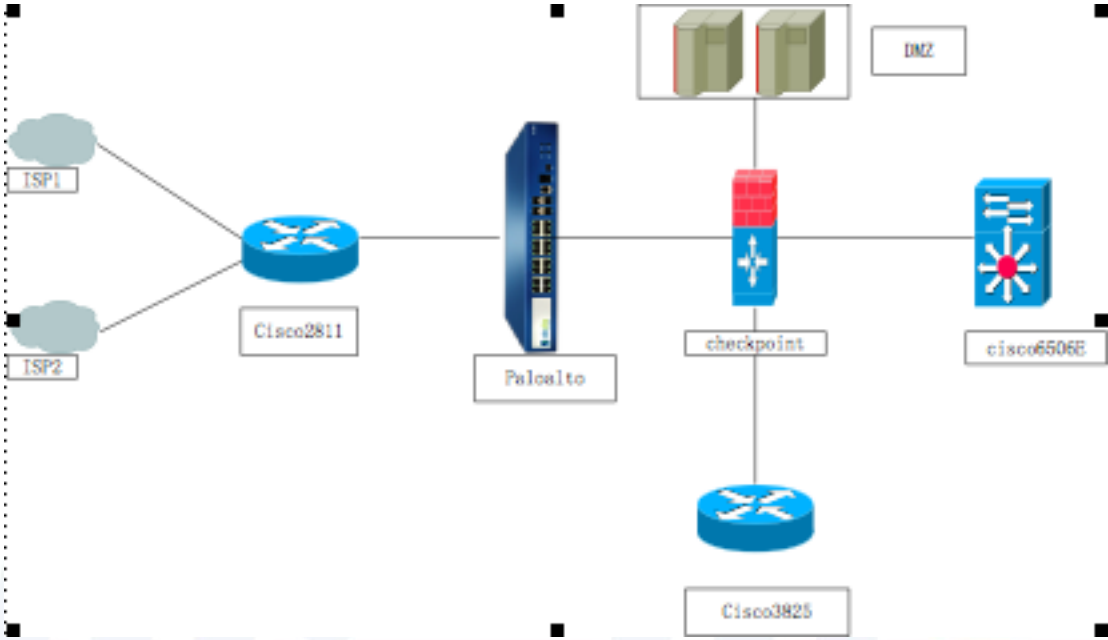
成功应用

机遇

- 防火墙升级
- 缺少安全解决方案
- 希望有更好的VPN解决方案。

结果

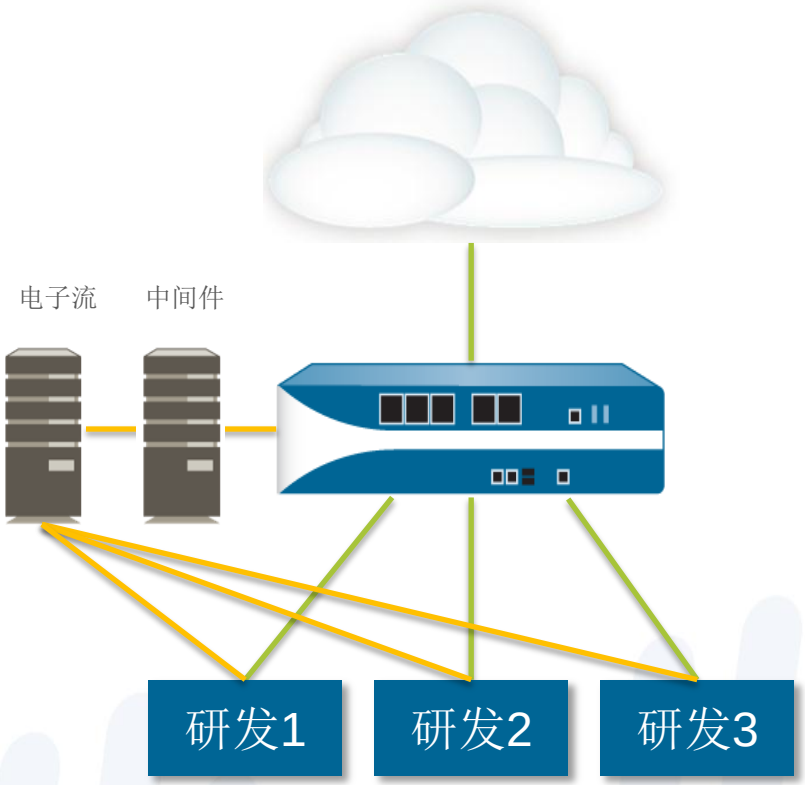
- 完整覆盖- 防火墙、应用程序控制、威胁防范
- 易于远程管理—统一安全策略
- 灵活智能的移动用户接入
- 根据用户身份开放核心服务器的访问



安全防护

案例分享——XX通讯

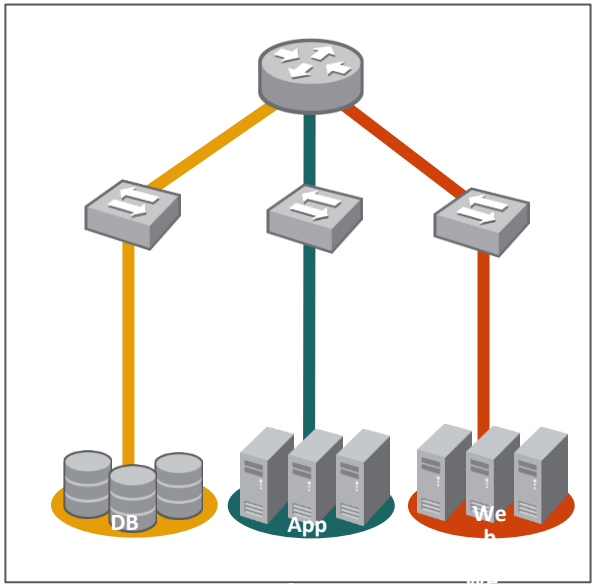
- 透明接入，不影响网络结构
- 普通用户仅能够使用限定应用，禁止上传
- 全面禁止可能导致数据外泄的应用
- 需要特殊权限的用户通过电子流申请
- 电子流经过N层批准后自动向PAN下发策略
- 中间件服务器自动维护策略
- 双向安全防护（IPS、防病毒）

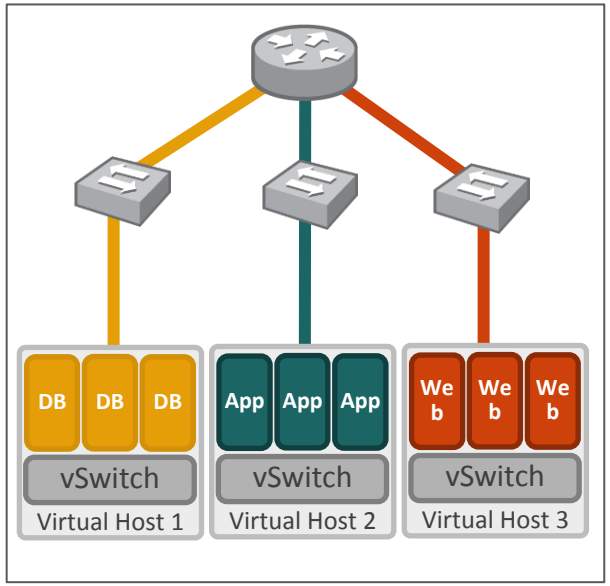


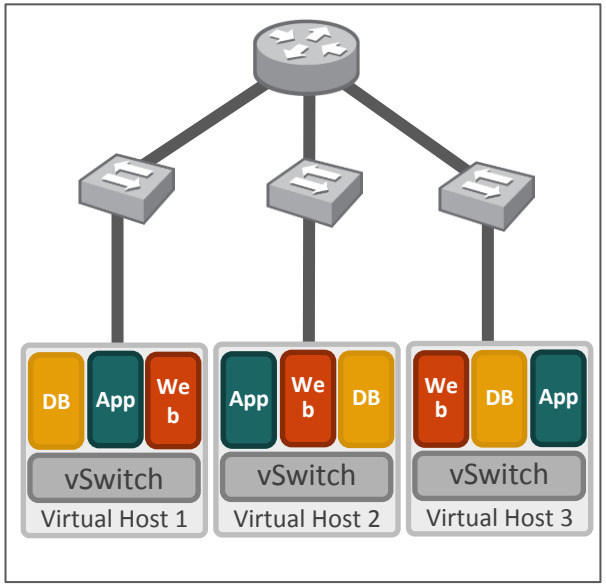
企业数据中心

paloalto NETWORKS
the network security company™

虚拟化







传统数据中心
- 专用应用程序服务器
- 服务器使用率 ＝15%
- 横跨流量

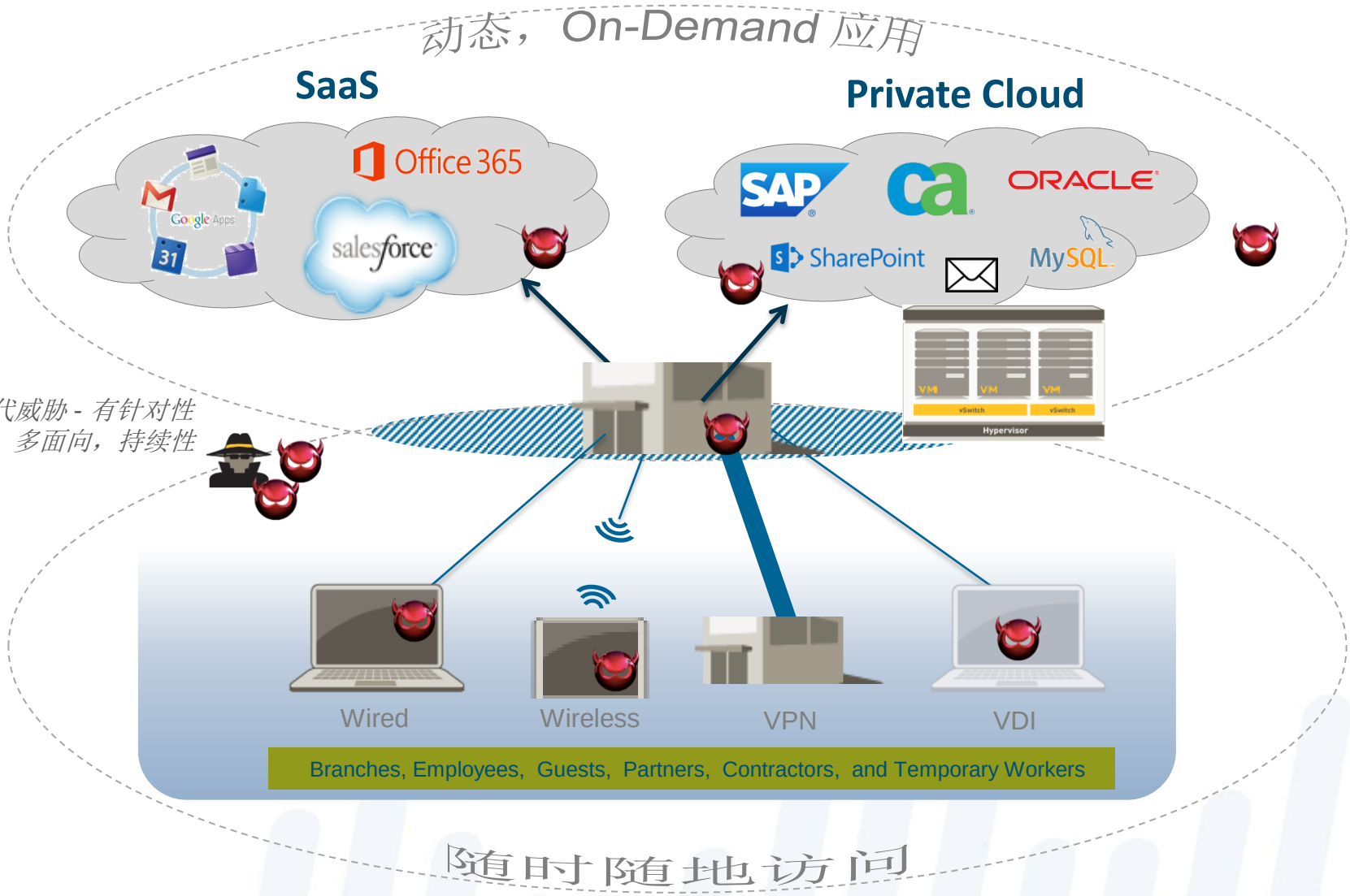
虚拟数据中心
- 每个服务器多个应用
- 提高运营效率
- 提高服务器利用率

云（私有/公共）
- IT 即服务
- 按需服务
- 自动化和编排化

业务灵活性 Vs 节省成本 Vs 安全

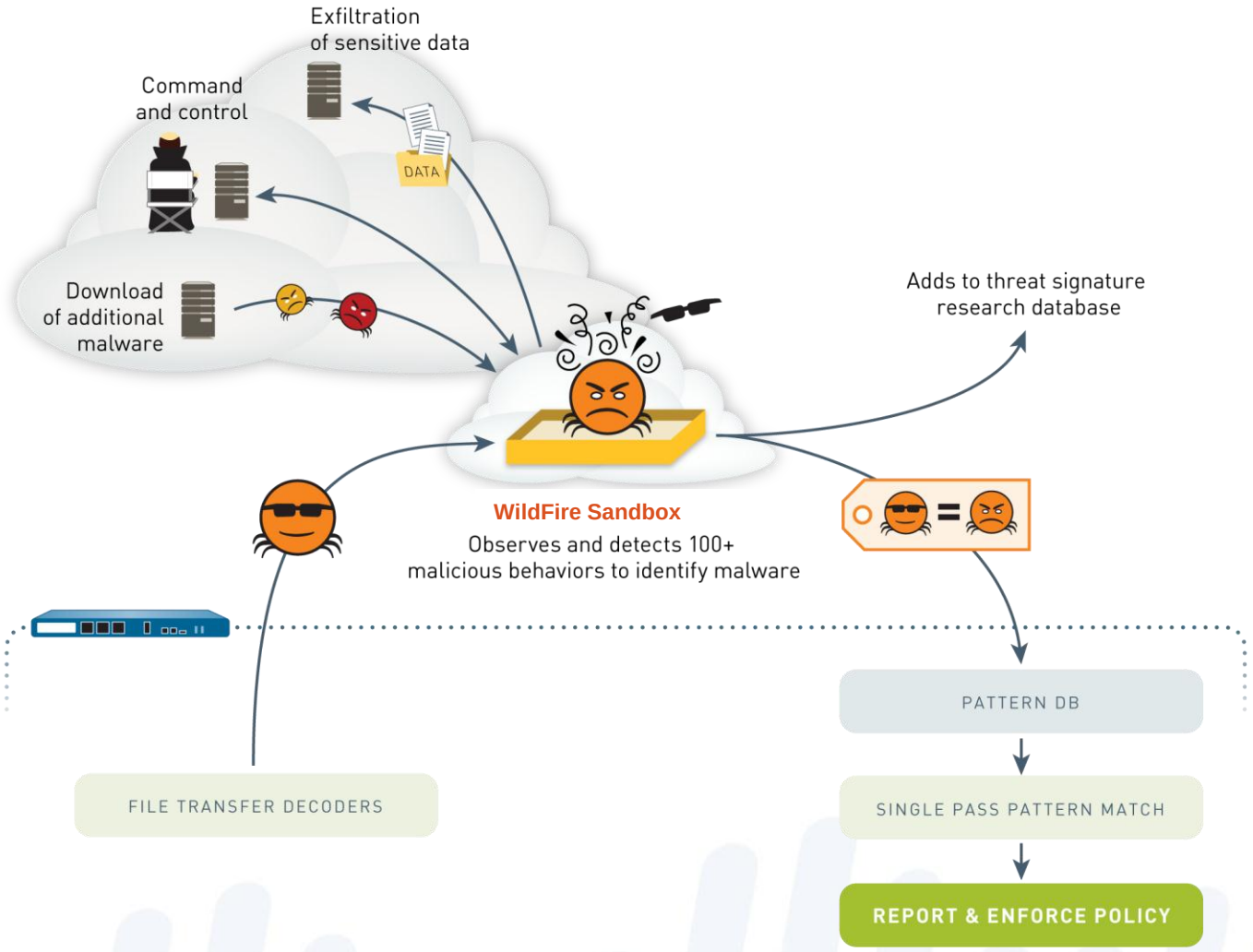
paloalto NETWORKS

安全的问题到处可见

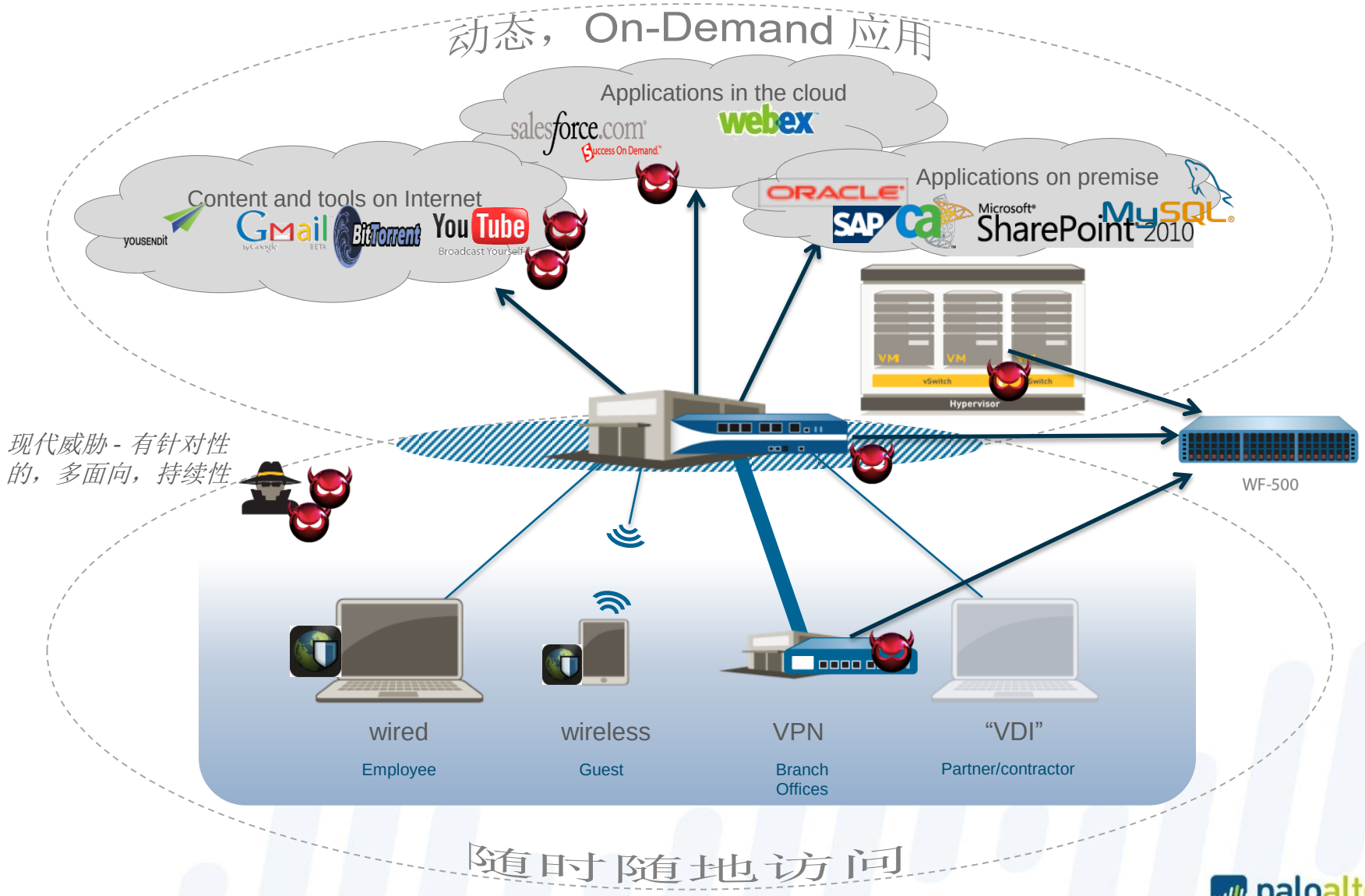


paloalto NETWORKS

我们在市场上保持领先的创新

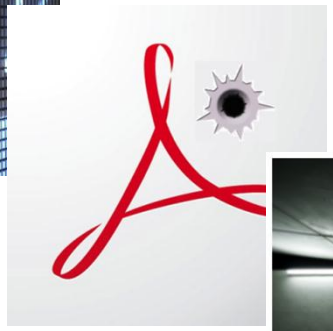


任何位置有一致的安全保护

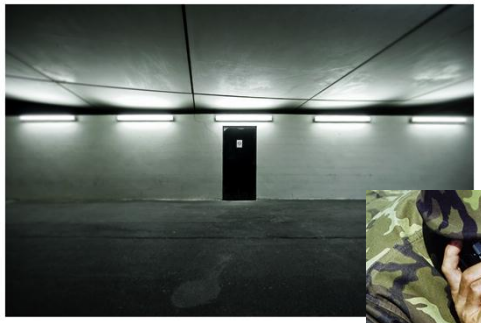


结果：单一综合平台，对付多阶段混合形攻击

诱骗



漏洞



下载

后门通道

偷盗

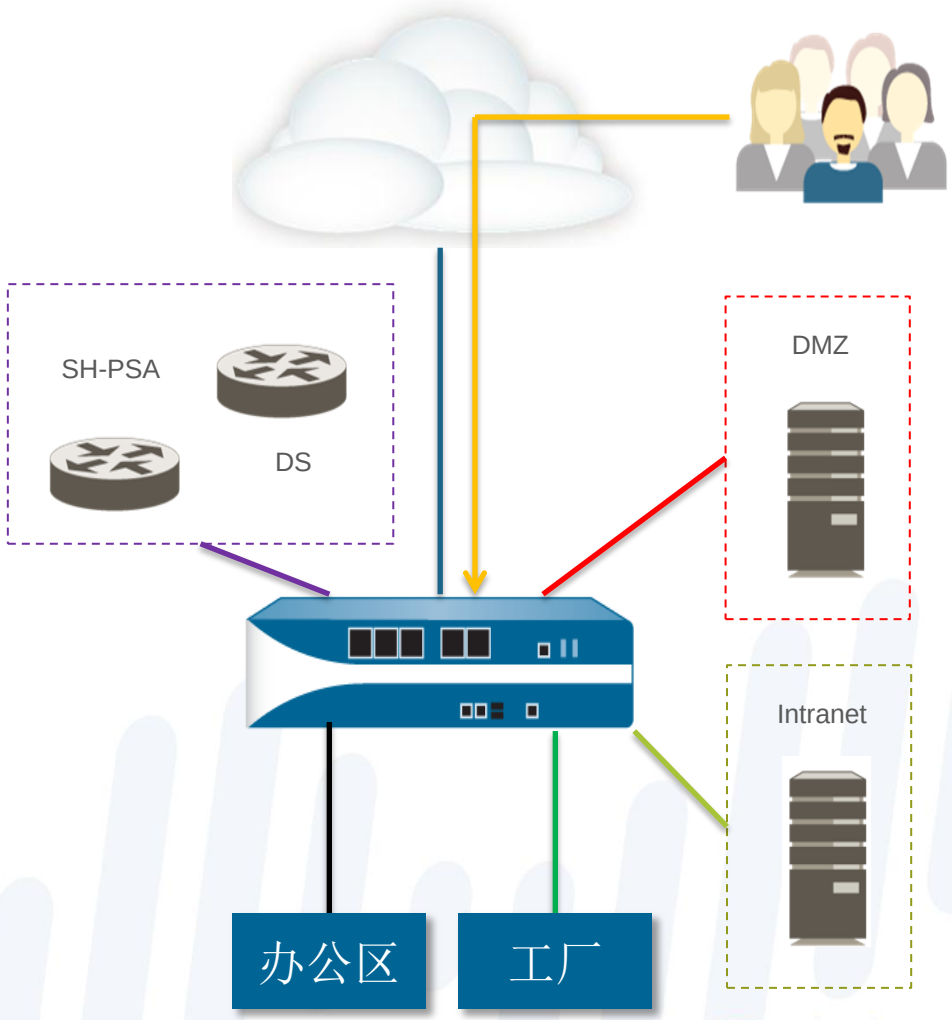
和纯沙箱，IPS，UTM差异

APT 阶段	需求	UTM	Sandbox	IPS
引诱用户	基于端口和IP的控制	✔	✗	✗
	正向控制应用程序和用户	O	✗	✗
	阻止恶意网站	✔	✗	✗
	阻止恶意域名/IP地址	✔	✗	✗
	应对未知的恶意软件阻止新的恶意网站和域名	✗	✔	✗
	新的恶意域名和网站到DNS & URL 数据库反馈	✗	✗	✗
漏洞	阻止漏洞	✗	✗	O
Malware 下载	阻止 malware	✔	O	✗
	防止 drive-by-download	✗	✗	✗
	检测 未知/ 零日恶意软件	✗	✔	✗
	零日的恶意软件到AV签名库反馈	✗	✗	✗
建立后门通道	阻止C & C 流量	✔	✗	O
	在未知的恶意软件中检测新型 C & C 流量	✗	✗	✗
	反馈新型 C & C流量到间谍软件签名库	✗	✗	✗
挖掘和偷盗信息	基于签名、来源和行为相关的智能检测阻止主动的攻击	✗	✗	✗

数据中心安全

案例分享——国内某汽车企业

- 混合部署，最大限度利用资源
- 虚拟防火墙（VSYS）隔离业务区
- 应用管控
- 用户管控
- 双向安全防护（IPS、防病毒）
- 移动办公



数据采集结果概况

- Data Lost数据泄露(22%):
文件传输可导致数据泄露

- Compliance 合规(24%):
逃避检测或传递其他应用导致合规风险

- Operational Cost运营成本(14%):
高带宽消耗等于增加成本

- Productivity(生产力 19%):
媒体应用导致降低生产力

- Business Continuity业务连续性(22%):
容易受到恶意软件和漏洞攻击的应用导致的业务连续性风险

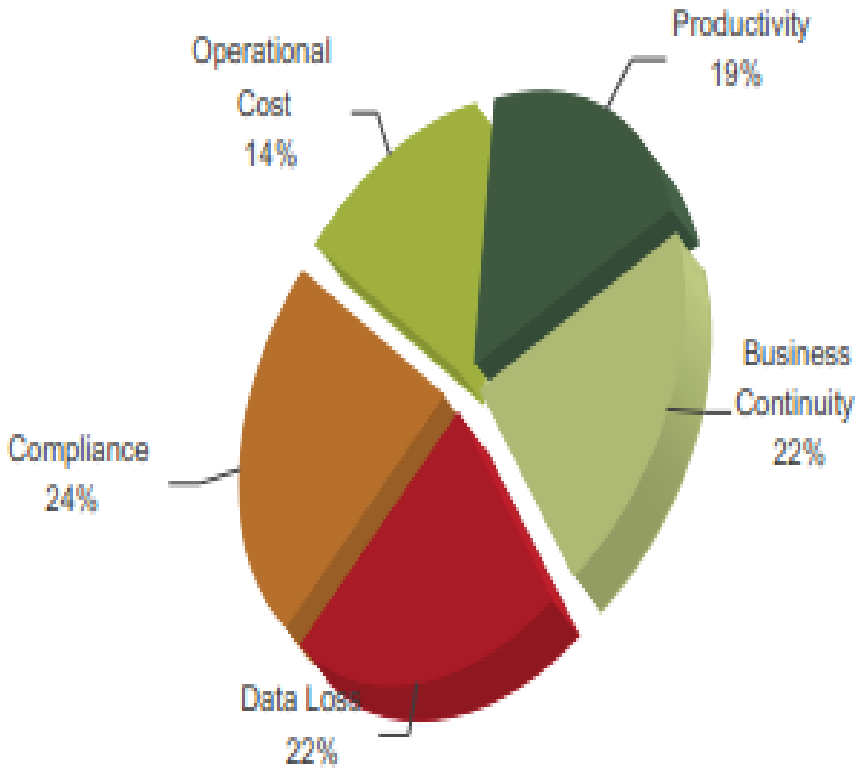


图 1：最高风险应用程序的业务风险细分

无线用户行为管理

paloalto NETWORKS
the network security company™

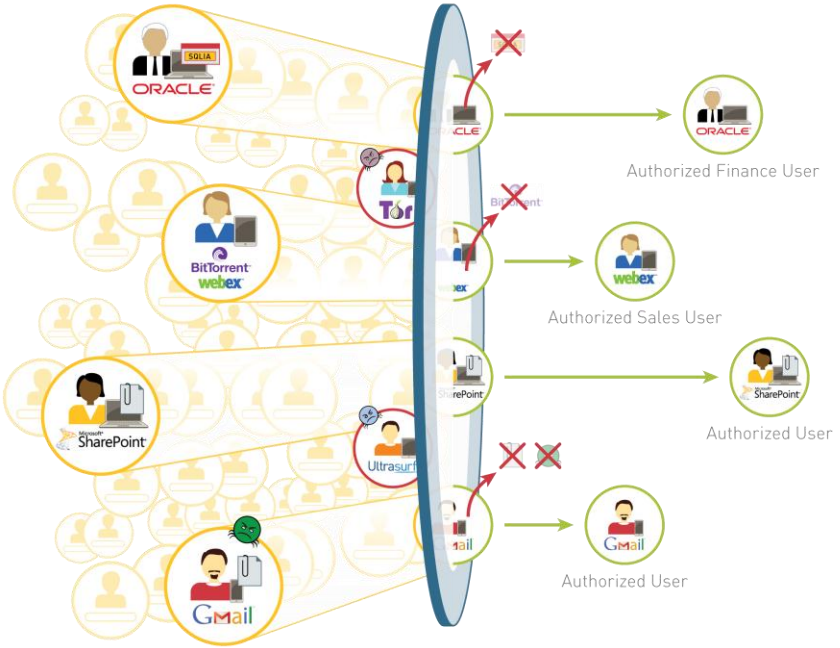
客户环境

- 趋势
  - 无线网络快速发展；
  - 需要对用户的网络访问行为进行计费；
  - 越来越多的应用系统；
  - 外联线路及合作机构增多；
  - 安全团队承担更多的管理工作；
  - 用户人数不断增加；
  - 具有多个分公司和数据中心。

- 问题
  - 对**用户行为没有**审计**和管控**；
  - **流量中有大量垃圾流量**；
  - **无法**实现对**核心服**务**器和**应**用的防**护；
  - **内部网**络**缺乏安全分割功能**；
  - **网**络设备**性能不**够。

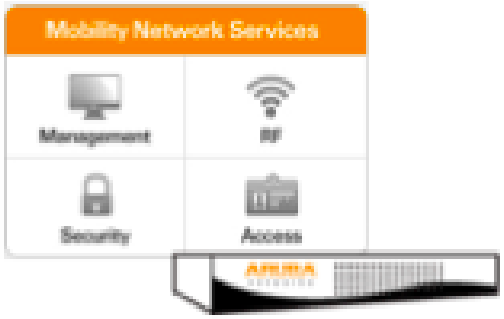
PaloAlto Networks解决方案

- User-id:多认证系统整合，实现基于用户角色的应用访问控制；
- 应用识别和管理：清理网络中的垃圾流量；
- 防止病毒的大规模爆发；
- 定位安全威胁源；
- 对用户上网行为进行规范和管理；
- 阻断针对核心服务器和站点的攻击；
- 联动第三方系统，和内部管理系统、计费系统等整合；
- 为大数据解决方案提供事件源。



PaloAlto Networks解决方案

Aruba MOVE & ClearPass



无线网络服务

- Core AAA, NAC
- Device Profiling
- Guest + BYOD

整合内容:

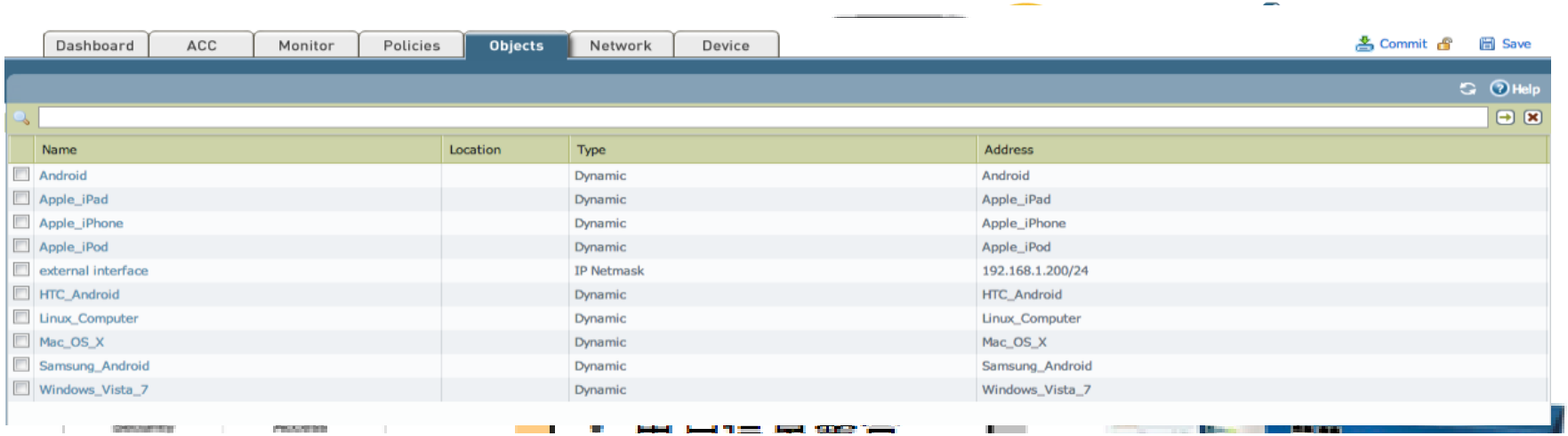
- 用户信息整合
- 灵活智能的网络访问控制
- 更好的内容安全

Palo Alto Networks

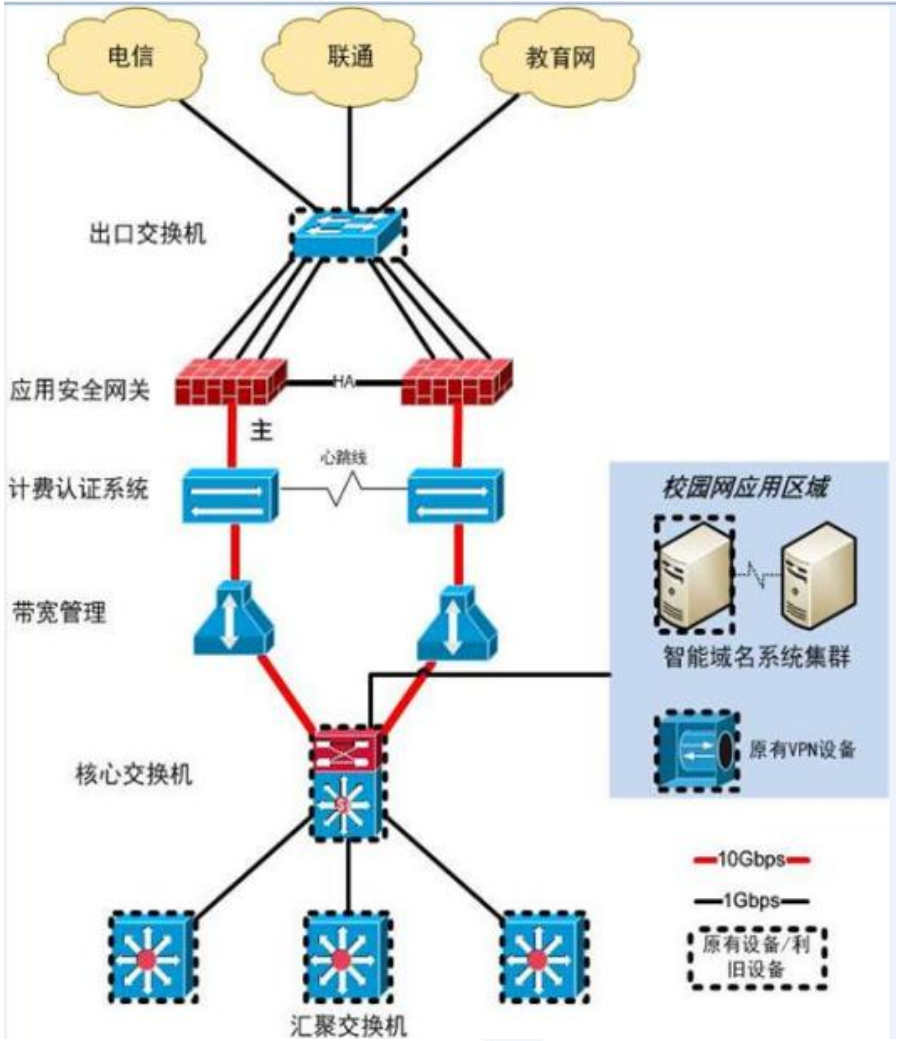
下一代安全网关

- 7层的应用识别管控
- 内容安全
- 威胁防护

PaloAlto Networks解决方案



成功应用



机遇

- 防火墙升级
- IPS，AV解决方案性能不好
- 希望整合FW+IPS+AV
- 希望对学生实现应用管控

结果

- 完整覆盖- 防火墙、应用程序控制、威胁防范
- 易于远程管理—统一安全策略

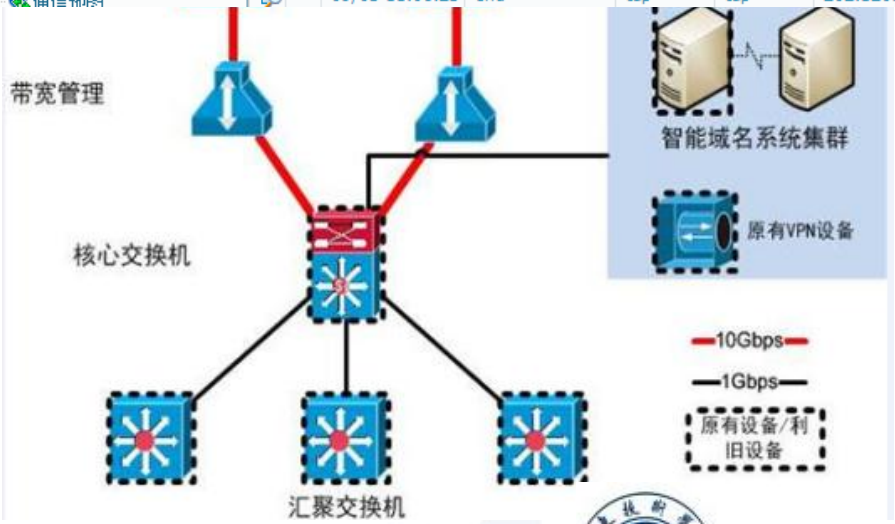
中康大学

The University of Science & Technology

Aerohive NETWORKS

paloalto NETWORKS

成功应用



- 易于远程管理—统一安全策略

ARUBA networks

Aerohive NETWORKS

中原大学

The University of Science & Technology

paloalto NETWORKS

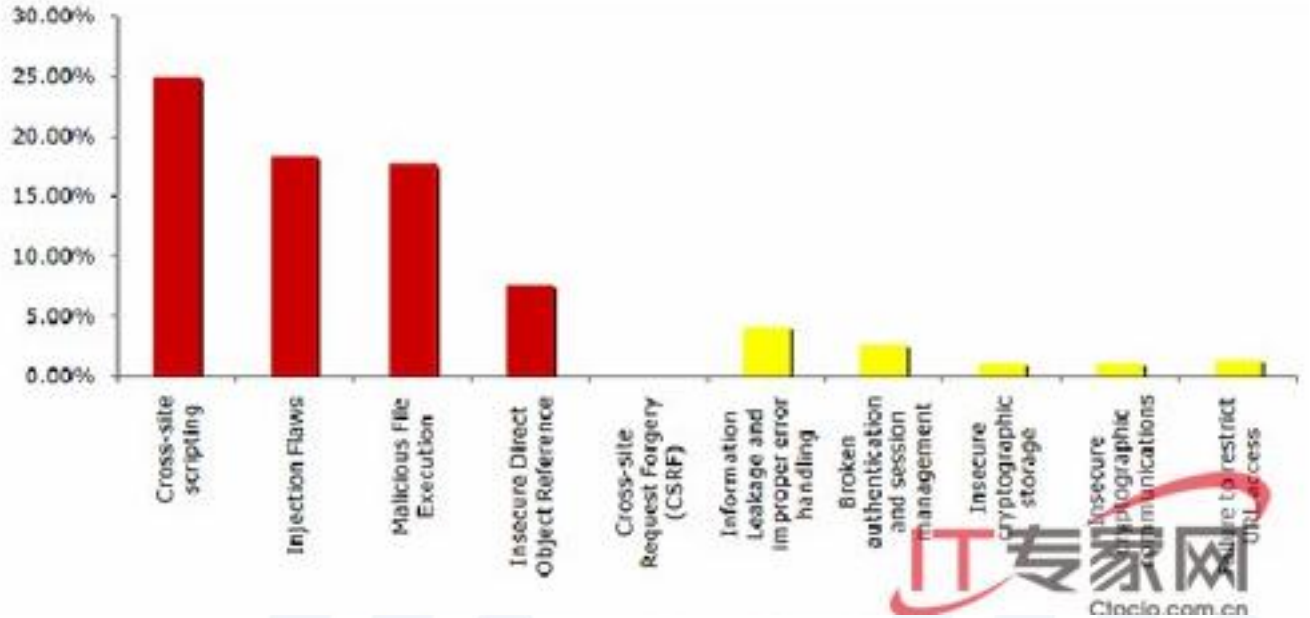
Web站点综合防御

paloalto NETWORKS
the network security company™

Web站点综合安全防御

- 趋势
  - Web站点增加；
  - 针对Web的攻击大量出现；
  - 对服务器访问行为的规范；

- 问题
  - IPS和AV解决方案影响性能；
  - 串接多台设备难以管理；
  - 针对https流量难以防御；
  - 缺乏应用识别能力；



paloalto NETWORKS

更好的Web防御解决方案

需求	Palo Alto Networks NGFW	传统 IPS
应用识别和管理	超过1800种	仅能识别很少的部分，不超过100种，误判率高
IPS特征库	超过7000	2000-7000
扫瞄SSL流量	支持双向SSL流量检测	不支持
高性能、低延迟	是	取决于开启特征库的多少
研发机构	具有全球最领先的研究团队，近三年发现大量微软和Adobe漏洞	多数情况依赖厂商的补丁信息更新特征库
功能	支持多种网络功能，部署灵活，支持NAT、Layer3、Layer2、VPN等多种功能	功能单一，仅仅支持包特征检测

paloalto NETWORKS

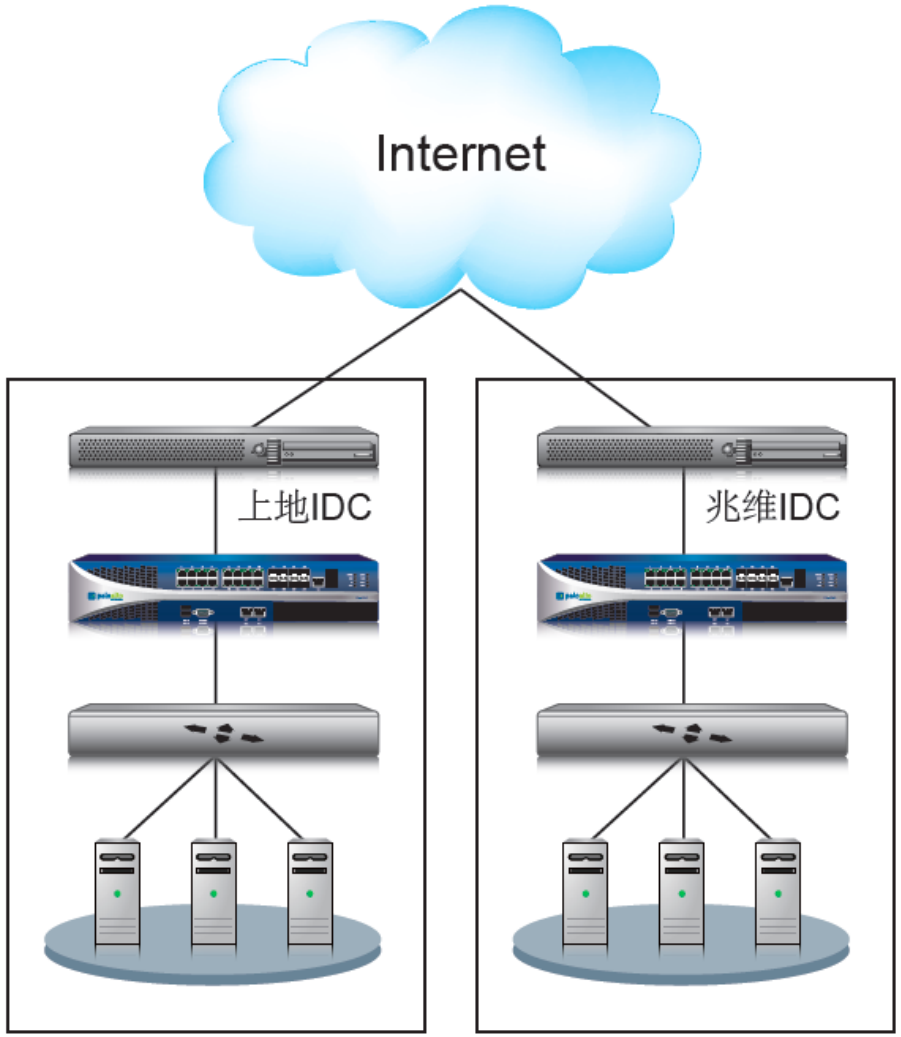
成功应用

机遇

- 用户行为管理
- 缺少安全解决方案
- 希望对营销站点进行防御

结果

- 对DMZ的Web站点进行全面防御
- 开启多数攻击阻断策略
- 保护Web站点不受病毒影响
- 实现应用识别，让管理员了解DMZ访问情况



途牛旅游网 ebay 开心网

paloalto NETWORKS

多分支企业智能组网

paloalto NETWORKS
the network security company™

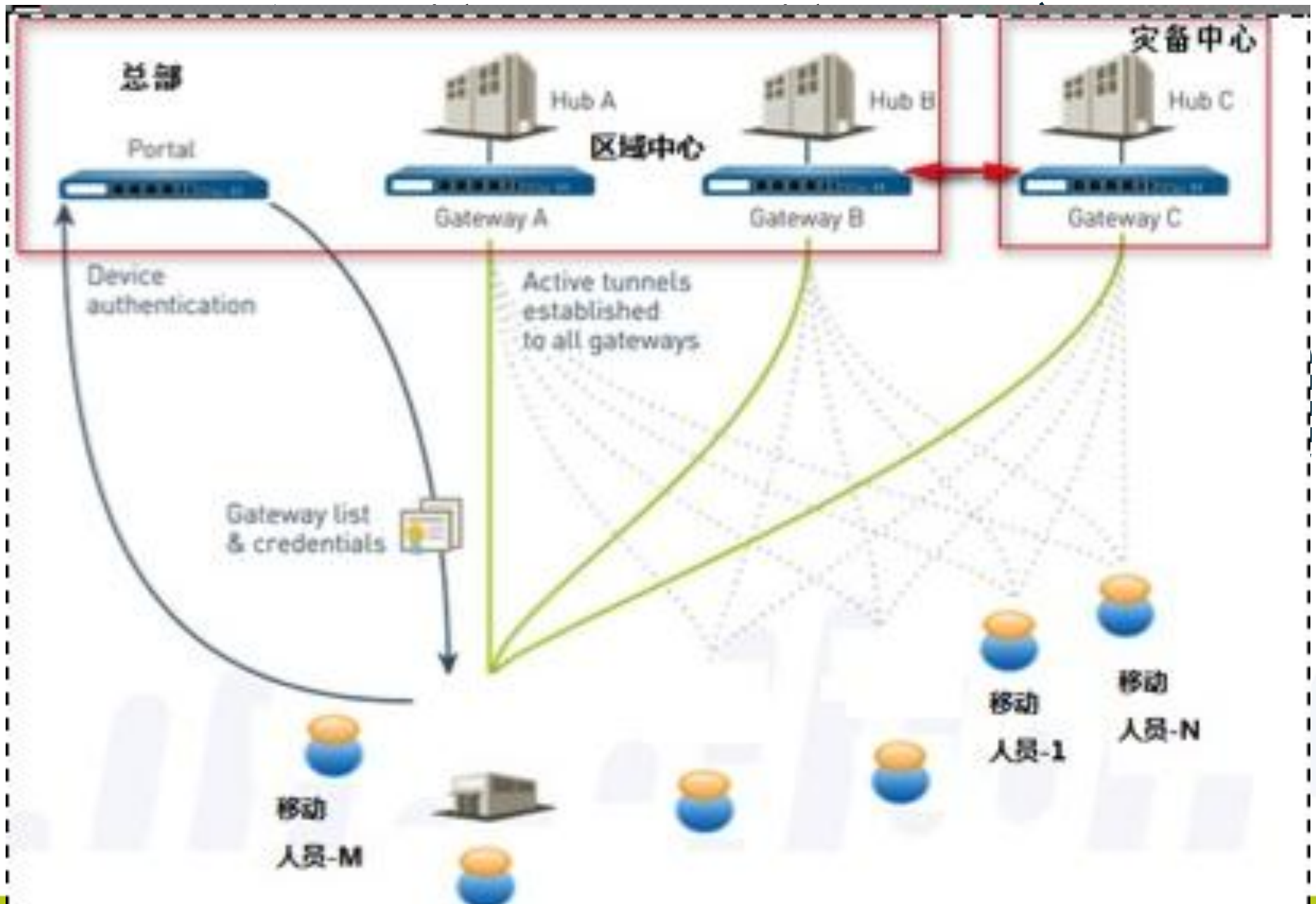
IT建设的挑战

- 分公司情况各异，要求建设简单、快速；
- 管理人员技术薄弱或无管理人员，要求维护方便；
- 如何保障分公司到总部的网络稳定和安全，数据在公网传输不被窃取；
- 数据存储到分公司终端后不被泄露；
- 分公司的IT状态实时可见且可追溯。

设计原则

- **集中管理原则**
  - 所有管理系统都放在总部；
  - 全网集中策略和报告。
- **自动化原则**
  - 可视化和自动化；
  - 自动联网，统一认证；
  - 自动阻止异常行为，定制和固定可用的应用程序。
- **合规原则**
  - 审计所有系统和应用的日志；
  - 满足相关法律法规。

客户应用


总部
Portal
Hub A
Hub B
区域中心
Gateway A
Gateway B
灾备中心
Hub C
Gateway C
Device authentication
Active tunnels established to all gateways
Gateway list & credentials
移动人员-M
移动人员-1
移动人员-N

三层架构部署描述

- **总部数据中心**

部署采用PA设备，用于与互联网、分公司的网络连接（VPN或专线）和边界隔离，启用网络访问管理及安全防护策略，确保总部的高安全性、高稳定性。

- **各个分公司**

部署采用PA设备，用于与总部之间、分公司的网络连接（VPN）和边界隔离，可接受区域内的移动终端的VPN互联请求，各分公司之间形成互为备份。

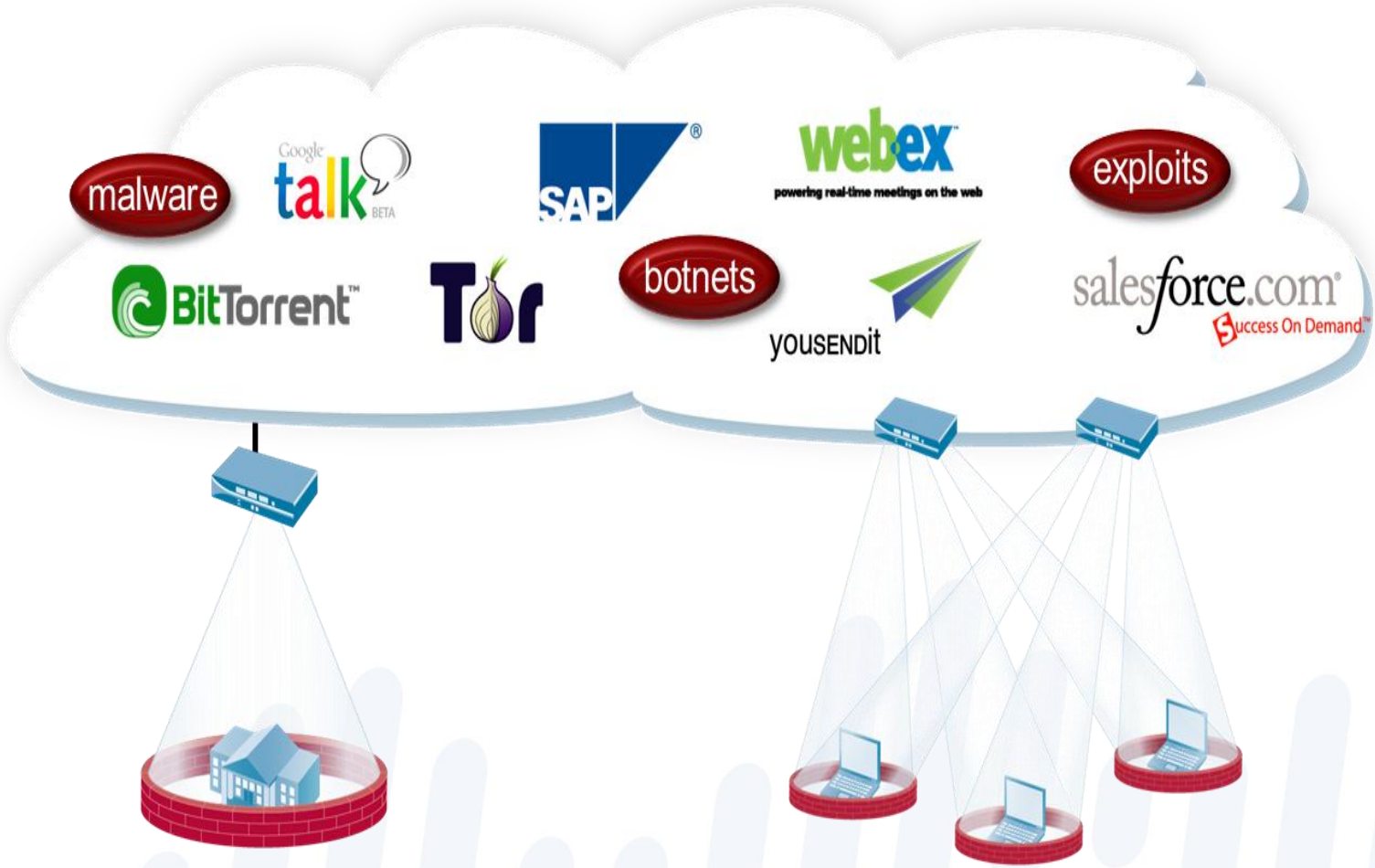
- **移动办公人员**

移动办公人员的电脑和智能终端设备上安装PaloAlto的VPN客户端软件，随时随地可以与所有分公司或者总部的PaloAlto网关设备连接，并访问内部资源。

分布式部署、多样化接入

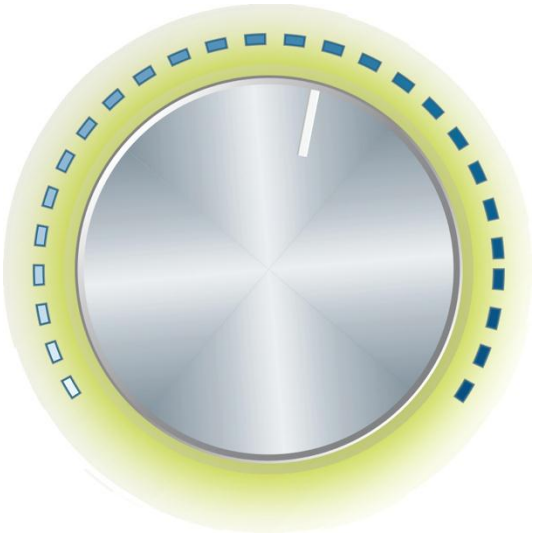
Deloitte.

案例分享：



paloalto NETWORKS

对比



允许特定用户　　只允许某些功能

“允许”并
流量整形（QoS）

允许并扫描
敏感数据

允许并扫描威胁？

允许并限制
访问时间

允许所有　　阻止所有

Palo Alto Networks 带来新一代应对方式！！

小结

Palo Alto Networks 为企业提供全面的网络安全、应用安全、用户安全解决方案，帮助企业提高安全管理效率，尽可能降低企业面临安全威胁的风险和几率。

Palo Alto Networks为企业提供全新的安全价值：

1. 全网流量及应用可视化
2. 全流量威胁防护
3. 基于用户、应用的策略管控
4. 多途径安全接入
5. 集中统一的安全管理

谢谢!

paloalto
NETWORKS
the network security company℠