

Blue Coat

高速 的- 安全的 - 可管理的互联网应用



内容提要

- BlueCoat公司介绍
- 互联网访问面临的问题
- BlueCoat SG解决方案
- BlueCoat SG特色应用
- BlueCoat SG产品介绍
- BlueCoat SG案例分析

关于Blue Coat

- 成立于1996年，致力于网络加速
 - 加速Web应用...使互联网应用更快
 - 创新的Proxy缓存专用设备，具有并发抓取、动态缓存内容刷新等
- 2002年延伸到策略控制和安全领域
 - 丰富的策略框架，具有高性能的引擎，对用户、内容和应用具有可见和控制
 - 可见：谁，做什么，在什么地方，什么时间，如何
 - 控制：加速，拒绝，限制，扫描，剥除，转换...
- 安全的内容和应用传递市场领导者
 - 500+员工;
 - 30,000+ 专用设备
 - 全球 4,000用户
 - 在安全的内容和应用传递市场#1 (IDC)

加速和安全的集成解决方案

全球主要机构信任 Blue Coat

Financial Services



Health & Pharmaceuticals



Energy, Oil & Gas



Mfg/Industrial



Consumer & Retail



Government



中国主要的机构信赖BlueCoat

Financial

Health & Pharmaceuticals

并且每个季度增加
350 + 新用户
!!!

Energy, Oil & Gas

Mfg/Industrial

telecommunication

 中国石油天然气股份有限公司
PetroChina Company Limited

 中国石油化工股份有限公司
CHINA PETROLEUM & CHEMICAL CORPORATION



 神龙汽车
DONGFENG-CITROËN

 江铃汽车

 中国银行
BANK OF CHINA

 上海银行
Bank of Shanghai

 中国进出口银行
THE EXPORT-IMPORT BANK OF CHINA

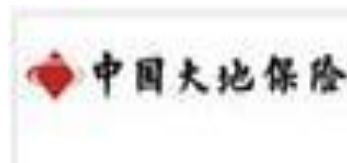
 国家开发银行
China Development Bank

 中国建设银行
China Construction Bank

 交通银行
BANK OF COMMUNICATIONS

 中远集团

 平安人寿
PING AN LIFE

 中国大地保险

 AMERICAN INTERNATIONAL ASSURANCE
EVERLASTING
AIA

 平安集团

 信诚
人类保险
聆听所至 信诚所在

 中国电信
CHINA TELECOM

 CNC
中国网通

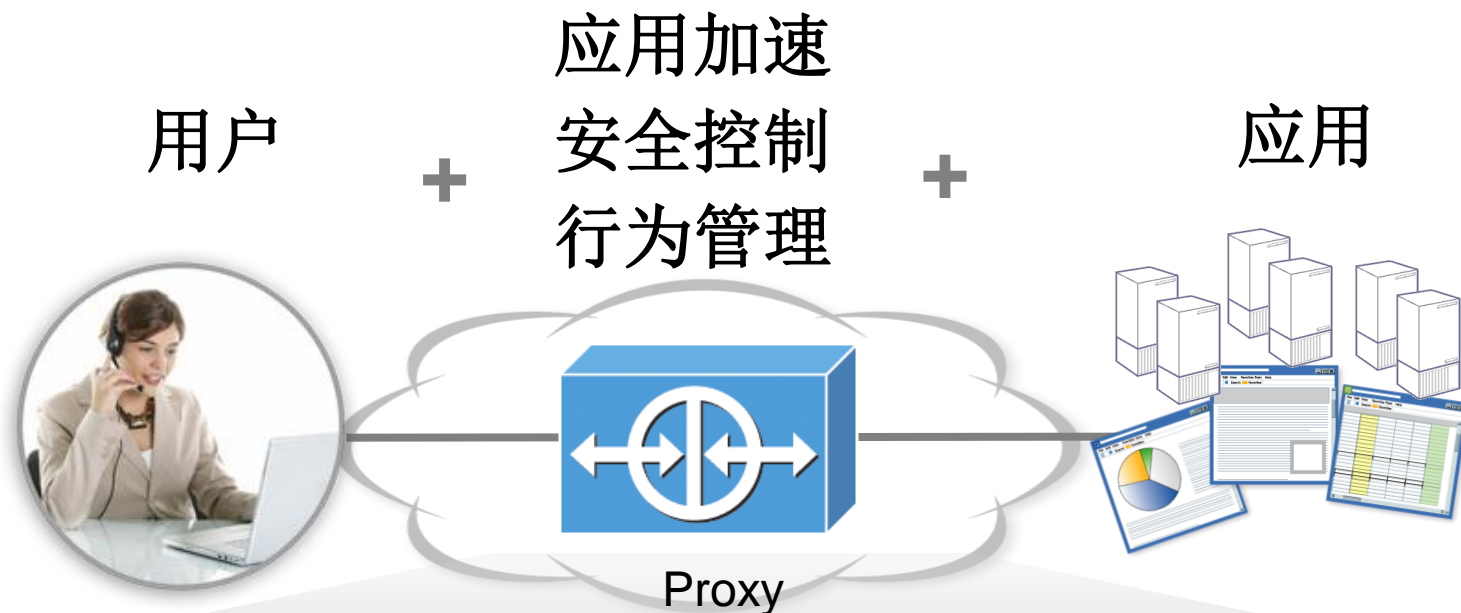
 China unicom 中国联通

 中国移动通信
CHINA MOBILE
移动通信专家

互联网访问面临的问题...

- 多数用户抱怨上网速度慢，为什么？
 - 没有缓存，热门的内容频繁重复下载，降低带宽利用率；
 - 不适当使用，没有控制如流媒体/P2P下载等带宽消耗大的应用，占用了大量带宽；
 - 恶意应用偷偷地消耗了网络连接和带宽，如病毒程序，间谍软件（包括流氓软件、木马）等；
- 应用层安全管理缺乏手段
 - 通常会部署桌面/服务器/邮件防病毒系统，但对于文件下载/隐藏在网页中恶意代码/Web Mail中病毒威胁怎么办？
 - 面对频繁的恶意间谍软件、流氓软件、木马程序感染，有高效的控制手段吗？
 - 面对对企业机密信息外泄，如何控制？
- 上网行为管理工具缺乏
 - 传统的管理工具多数是基于IP地址的，无法识别用户/用户组等应用层用户特征，对于规模稍大的网络灵活性不足；
 - 一般的工具多基于端口进行应用控制，对于那些自动选择端口的应用如Skype/BT等，就束手无策了；
 - 无法在应用层进行带宽管理，保证关键应用的带宽，限制一班应用或者恶意应用程序的带宽，制定访问优先级策略；

BlueCoat SG解决方案 – 概述



全部协议终结 = 全部可见 & 控制策略
(HTTP, SSL, IM, Streaming, P2P, SOCKS, FTP, CIFS, MAPI, Telnet, DNS)

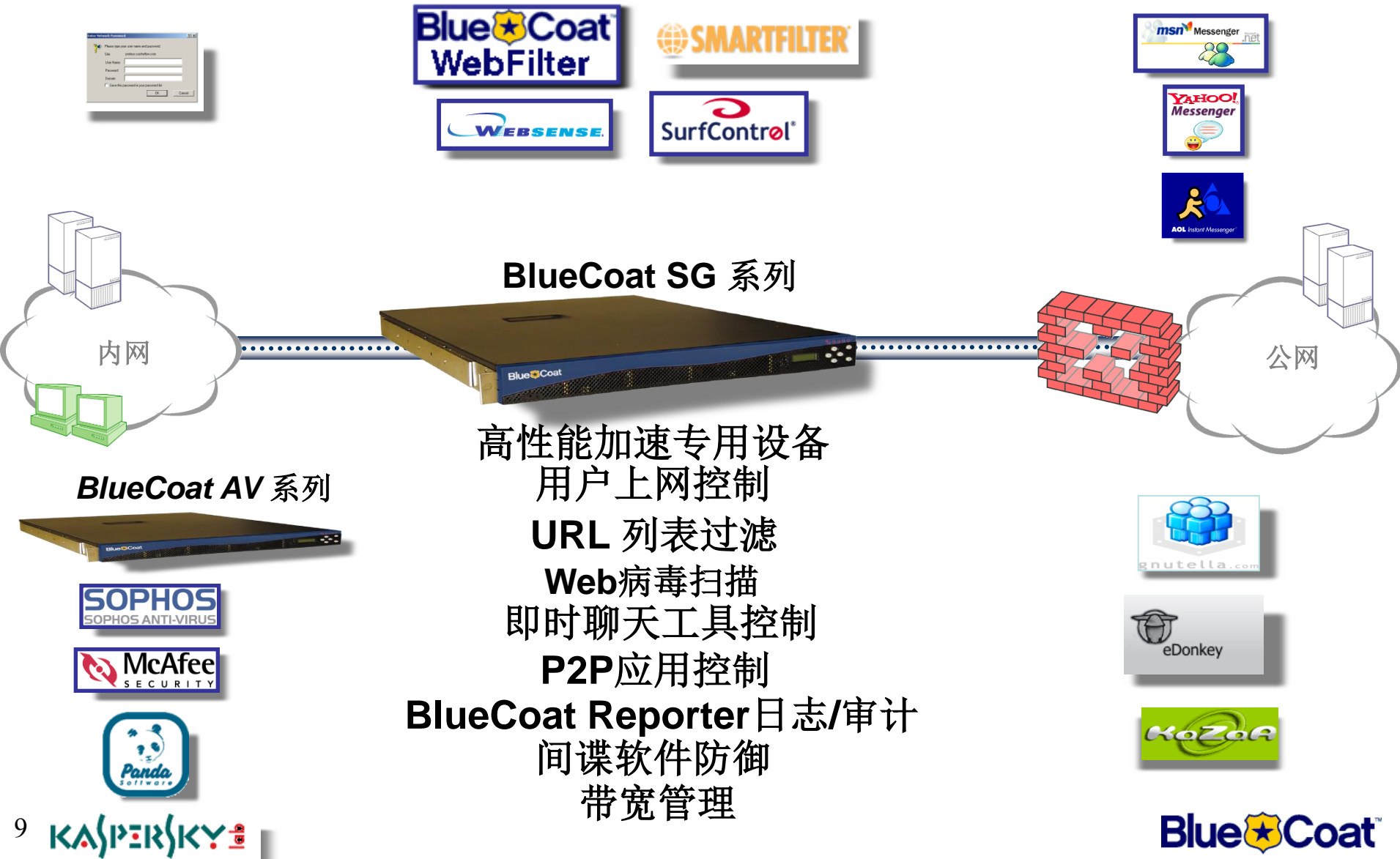
BlueCoat Secure Proxy Appliance

BlueCoat 安全代理专用设备

BlueCoat SG解决方案 – 逻辑功能示意



BlueCoat SG解决方案 – 功能解释



BlueCoat SG解决方案 – 专用设备全系列

企业总部

RA810 系列SSL VPN



SG8100 系列



RA510 系列SSL VPN



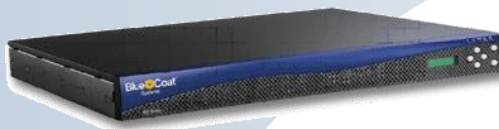
SG810 系列



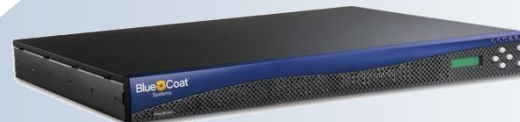
AV810 系列病毒网关



SG510 系列



AV510 系列病毒网关



分支机构

SG200 系列



并发用户	最多100用户	100-500用户	500-2000用户	2000 – 10,000+ 用户
吞吐量	最多 10Mbps	10M-60Mbps	60M – 150Mbps	150M – 400+ Mbps

性能参考

应用1 认证、授权和统计

- 用户认证

与LDAP、Radius和NTLM等认证系统协同工作进行认证。认证方式可以基于单个用户、基于组成员（多个用户组成的组）以及基于网络标识（IP地址、子网地址或其他网络标识等）

- 授权

自定义的策略规则成为授权的潜规则。Visual Policy Manager(VPM) 提供策略制定工具。

- 统计

提供用户相信的网络访问信息，方便公司调看。

应用2: Proxy代理 服务

- Proxy支持
 - HTTP, HTTPS, FTP, Telnet, SOCKS, DNS, IM (AOL, MSN, Yahoo!), TCP-Tunnel, MMS, RTSP, QuickTime
 - 高性能缓存, 提高访问速度, 节省带宽;
- IM (聊天) 控制, P2P屏蔽, 广告屏蔽, 能识别应用级协议, 而不是根据端口进行控制;
- 流媒体控制, 能实现缓存, 控制, 拆分等;
- 能根据用户与应用为条件制定灵活的带宽管理策略, 确保关键应用带宽, 限制或屏蔽部分应用带宽, 如BT/FTP;

应用 3: 内容过滤



- BlueCoat WebFilter 网站分类列表数据库
 - 具有超过50个分类, 1500万条URL纪录, 每天自动更新;
 - 独特的DRTR动态网站分类技术, 能自动归类动态内容和新的URL;
 - 支持第三方的分裂列表如Webesesnse, SmartFilter等;
- ProxySG 是内容过滤的高性能平台
 - SGOS 在运行URL解决方案是具有10倍与通用操作系统平台
 - 专用的Blue Coat对象存储优化了过滤性能
 - 通过缓存保证内容的快速提交
- 建议、指导和强制等高粒度策略能够控制到用户级
 - 支持过滤数据库以外的自定义分类
 - 定义allow/deny列表、跨越和例外
 - 自定义的认证、告警、提示页面
 - 在各种环境中提供对用户ID的透明认证

应用4：网关防御“间谍软件”



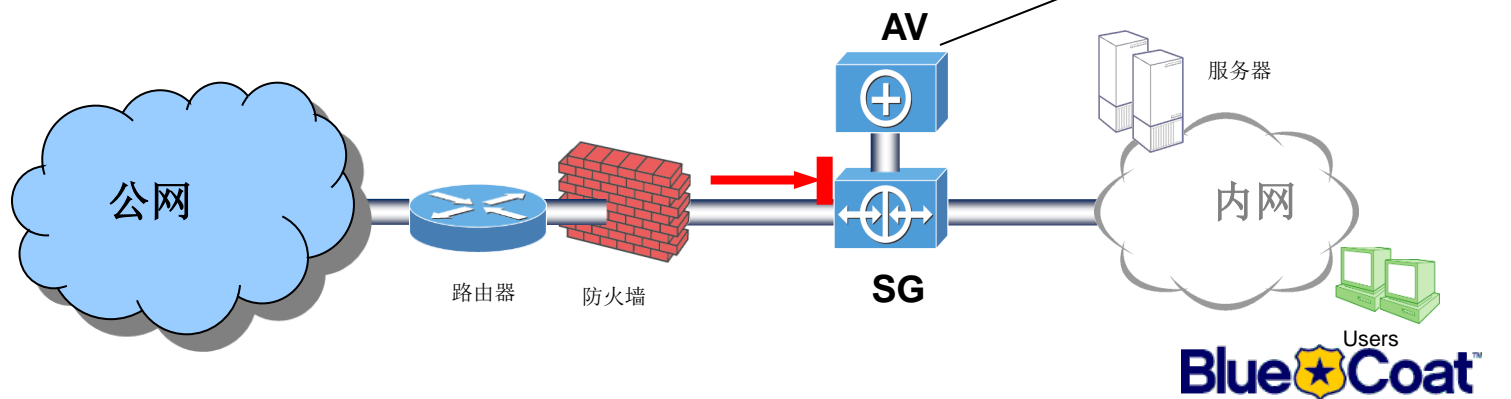
- 防御新的和未知的“间谍软件”
 - 阻止从已知或可疑的“间谍软件”站点的所有下载
 - 揭开“间谍软件”执行文件的后缀伪装
- 定位被感染的PCs
 - 屏蔽“间谍软件”“calling home”
 - 保护私人信息，提示IT人员
- 允许合法的内容
 - 允许授权的驱动式安装
 - 允许安全地访问“间谍软件”站点，以满足业务需要

应用5：提供快速的Web病毒扫描

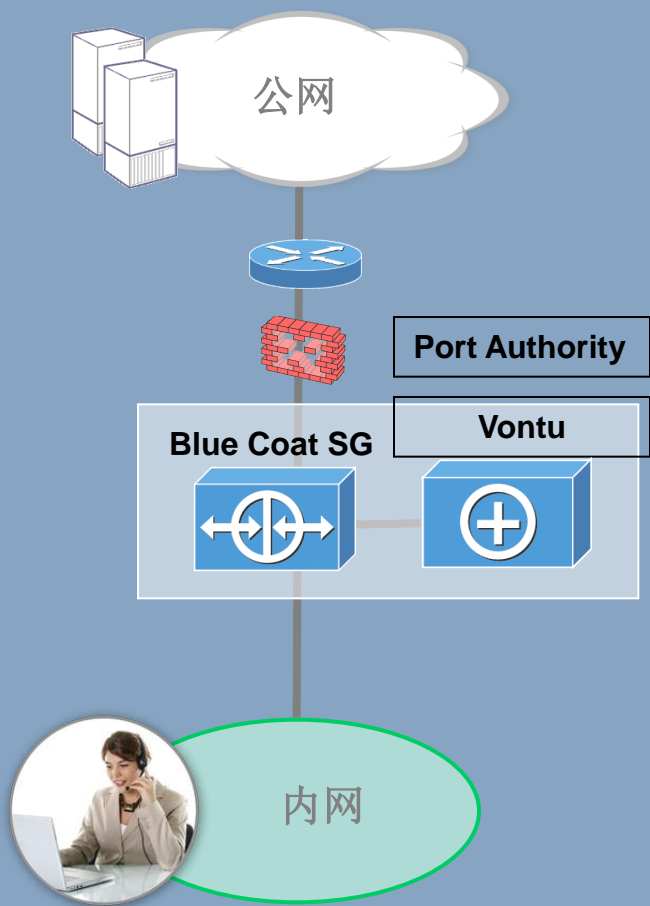
- BlueCoat AV510/810专用的Web病毒扫描专用设备
 - 选择AV引擎，能够进行自动更新
 - 与 Blue Coat SG集成，可扩展和高性能
- 扫描HTTP, HTTPS 和 FTP协议
 - “扫描一次、服务多次”，得益于缓存
 - 启发式指纹缓存，为不能缓存的Web对象提供性能增益
 - 关闭Web Email带来的病毒和木马下载的后门

Integrated AV Scan

缓存智能，实现一次扫描，多次服务，病毒库更新将同步更新缓存内容



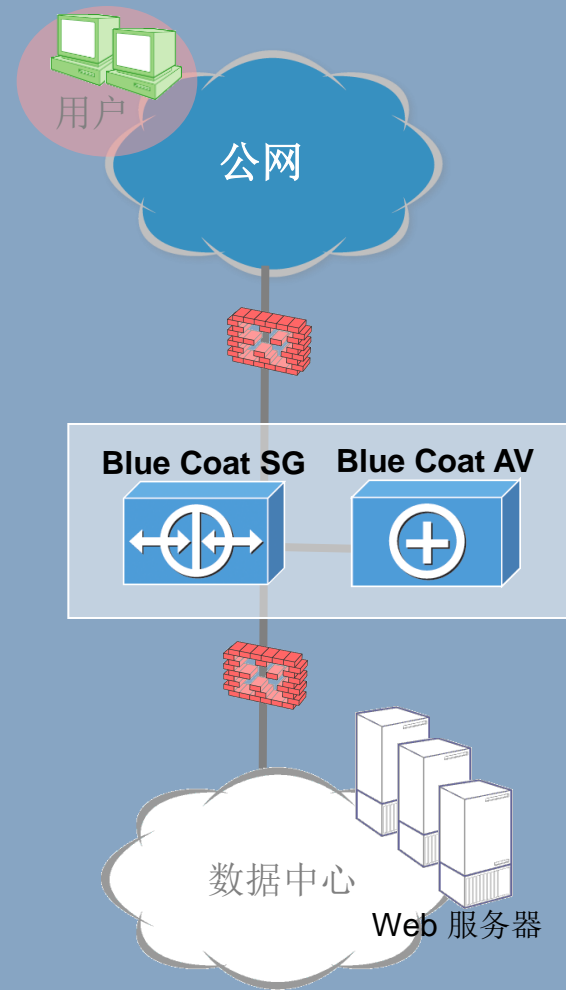
应用6：防止机密数据外泄



- 屏蔽出网的“间谍软件”
- 对IM、P2P和流媒体实施方法级控制
- 与“数据丢失保护”合作厂家集成
 - 监控/屏蔽带有敏感信息的通讯
 - 提供对HTTP、HTTPS和FTP的可见和控制
 - 集成先进的防泄密功能

应用7：数据中心-反向代理

- 保护Web服务器
 - 控制对Web服务器的访问
 - 对上传文件进行病毒扫描
 - 保护数据的保密和安全
- 加速Web内容
 - 处理高峰或瞬间通讯
 - 处理动态和静态内容
 - 减少Web服务器的SSL处理的负载
- 简化操作
 - 可扩展的、优化的专用设备
 - 性价比超过Web服务器



竞争分析

- **MicroSoft - ISA Server**
 - 运行在通用操作系统上的软件，作为网关设备，在安全性、性能方面都欠缺，通常用于中小企业网络环境；
- **Network Appliance - NetCache**
 - 专用设备，强调大容量缓存，在安全策略控制方面不够全面，需要借助第三方报表工具进行日志分析，多用于流媒体/CDN；
- **Cisco – Content Engine (ACSN)**
 - 专用设备，强调缓存功能，安全控制策略较弱，多用于流媒体/CDN；

BlueCoat SG——产品全系列

企业总部

RA810 系列SSL VPN



SG8100 系列



RA510 系列SSL VPN



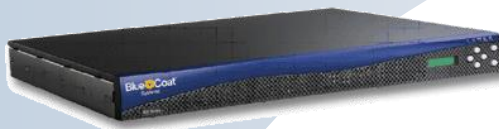
SG810 系列



AV810 系列病毒网关



SG510 系列



AV510 系列病毒网关



分支机构

SG200 系列



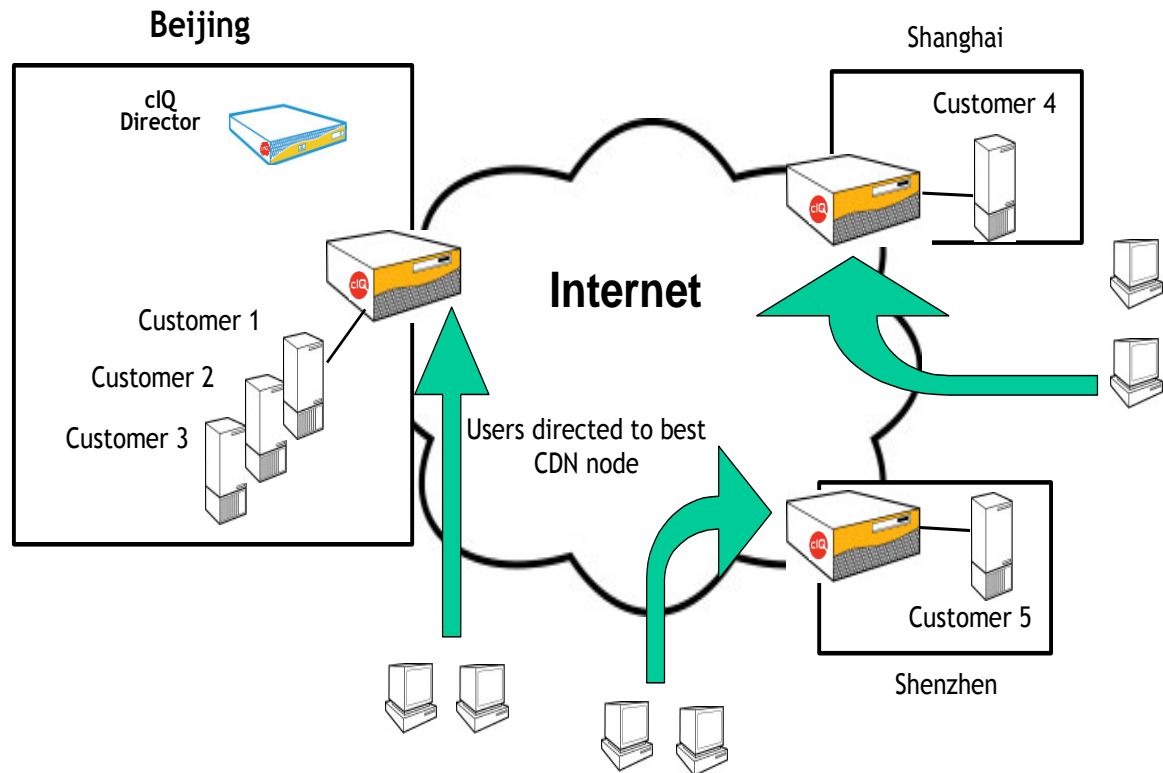
并发用户	最多100用户	100-500用户	500-2000用户	2000 – 10,000+ 用户
吞吐量	最多 10Mbps	10M-60Mbps	60M – 150Mbps	150M – 400+ Mbps

性能参考

案例一 ChinaCache

- China Cache是目前中国最大的CDN 运营商，其当前的运营目标是能够为ICP提供内容分发到中国的50个大中城市。China Cache为其用户提供的服务包括更低的带宽收费、降低Web Server负载、提供最终用户的响应时间
- 以较低成本提供高回报的内容分发服务
- 提高带宽增益比率
- 提供具有竞争力的特色
- 具有开发创新产品和服务所要求的能力
- 采用可靠的和可管理的方案
- 技术支持复杂程度最低化
- 业务运营操作自动化
- 用户服务自动化
- 保证用户的内容保持最新
- 为尽快投入运营，系统要利用现有的网络基础设施；
- 不需改变最终用户的机器设置和配置

案例一 ChinaCache



案例一 ChinaCache

- 实现方式:

- 1、在全国主要城市部署Blue Coat的缓存及安全专用设备（正向加速器）
- 2、采用L4 GSLB完成用户请求的转向到最近的加速器
- 3、安装Director在需要的时候将要求的内容分发到要求的加速器上
- 4、跟踪内容服务记录用于对ICP收费

- 项目实施结果

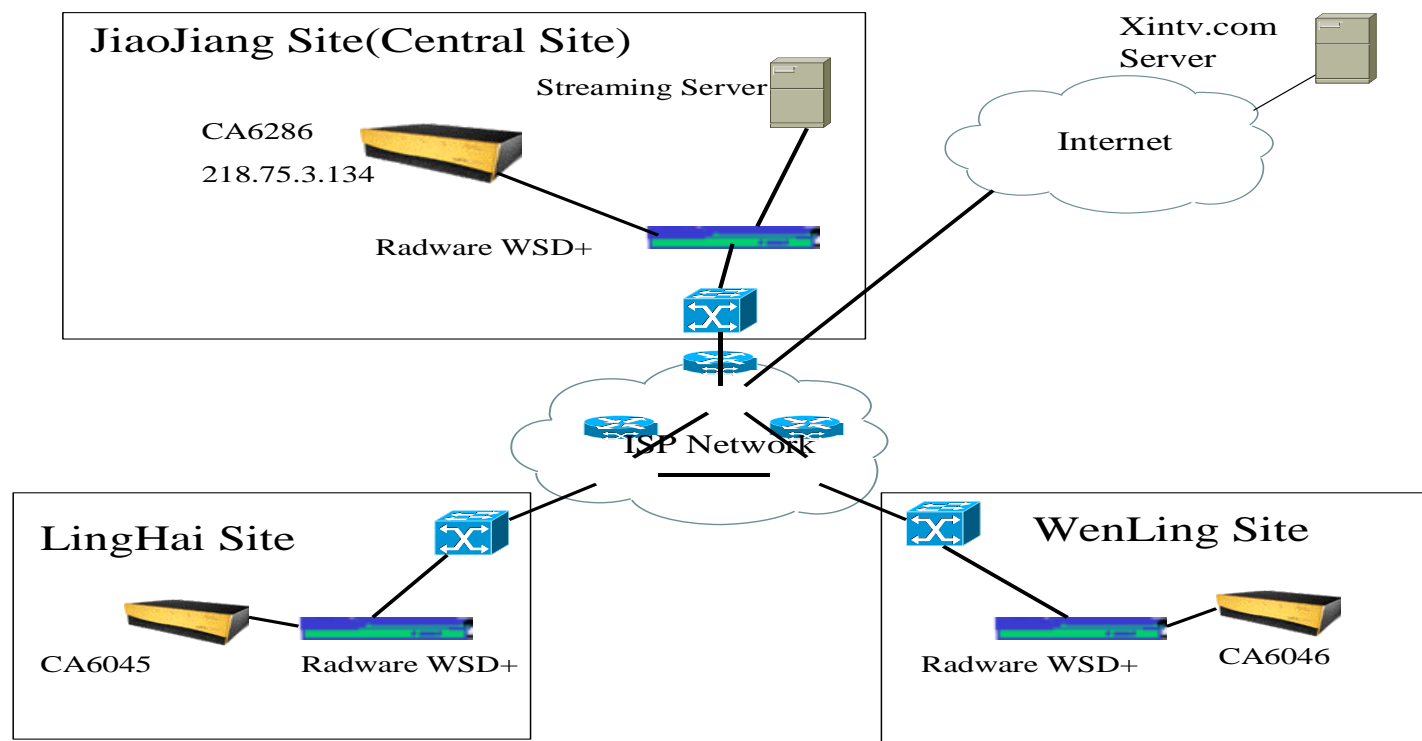
- 1、快速实现了内容分发服务
- 2、节省了带宽利用和费用
- 3、维护极低的专用设备使总体拥有成本（TCO）最低
- 4、灵活的体系结构允许China Cache不断定制自己的服务，提高竞争特色
- 5、Director可以让每个内容提供商同步和管理他们自己的内容
- 6、提供HTTP、MMS、Real Streaming等各种类型的服务

案例二 浙江台州电信流媒体CDN

- 业务需求:

- 1、台州电信作为当地主要的电信运营商，为开展宽带业务，吸引宽带用户上网，在其网络中提供宽带流媒体服务
- 2、利用现有网络基础，减少流媒体服务对全网的影响
- 3、支持1G以上的流媒体吞吐

案例二 浙江台州电信流媒体CDN



案例二 浙江台州电信流媒体CDN

- 实现方式:

- 1、通过三台CA6xxx高速缓存在全网建立Streaming CDN
- 2、通过Radware四层交换机和Viewtoo的CDN管理软件实现用户的就近访问，内容的分发等功能
- 3、各节点缓存设备提供MMS Streaming服务
- 4、内容分发采用HTTP线速分发和用户访问后缓存相结合的方式

- 项目实施结果

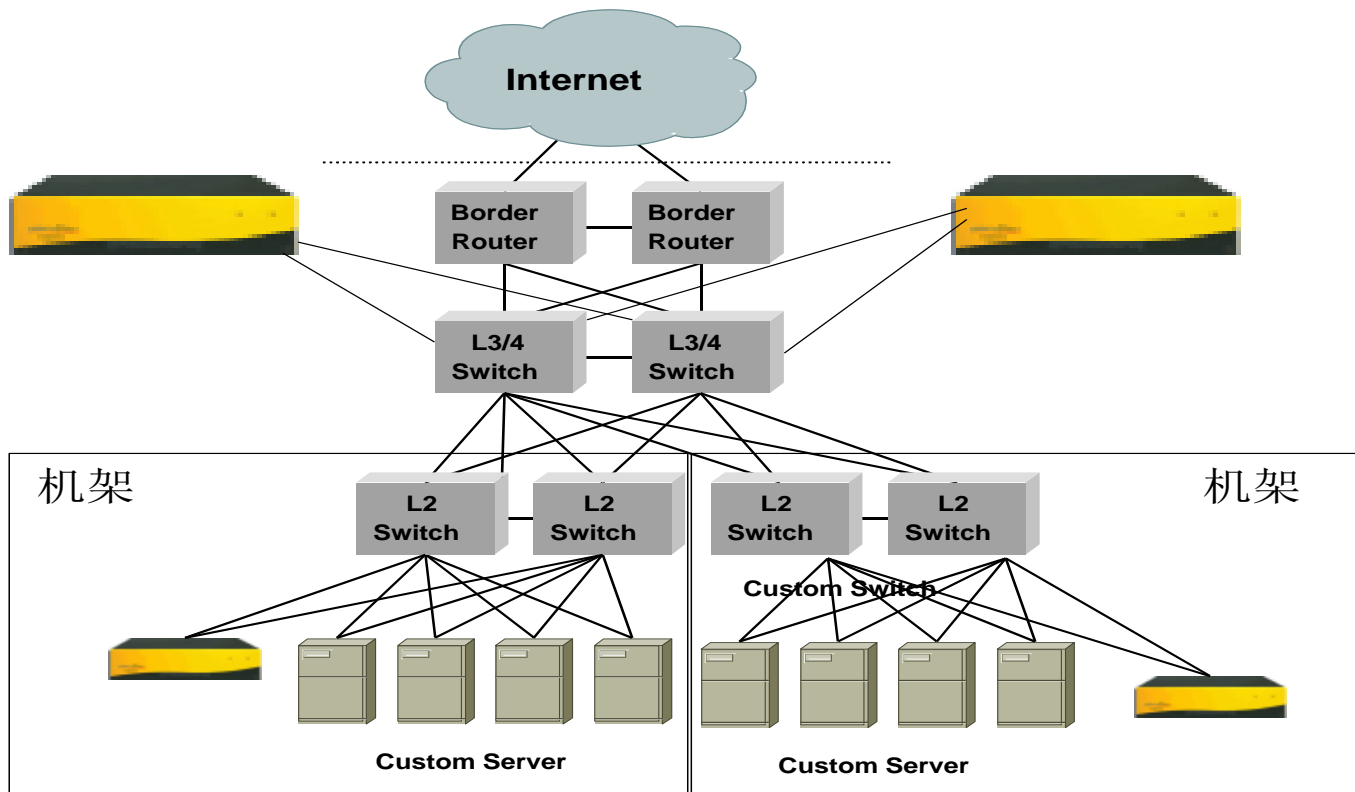
- 1、快速实施了streaming CDN系统
- 2、提供高带宽、高质量的streaming服务
- 3、整体流量超过1Gbps
- 4、有效促进了宽带业务的开展

案例三 北京263IDC机房

业务需求

- 北京263IDC是国内主要的互联网信息中心之一，为ICP和企业提供主机托管、带宽服务、数据服务等多种服务业务；在北京、上海、广州等地设有IDC机房。
- 为ICP及企业用户提供更多增长服务，包括：Web服务器加速，互联网内容的异地分布服务、减轻防火墙负载服务、虚拟主机托管服务等。
- 采用可靠的和可管理的方案
- 技术支持复杂程度最低化
- 业务运营操作自动化
- 用户服务自动化
- 为尽快投入运营，系统要利用现有的网络基础设施；

案例三 北京263 IDC机房



案例三 北京263IDC机房

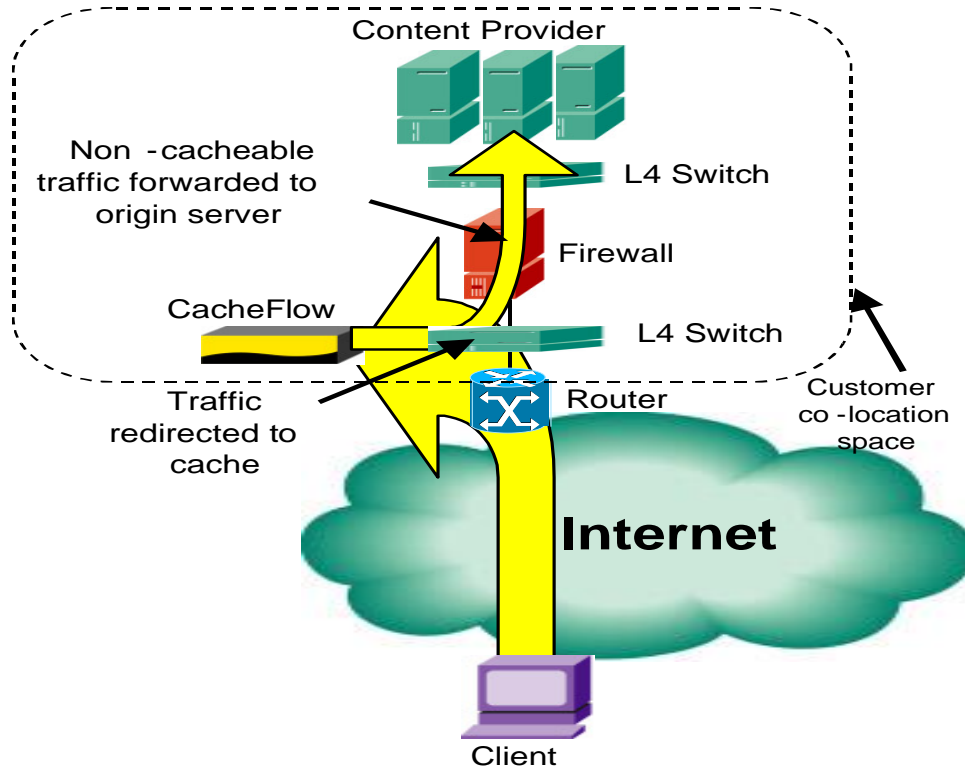
- 实现方式：
 - 在IDC出口配备两台高端Blue Coat缓存专用设备，为IDC内所有托管主机提供缓存加速，并提供虚拟主机托管业务
 - 通过在加速区内的机架中的中、低挡缓存专用设备，根据ICP用户选购的服务，为指定Web服务其提供加速服务
 - 出口处高速缓存还为异地IDC中心的Web服务器提供异地内容分发服务
- 项目实施结果
 - 快速实现了IDC的增值服务，拓宽业务范围
 - 维护极低的专用设备使总体拥有成本（TCO）最低

案例四 Sohu.com

业务需求

- Sohu.com是国内大型网站之一，日点击量上千万次，由超过100台服务器提供内容服务
- 巨大的访问量对服务器系统产生巨大的压力，需对Web服务器的处理能力进行扩展
- 大量的服务器给管理代理很大压力，包括：内容的同步，负载的均衡，日常维护等，并且占用很大的机架空间
- 要求一种高效的Web服务器扩展手段，管理简便、维护工作量小等

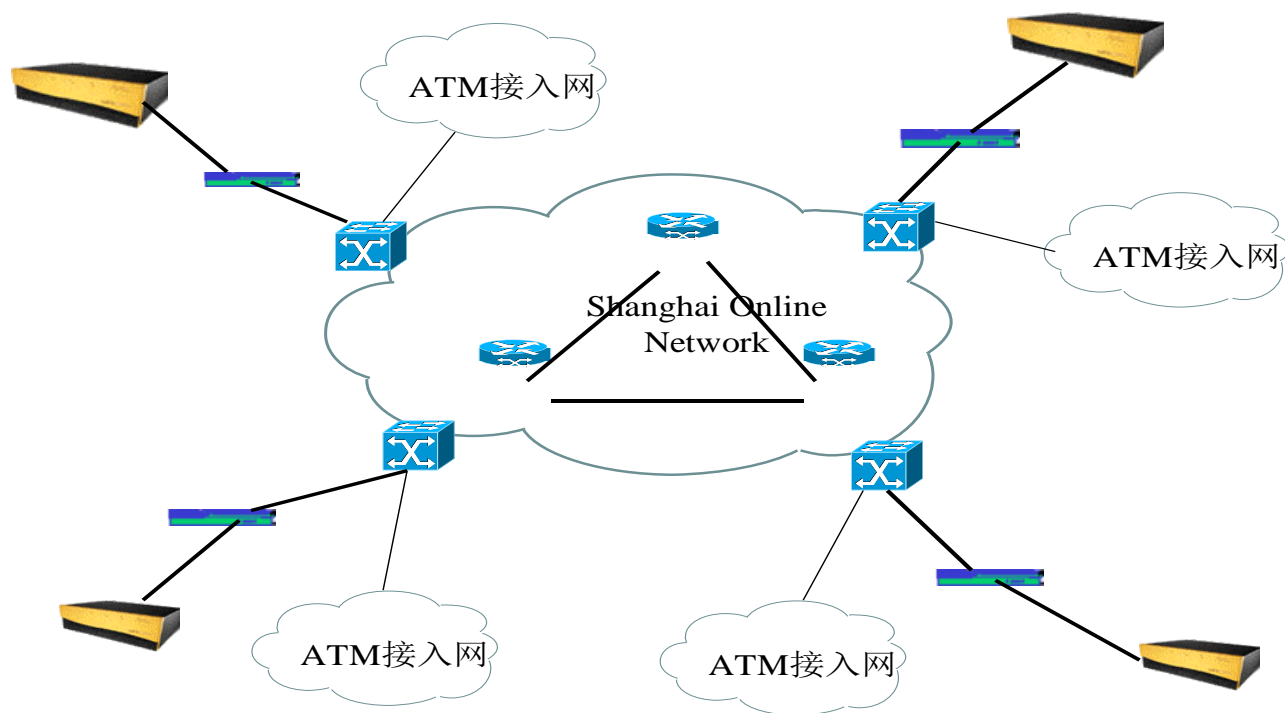
案例四 sohu.com



案例四 sohu.com

- 项目实施结果
- Blue Coat缓存专用设备运用于Sohu.com访问流量最大的频道，有效降低了服务器的负载
- 作为专用设备的使用，管理非常简便，内容同步采用Blue Coat动态刷新和静态设置相结合的方式，日常的内容同步工作
- Blue Coat专用设备以其强大的处理能力，替代多台服务器的工作，减少了所需机架空间，和维护工作量
- 专用设备的独特安全性使其在诸多互联网攻击下，保持正常的工作，并提供正常的内容服务

案例五 上海online APEC



案例五 上海online APEC

- 项目实施结果
- Blue Coat缓存专用设备提供了APEC期间Live和On Demand的流媒体服务
- 与L4的GSLB协调工作，实现CDN网服务，网络及用户端无需任何改动
- Blue Coat缓存提供的分布播放，有效保证了Streaming的播放质量，并降低了流媒体播放对网络产生的压力

谢谢！