



Secure and Manage
Your Internet Access



Anchiva Web 安全网关

概
览

网络信息化时代，企业上网面临的风险与问题。

随着网络技术的发展，与之相关的网络应用也越来越丰富，通过上网可以获取知识，传递信息，创造商机，加快业务的拓展，增强企业的竞争能力。

然而，病毒、木马、间谍软件、蠕虫等也随着Internet应用进入内部网络，这不仅仅会使感染相关恶意软件的计算机运行缓慢甚至崩溃，破毁相关数据，更有木马和间谍软件等会在用户不知情的情况下偷窃商业信息或使其成为僵尸网络中的成员，并获取巨大的经济利益，而且随着人类物质文明的发展，以窃取商业信息获取经济利益为目的的恶意软件在网络中盛行，而且呈上升趋势。Gartner 曾经报道，75%的企业感染未被发现的，具有经济动机，有针对性的，并且回避传统外围设备和主机防线的恶意软件。

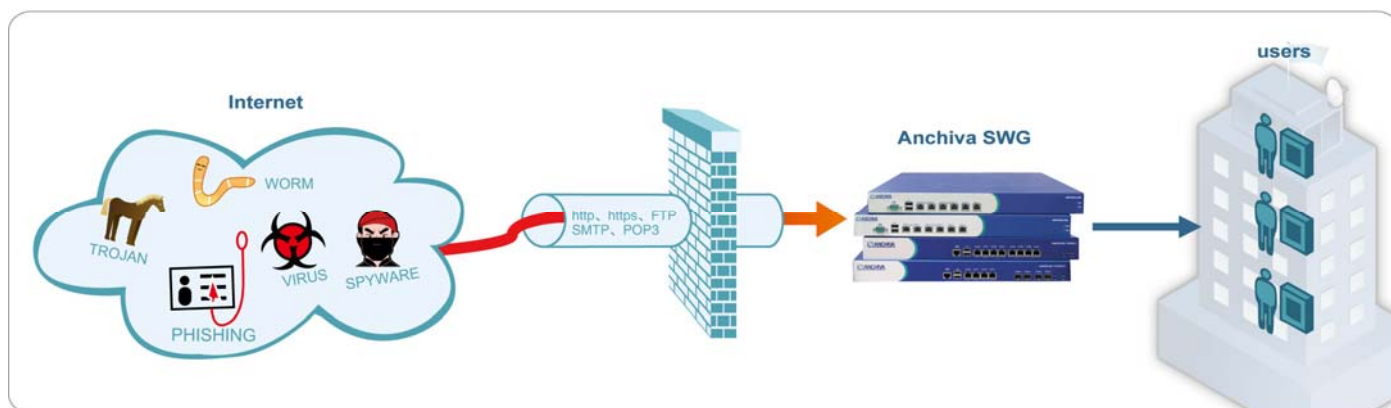
同时，企业员工也可以利用开放的网络在上班时间闲聊，网上购物，进行网络游戏大战，网上炒股，观看网络电视/流媒体，疯狂的利用 BT 等工具下载，这不仅会降低工作效率、造成网络拥塞更有甚者会利用相关的 Internet 应用泄漏机密信息，在网络上散布非法言论，使企业遭受经济损失、承担法律责任。

Anchiva 解决方案

如何规避上网所引发的风险与问题，充分利用网络资源，保障内网安全，提高办公效率，节省网络带宽投资，防止机密信息泄漏，避免法律风险？Anchiva 集 Anti-malware、URL 过滤、Internet 应用控制、带宽管理、web 应用防火墙等多功能于一身的 web 安全网关提供了良好的 Internet 应用安全与管理解决方案：

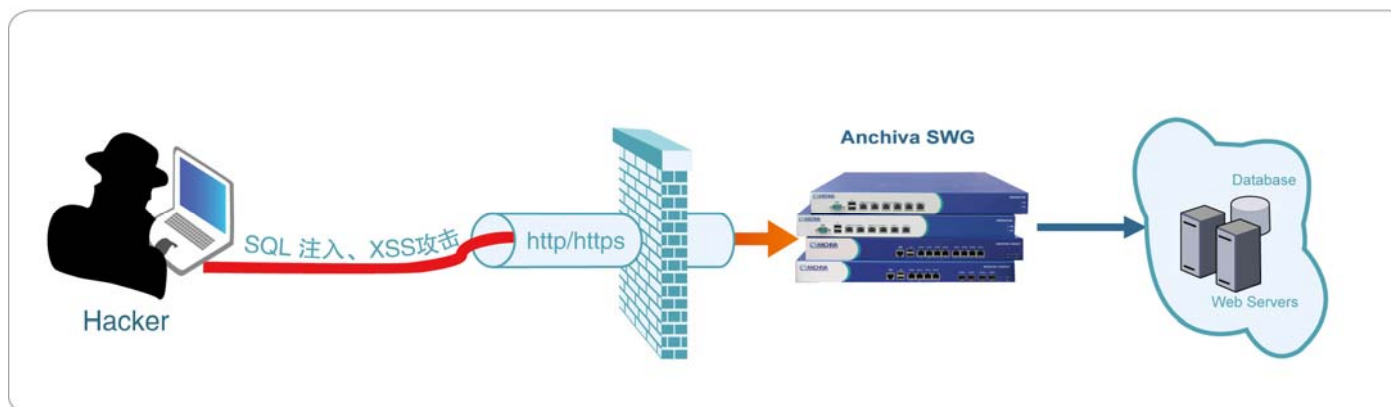


- 保护企业内网免遭网络威胁 (Malware) 侵袭，保障企业Internet应用安全性与可靠性。



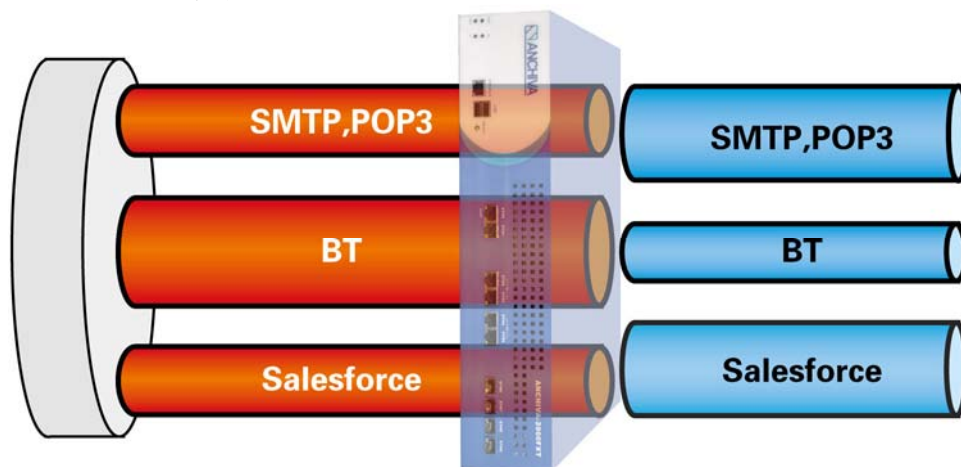
方案价值：应对病毒、木马、间谍软件、僵尸网络等危害。

- 保护企业web服务器免遭攻击，保护企业财产，降低企业名誉损失。



方案价值：应对web应用服务器遭受攻击而不能正常提供服务、网站数据库内容被窃取或篡改等问题。

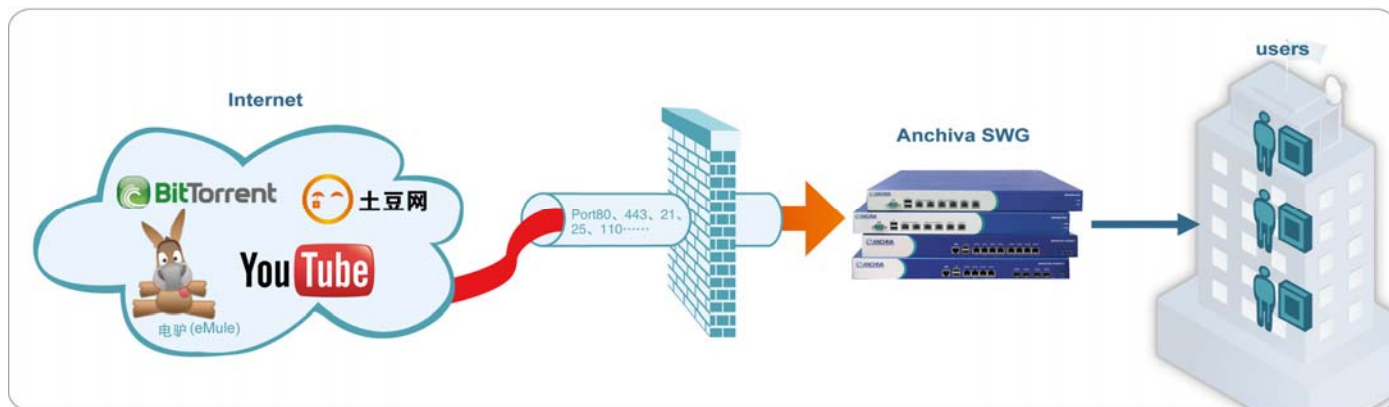
- 为企业生产性网络应用提供带宽保证，非生产性网络应用提供带宽限制，达到网络流量整形与优化，加速企业业务的运营，提高生产效率。



方案价值：应对带宽多大都不够用，关键业务服务效果差等困境。

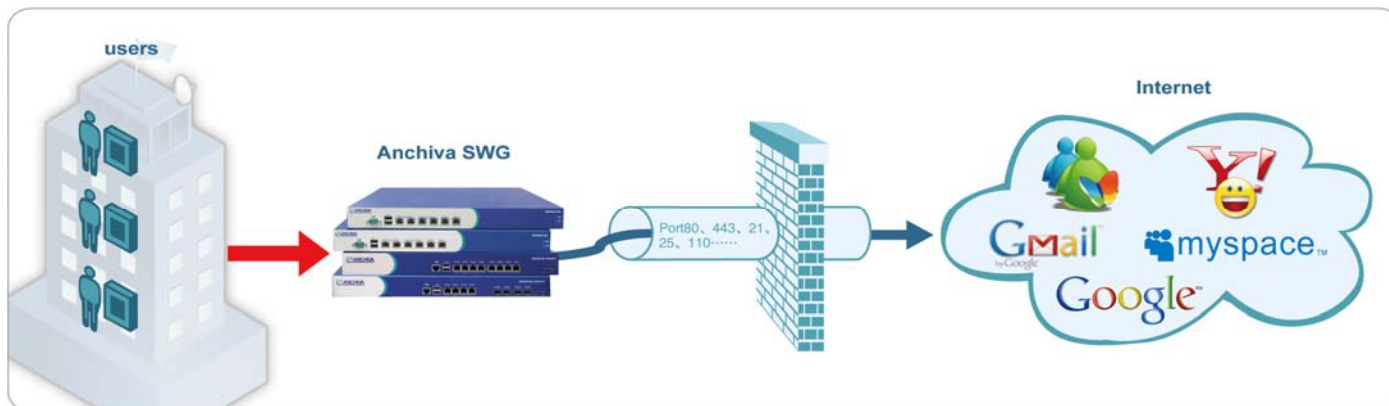


- 管控各种BT下载软件、流媒体播放软件，合理进行带宽分配与流量控制，提升带宽利用率，节省企业网络带宽投资。



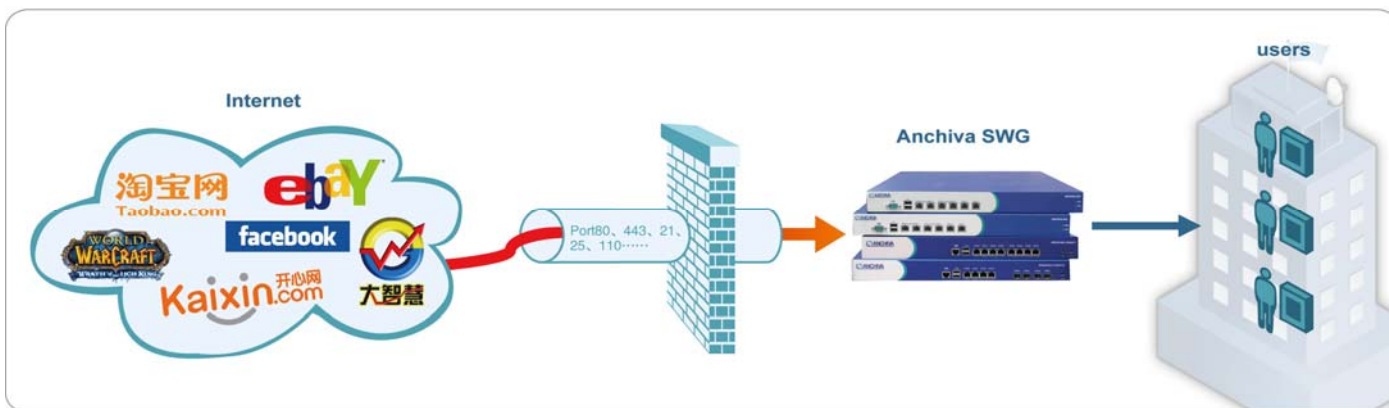
方案价值：应对网络内各种BT下载和流媒体等无法管控问题。

- 对IM（MSN、Yahoo）聊天内容进行审计，对webmail正文及附件，网络论坛发帖，网络搜索等进行关键字过滤，防止通过网络泄露商业机密信息。



方案价值：防止通过网络泄露机密信息等问题。

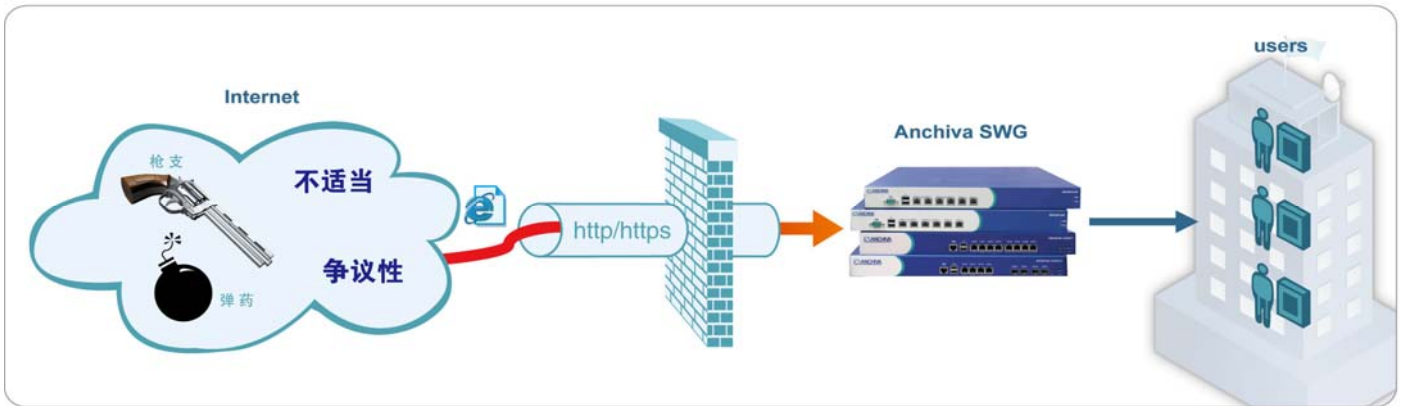
- 管控员工上班时间的IM闲聊，网上购物，进行网络游戏大战，网上炒股，网上冲浪等，规范员工上网行为，提供工作效率。



方案价值：应对员工上班时间的IM闲聊，网上购物、玩游戏、炒股等网络行为较严重的现象。



- 过滤员工访问不适当或有争议性的网络内容，避免企业承担不良影响风险。



方案价值：防止不适当Internet内容流入企业内部。

功
能
特
点

Anti-malware

Anchiva web 安全网关 anti-malware 功能中主要利用“*Malicious Sites 过滤引擎*”、“*深度内容检测 (DCI) 与特征匹配引擎*”和“*Heuristic Engine*”三大过滤引擎对进出网络的HTTP、HTTPS、FTP、SMTP、POP3等5种协议流量进行依次的扫描过滤，最大程度的确保检测的准确性，减少漏查和误报。具体功能点如下：

- 分析检测并阻止 HTTP、HTTPS、FTP、SMTP、POP3 **双向**流量中的病毒、木马、间谍软件、蠕虫、后门等网络威胁
- 间谍软件回传阻止
- 过滤阻断 Malware 发布源
- 防钓鱼
- 过滤分块下载中的 malware
- 应对零日攻击
- 快速定位内部威胁终端

Anchiva RapidRX 安全实验室每日提供常规更新服务 6 次

带宽管理

递进式的带宽统计报表，能够提供基于网络应用和基于用户的精细化流量分析，帮助管理员在全局与细节上掌握网络带宽使用状况，提升企业网络透明度，指导网络运维。从而方便企业管理员有针对性的实施基于网络应用、用户和时间段的带宽分配与管控策略。

基于网络应用、URL 类别、IP/IP 组/IP 地址段、用户/用户组、时间段的上行流量和下行流量带宽保证以及带宽限制，不仅能够提供对非关键网络应用的控制和限速，达到为企业网络流量整形的目的，还能够为关键的业务系统或网络应用提供带宽保证，达到网络流量优化和网络应用加速的目的。

支持用户自定义协议和 URL 类别，并且提供不间断的特征库定制、更新服务。



Internet 应用控制

Anchiva web 安全网关在分析识别 IM、P2P、流媒体、网络游戏、网络炒股等 Internet 应用或内容后，通过基于用户按时间段制订允许、阻断、限流和记录日志等颗粒度的策略达到对 Internet 应用的控制、分析与监控；同时为了满足策略群组中特定用户的需求，还可以设定特定的例外 IP 或用户。

提供不间断的特征库定制、更新服务。

URL 过滤

采用数据云 URL 过滤技术，60 多种 URL 类别，云技术智能收集分类平台，使企业能够避免因职员访问聊天类、金融类、购物类、娱乐类等网络内容所带来的生产力的损失，能够避免因对网络下载、流媒体和 P2P 等类别站点的访问所带来的网络带宽损失，能够避免职员对毒品类、犯罪活动等类别站点的访问所带来的法律责任，并且通过用 URL 过滤直接屏蔽存在 malware 的站点，屏蔽网络钓鱼、僵尸网络类站点或 URL，从而进一步消除网络安全风险，加强企业网络的安全性。

云技术提供随时随需更新服务

Web 应用防火墙

部署在 Web 服务器的前端，通过对进出 web 服务器的 http/https 协议相关内容的实时分析监测、过滤，来精确判定并阻止各种 Web 入侵行为，阻断对 web 服务器的恶意访问与非法操作，适应 web2.0 时代的主动实时监测过滤风险技术，而不是被动的遭受攻击后的恢复，将恶意代码、非授权篡改、应用攻击等众多因素结合在一起进行综合防范，从而做到对 web 服务器的保护，防止网页内容被篡改，防止网站数据库内容泄露，防止口令被突破，防止系统管理员权限被窃取，防止网站被挂马和植入病毒、恶意代码、间谍软件等，防止用户输入信息的泄露，防止账号失窃，防 SQL 注入，防 XSS 攻击，控制 web 爬虫等。

具体特点如下：

- **对 HTTP/HTTPS 协议的深入分析**

对 HTTP/HTTPS 协议进行深入的解析，精确的识别出协议中的各种要素，比如 Cookie, Get 参数, Post 表单等，并对这些数据进行必要的解码，以还原原始信息，根据这些解码后的原始信息，可以准确的检测其是否包含攻击内容。

- **Anchiva 提供专业的攻击特征库**

Anchiva 的 Web 安全研究员通过对大量的实际网络中的各种 Web 入侵攻击方式的深入分析，提炼出用于检测 web 攻击的特征库。Anchiva 提供的特征库，可精确判定 web 攻击行为。一旦发现新的攻击形式，Anchiva 将会及时更新相关的特征库，用户通过自动升级可及时得到最新的特征库。

- **用户可自定义许可规则**

除了使用我们 Anchiva 提供的攻击特征库外，用户还可以根据特定 Web 站点的实际情况，选择制定更严格的许可规则，杜绝一切不合规则的访问。这将有助于加强防御未知的 web 攻击。

特征库由 Anchiva RapidRX 安全实验室专业维护升级，对用户无专业要求。



全面的功能

Anchiva 全面的功能给客户带来多种 Internet 应用安全与管理解决方案。客户不需要考虑多种产品的组合或集成问题，利用 Anchiva 的产品就能解决 Internet 应用安全防护与过滤、管控等问题，并且降低了总投资成本。

高性能的产品平台

具有专利技术、优化重写 TCP 协议栈且支持多核和 ASIC 加速卡的 AnchivaOS，并结合具有专利技术的 ASIC 加速扫描技术，是 Anchiva 高性能的技术保障，使 Anchiva web 安全网关突破了应用安全网关性能瓶颈，为客户提供了高性能的产品平台，并且随着硬件配置的提升，性能可近似线性增长。Anchiva web 安全网关 2007 年已通过 ICSA 的性能认证，证明了其全球领先的高性能。

全球化的安全实验室

Anchiva 的 RapidRX Labs 安全实验室，是 WildList 成员和积极贡献者，具有全球化样本采集网络、处理中心和 ASDN (Anchiva Service Distribution Network) 分发网络。Anchiva 每天处理 malware 样本数万条，每日常规 malware 特征更新 6 次，最新爆发 malware，2 小时之内响应，为客户提供 365 天不间断的 Internet 应用安全防护更新服务；同时 Anchiva 领先的数据云 URL 过滤技术和专业及时的 Internet 应用识别技术，为客户提供高效的 Internet 应用管理服务。

最大板载特征库

通过 Malware 特征转换技术将常规的 Malware 特征转换为 ASIC 加速卡识别的 Malware 特征格式，并将其写入 ASIC 高速存储单元，实现了动态刷新 ASIC 硬件加速卡内的特征，从而突破了 ASIC 难以升级的业界难题，做到板载特征库能够随时升级；目前 Anchiva web 安全网关在正常负载下能够查杀的 malware 样本超过 1000 万。

通过 ICSA anti-virus 认证

Anchiva Web 安全网关通过了 ICSA 病毒检测认证，证明了其 100%覆盖流行病毒的监测能力；并且在 ICSA 进行的所有月度测试中，Anchiva web 安全网关至今为止全部通过。

良好的网络适用性

Anchiva 产品良好的网络适用性使其能无缝部署到用户现有的网络中，而无需改变客户现有网络架构和网络应用。并且是业界唯一一款全部支持 VLAN、非对称路由、U-turn、HA 等网络环境的 web 安全网关。

灵活的部署方式

Anchiva web 安全网关不仅支持串连部署作为检测阻断与管控模式工作，还支持旁路监听模式。而无论哪种部署模式，Anchiva web 安全网关在网络中都相当于一个 2 层设备，不需要修改网络的 IP 分配策略和任何现有的网络应用策略。



产品线

产品系列	低端系列	中端系列	高端系列			运营商系列
产品型号	206T	506FT	806FT	1000FXT	500*	2000FXT
*推荐用户终端数	400	1000	2000	5000	10000	10000
*HTTP 吞吐量一	45 Mbps	220Mbps	390Mbps	410Mbps	500Mbps	710Mbps
*HTTP 吞吐量二	35Mbps	135Mbps	220Mbps	515Mbps	600Mbps	980Mbps
*HTTP 最大并发连接数	27000	33000	150000	180000	200000	300000
*HTTP 每秒新建连接数	900	1800	2000	2200	2300	2500
*UDP 吞吐量(单向)	(30-305)Mbps	(100-1000)Mbps	(110-1000)Mbps	(115-1000)Mbps	(120-1000)Mbps	(135-1000)Mbps
Anti-malware(Optional)						
Malicious site 过滤引擎	●	●	●	●	●	●
深度内容检测 (DCI) 与 Malware 特征匹配引擎	●	●	●	●	●	●
Heuristic Engine	●	●	●	●	●	●
HTTP,HTTPs,FTP,SMTP,POP3	●	●	●	●	●	●
Inbound and Outbound Inspection	●	●	●	●	●	●
WAF(Optional)						
防 SQL 注入	●	●	●	●	●	●
防 XSS 攻击	●	●	●	●	●	●
防缓冲区溢出攻击	●	●	●	●	●	●
防 Cookie 毒化	●	●	●	●	●	●
防 command 注入	●	●	●	●	●	●
自动攻击黑名单	●	●	●	●	●	●
控制 web 爬虫	●	●	●	●	●	●
URL 过滤(Optional)						
64 种 URL 类别	●	●	●	●	●	●
支持自定义 URL	●	●	●	●	●	●
支持带宽管控	●	●	●	●	●	●
应用控制(Optional)						
IM	●	●	●	●	●	●
P2P	●	●	●	●	●	●
Stream media	●	●	●	●	●	●
支持带宽管控	●	●	●	●	●	●
Deployment						
即插即用	●	●	●	●	●	●
在线透明部署	●	●	●	●	●	●
旁路镜像部署	●	●	●	●	●	●
VLAN	●	●	●	●	●	●
Hardware						
网口	4C	5C+2F	5C+2F	4C+4F	6C+2F	6C+4F
Bypass	1 对	2 对	2 对	2 对	3 对	2 对
平均无故障运行时间	85000 小时	85000 小时	85000 小时	85000 小时	85000 小时	85000 小时



产品线
(续)

备注:

- 1、500*为专为电信级用户定制产品型号。
- 2、*推荐用户终端数是结合 Anchiva 在用户网络中的大量实际部署案例所得到的经验值，供 anti-malware 选型参考。
- 3、*HTTP 吞吐量一：以 www.google.com 首页测试结果，供 anti-malware 选型参考。
- 4、*HTTP 吞吐量二：以 windows 中 notepad.exe 文件测试结果，供 anti-malware 选型参考。
- 5、*HTTP 最大并发连接数：以 64 字节 text/html 文件测试结果，供 WAF、URL 过滤选型参考。
- 6、*HTTP 每秒新建连接数：以 64 字节 text/html 文件测试结果，供 WAF、URL 过滤选型参考。
- 7、*UDP 吞吐量（单向）：以 RFC2544 为标准测试结果，供带宽管理选型参考。
- 8、支持定制光口 Bypass。

典型客户



安启华公司
北京市海淀区清华科技园科技大厦B座 601 邮编：100084
电话：+86-10-51266678 传真：+86-10-62703326
更多信息请拨打免费电话400-650-1886，或访问www.anchiva.com

产品质量保证和服务

Anchiva提供一系列的服务选项供购买。我们强烈建议您购买持续的服务以确保得到最新的软件版本和用户体
验。另外，Anchiva提供专业的咨询服务、安装服务和配置支持，并提供相应培训课程。

2009 年安启华公司版权所有。安启华公司保留修改本资料页上内容的权利，恕不另行通知。

AnchivaOS和Anchiva是安启华公司的注册商标或商标。

本文所提及的其他已注册和未注册商标都是各自所有者的专有财产。