

web 应用安全挑战

随着 Internet 应用与技术的日益进步，web 网站所承载的业务越来越多，针对 web 网站服务系统的各类攻击也日益增多，如 SQL 注入攻击、XSS 跨站脚本攻击、网站挂马等，而防火墙、IPS 等传统安全设备不能对 web 业务提供完善有效的防护。

因此，众多政府对外服务网站、IDC 托管服务器、电子交易网站、游戏服务器、聊天网络等 web 服务系统长期以来一直被 web 应用攻击所困扰，随之而来的是名誉受损、客户投诉、同虚拟主机用户受牵连、法律纠纷、商业损失等一系列问题。于是，解决 web 应用安全问题成为当今企业必须考虑的头等大事。

Anchiva web 应用安全网关解决方案

web 应用安全问题本质上源于代码质量。但 web 应用不同于其他的应用软件，例如文字处理、图像处理软件等，其往往具有某个企业机构独有的业务应用，而且需要频繁的变动以满足业务发展的需要。而通常人们认为 web 开发很简单，缺乏经验的开发者也可开发出满足相关需求的 web 应用，但很多情况下开发者只是照着葫芦画瓢，没有很好的理解 web 业务流程，更没有考虑客户端与服务器端以及后台数据库端复杂的交互操作。于是对于这类具有定制化特点的 web 应用，没有通用的补丁可用，整改代码因代价过大变得较难实施或者需要较长时间的整改期。

针对上述 web 应用现状，专业的针对 web 应用交

Anchiva web应用安全网关提供积极、主动式web应用防护：

- 阻止SQL注入
- 阻止XSS攻击
- 阻止OS命令注入
- 阻止利用服务器中已存在的后门程序进行网页挂马
- 阻止弱口令入侵
- 防网页篡改
- 防溢出检查
- Cookie防篡改
- Cookie防劫持
- 具有Cookie加密功能
- 服务器挂马监控
- 对上传文件进行病毒扫描
- 对提交内容进行病毒扫描
- 阻止目录遍历攻击
- 禁止浏览网站目录的内容
- 阻止特定文件类型下载
- 阻止特定文件类型上传
- URL关键字过滤
- URL查询参数关键字过滤
- 上传内容敏感信息过滤
- 对网站管理入口设定授权IP
- 屏蔽服务器版本
- 屏蔽服务器错误响应
- 屏蔽数据库错误信息
- 阻止服务器程序代码泄露

互数据进行检测并提供防御的产品成为一种合理且很有必要的选择。Anchiva web 应用安全网关应需而生，基于对 HTTP/HTTPS 流量内容的双向检测分析，识别检测各类 web 编码、交互技术、URL 参数以及表单输入等，为 web 应用提供实时、动态的主动性防护。

Anchiva web 应用安全网关，通过对进出 web 服务器的 HTTP/HTTPS 流量相关内容的实时分析检测、过滤，来精确判定并阻止各种 web 应用入侵行为，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 服务器的多重保护，确保 web 应用安全的最大化，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 攻击等。

防护机制

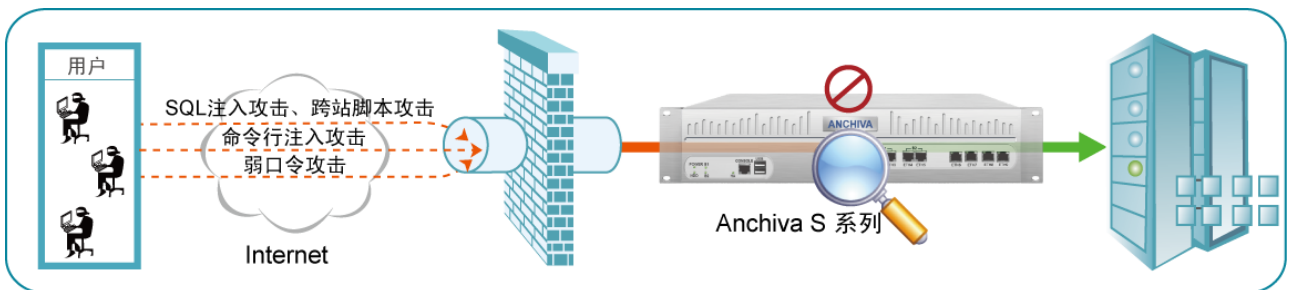
事前预防

事前，Anchiva web 应用安全网关针对 web 应用架构中的各种敏感信息进行检测屏蔽，如服务器版本信息检测屏蔽、web 程序代码泄漏检查、web 站点目录内容泄漏检查、数据库报错信息检测屏蔽、HTTP 错误检测屏蔽等，并且对危险文件下载进行检查过滤，从而防止黑客获得采取下一步攻击的有用信息。



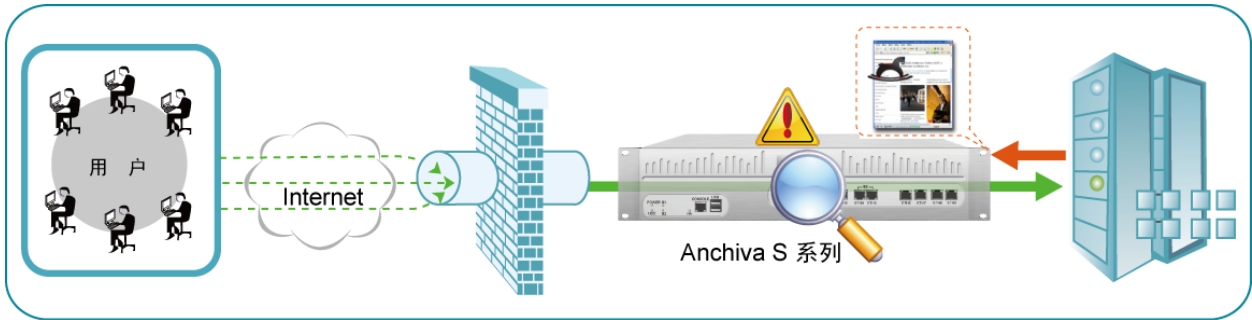
事中拦截

事中，Anchiva web 应用安全网关检测 web 应用交互会话中是否存在 SQL 注入攻击、跨站脚本攻击、命令行注入攻击、弱口令攻击等攻击行为，并及时阻断保护 web 服务系统的安全。



事后监控

事后，针对当前的安全热点问题，例如网页挂马，提供监控诊断功能，并及时报警，降低安全风险，维护企业的信誉度。



产品特点

动态页面的防护技术

对采用 web2.0 技术的动态页面，Anchiva web 应用安全网关提供针对 web 输入请求的实时检测过滤技术，防御利用动态页面程序设计上所存在的安全漏洞而发起的 SQL 注入、XSS 跨站点脚本攻击、缓冲区溢出等攻击，从而防御这些攻击所要达成的目的，包括：绕过登陆身份检查、获得系统管理员密码、非法获取数据、非法篡改数据、生成非法文件、执行非法命令等一系列修改、破坏网站数据库内容、网站架构等的攻击行为，保护 web 站点内容与服务的安全性及可靠性。

静态页面的安全防护技术

对静态的网页元素，例如 HTML、图像文件、多媒体文件等，Anchiva web 应用安全网关具有专门的缓存检测机制，对交付给用户的网页做交付前的检查核实，只有确认合法的网页才能被输出到客户端，被篡改的非法网页将被锁定，不会被访问用户看到，并及时通知管理员进行篡改恢复。

网站挂马检测、过滤与监控、报警

网页挂马是一种相对隐蔽的网页篡改方式，挂马后的页面从表面页面内容呈现上不易察觉，本质上却破坏了页面的完整性。攻击者利用网站挂马达到其黑色地下经济利益的获取。挂马网站作为木马的传播帮凶，严重影响了站点的信誉度。Anchiva web 应用安全网关能够对用户输入或上传的内容进行检测过滤，一旦发现挂马企图，将及时阻断。

在未部署 web 应用防火墙之前，用户的 web 页面可能已经被挂马，因此基于这样的现状需求，Anchiva web 应用安全网关不仅能对 web 应用的交互行为进行分析，还能够对 web 页面中的嵌入式内容进行检测过滤，一旦发现被挂马将及时通知管理员，并且提供客户可定制的替换页面，直到网页恢复正常。

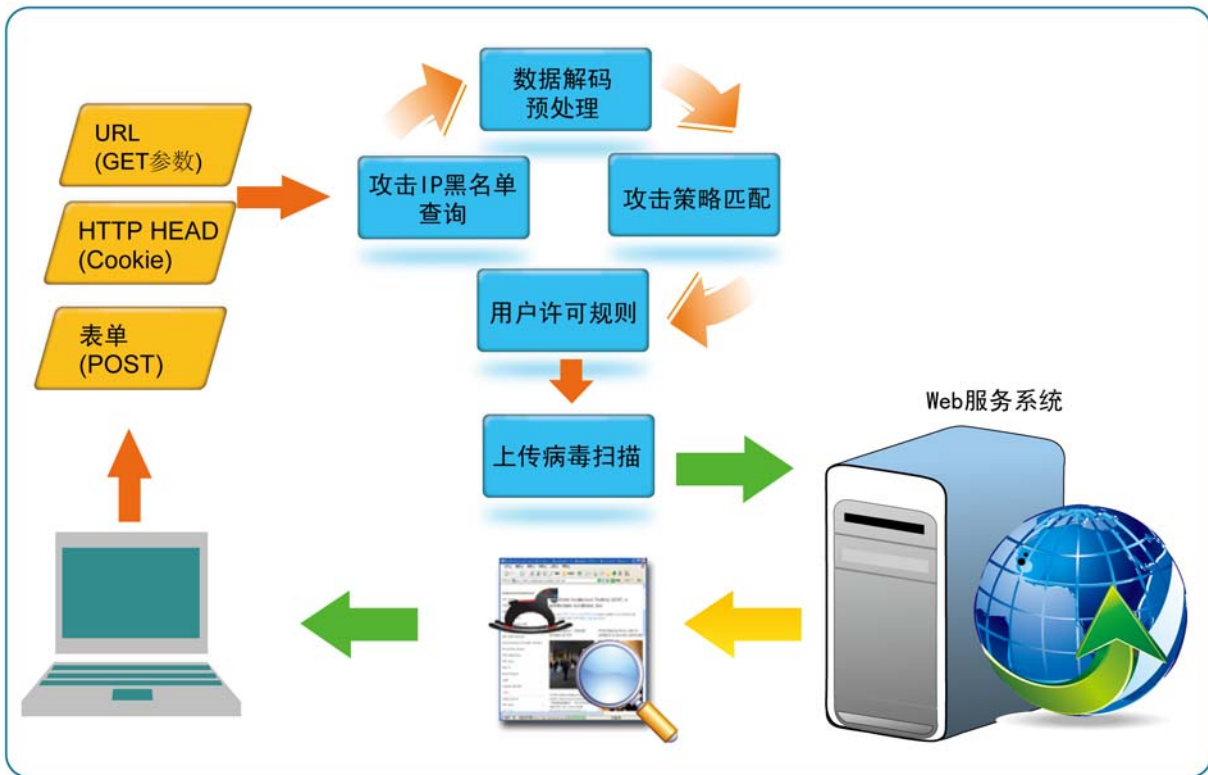
独有的恶意文件上传过滤功能

Anchiva web 应用安全网关会对 HTTP/HTTPS 应用交互中上传附件进行病毒检测过滤，并内置强大的病毒特征库，防止感染病毒的文件上传到 web 服务器后造成大范围的病毒扩散，致使服务器瘫痪；更重要的是能阻断后门病毒上传到服务器，从而获取服务器的控制权限，达到攻击 web 应用系统的目的。

双向深度数据解码及内容级多重检测过滤

Anchiva web 应用安全网关作为 web 客户端与服务器端请求与响应的中间人，避免 web 服务器直接暴露在互联网上，检测过滤 HTTP/HTTPS 双向交互流量数据，对其中的恶意成分进行实时在线清洗过滤。通过对 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，准确的检测识别是否包含攻击内容。

图：Anchiva web 应用安全网关威胁检测流程图



易于部署与管理

纯透明式在线部署，能够即插即用，自动升级，无需更改网络和 web 服务系统架构，且与网络中已有的防火墙、路由器、交换机等设备均能直接连通。

多级灵活防护

针对不同的 web 域、web 服务地址、web 目录、URL 等提供不同的防护策略。基本防护策略与高级防护策略配合使用，达到对 web 应用交互内容的检测与合规性、安全性过滤。

良好的性能与稳定性

Anchiva web 应用安全网关完全继承了 Anchiva 在 Web 网关上的多年技术积累，支持多核均衡分发与优化重写 TCP 协议栈的操作系统是 Anchiva 产品具有良好性能与稳定性的核心保障技术。



高投资回报率

- 单一设备支持多对线路的同时防护。
- 根据 web 交互内容定位攻击，与服务器本身并无关联，可随意增加防护服务器。
- 部署在 IDC web 服务器前端，可建立不同的防护策略，为多个托管 web 服务系统既可提供集中式的防护，也可提供个性化的防护。

产品规格

型号	S100	S300	S600	S900
性能				
转发吞吐量	400Mbps	600Mbps	1Gbps	2Gbps
HTTP 吞吐量	200Mbps	400Mbps	600Mbps	900Mbps
HTTP 最大并发连接数	150000	200000	300000	400000
HTTP 每秒新建连接数	5300	7000	9000	11000
硬件				
接口	6C	6C+4F	6C+4F	6C+4F
冗余磁盘阵列 (RAID)		√	√	√
冗余电源		可选	√	√
外型规格	IU	2U	2U	2U
平均无故障运行时间 (MTBF)	大于 100000 小时	大于 100000 小时	大于 100000 小时	大于 100000 小时
管理				
WebUI	√	√	√	√
命令行界面 (SSH/Console)	√	√	√	√
报表系统	√	√	√	√
报警提示 (SNMP & E-mail)	√	√	√	√
高可用性				
操作系统闪存化	√	√	√	√
HA	√	√	√	√
硬件 Bypass	2 对	2 对	2 对	2 对
部署				
在线透明部署	√	√	√	√
旁路镜像部署	√	√	√	√
VLAN	√	√	√	√



结论

针对 web2.0 时代 web 应用类攻击呈上升且危害越来越严重的趋势，选择 web 应用防火墙是明智的，但是如何辨别、品鉴并选择市场上名目繁多的 web 应用防火墙，我们 Anchiva 的建议如下：

- 结合自身的 web 应用特点，明确安全策略目标。
- 品鉴产品是否真正具有 HTTP 应用代理功能，是否具备对 HTTP/HTTPS 交互数据内容的检查过滤能力，比如对 HTTP/HTTPS 协议中的 Cookie、Get 参数、Post 表单等进行识别检测过滤。
- 评估 WAF 产品可覆盖的风险类型，例如 SQL 注入、XSS 脚本、网站防挂马、网站防病毒等。
- 评估产品功能、性能以及可扩展性，以满足业务发展的需求。
- 评估厂商的技术服务支持能力，是否具有专业的安全服务团队。
- 评估产品的易用性与可维护性，以便内部团队的日常运维。
- 评估投资回报率。

关于 Anchiva RapidRX 安全实验室

Anchiva 具有全球化的安全实验室 RapidRX 及国际级的安全研究分析人员，能够及时跟踪、发现互联网上 web 应用攻击类型及发展趋势。为 Anchiva 全球客户提供不间断的规则库与防护算法的更新，与用户一起应对各类 web 应用攻击。



Anchiva 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公司提供服务选项供购买。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公司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。

2010 Anchiva版权所有。Anchiva保留修改本资料页上内容的权利，恕不另行通知。

AnchivaOS和Anchiva是Anchiva 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。