什么是web应用程序防火墙

概要

Web应用程序防火墙（WAF），顾名思义，即能够将web应用程序的出去的和进来的http流量进行过滤、监控和屏蔽。WAF 和传统意义上的防火墙还是有一定的区别的: waf 是关注特定web应用的内容过滤，而传统的防火墙则是服务器之间的守门人。通过检查Http流量，它可以防止来自Web应用程序安全漏洞的攻击，如SQL注入、跨站点脚本（XSS）、文件包含漏洞以及安全配置错误。

历史

能够控制应用程序或某个服务的输入、输出、访问等，也就是应用防火墙，首次出现是在上世纪90年代，由 Gene Spafford, Bill Cheswick, and Marcus Ranum等人开发，他们所开发的产品还并没有完全脱离传统意义上的防火墙，但是也可以支持几个应用程序了，如FTP、RSH等，当时主要是由DEC来发售。在接下来的几年，其他研究人员进一步开发产品，为其他厂商提供稳定的防火墙软件，为其他厂商打下坚实的基础。
然而，专门针对web的应用程序则是在2000年之后的事情了，这当然和互联网的迅猛发展有关，而伴随的就是网络攻击行为的日渐增多。
在市场上第一家提供专门的web应用程序防火墙的公司叫做：Perfecto Technologies ，产品名称：AppShield ，这款产品定位于电子商务市场，并在防止非法网页字符条目做的不错。Perfecto后来更名为Sanctum，并成功成为web应用程序防攻击的前十名的公司，为整个WAF的市场奠定了基础，后来WAF发展的防黑客技术有：

- 隐藏领域操纵
- Cookie篡改
- 参数篡改
- 缓冲区溢出
- 跨站点脚本
- 后门或调试模式
- 隐身指令
- 强制浏览
- 第三方配置错误
- 已知漏洞

在2002年，开源项目ModSecurity创建，目标是让WAF技术让更多的站点使用，以及解决行业内的障碍，如业务案例，成本障碍和专有规则集。ModSecurity 基于OASIS 的web应用安全技术委员会的漏洞最终发行了核心规则集（CRS）。在2013年，进一步通过了开放web应用安全工程（OWASP）的扩展和标准化的top10 列表，此列表每年都会排名Web安全漏洞。该列表已经成为许多合规主题的行业基准。
从那时起，WAF 这块市场突飞猛进，由于信用卡欺诈的上升所导致整个商业都对它开始青睐有加，随着支付卡行业数据安全标准（PCI DSS）的发展，组织机构增加对持卡人数据的控制，安全性受到更多的监管，引发了业内广泛的兴趣。据Forrest在2010年的说法，WAF市场规模突破2亿美元。

技术细节

web应用程序防火墙，即是专门针对web应用程序的应用程序防火墙。它部署在web应用程序之前，分析双向的Web（HTTP）流量——发现并阻止任何有害的行为。OWASP 为WAF 提供了一个广泛的定

义：
一个针对web应用层的安全解决方案，-从技术的角度来看 - 其并不依赖于应用程序本身。
根据PCI DSS 6.6 信息补充说明，WAF 被定义为：
位于Web应用程序和客户机端点之间的安全策略执行点。此功能的实现可以是硬件，也可以是软件，运行在某些特定的硬件中，也可以在服务器的操作系统中运行，它可能是单独的一台设备，也可以是和其它网络组件组合。
换句话说，WAF可以是虚拟或物理设备，可防止Web应用程序中的漏洞受到外部威胁的利用。这些漏洞可能是因为应用程序本身是遗留类型或设计编码不足。WAF通过规则集的特殊配置（也称为策略）来解决这些代码缺陷。
以前未知的漏洞可以通过渗透测试或通过漏洞扫描程序来发现。Web应用程序漏洞扫描程序，也称为Web应用程序安全扫描程序，在SAMATE NIST 500-269中被定义为“自动化程序，用于检查Web应用程序的潜在安全漏洞。除了搜索特定于Web应用程序的漏洞之外，这些工具还会查找软件编码错误。”解决漏洞通常被称为补救。可以在应用程序中对代码进行更正，但通常情况，需要更加迅速的响应。在这些情况下，可能需要应用针对唯一Web应用程序漏洞的自定义策略来提供临时但即时修复（称为虚拟补丁）。
WAF不是最终的安全解决方案，而是与其他网络周边安全解决方案（如网络防火墙和入侵防御系统）结合使用，以提供整体防御策略。
SANS研究机构称，WAF 的安全模式，有的遵循正向、有的遵循反向、有的是二者混合。WAF 使用基于规则的逻辑、解析和签名的组合来发现和预防诸如跨站点脚本、SQL 注入等攻击。OWASP 发布了web应用程序安全漏洞的 top10 列表，所有的商业WAF 产品都至少覆盖这十大漏洞，其实一些非商业的也同样提供。
正如前面所提及，著名开源WAF 引擎 ModSecurity 确实是大家主流的选择，仅WAF引擎是不足以提供足够的保护的，因此 OWASP 联合Trustwave's Spiderlabs 开发了 ModSecurity WAF 引擎的规则集——Core Rule Set(CRS)，并托管在GitHub上。

部署属性

尽管在名称上操作模式有所不同，WAF 还是通过不同的部署方式，按照NSS实验室的定义，部署属性有三种不同的方式：

- 透明桥
- 透明反向代理
- 反向代理

“透明”是指HTTP流量直接发送到Web应用程序，因此WAF在客户端和服务器之间是透明的。而反向代理是不一样的，在反向代理中，WAF扮演了代理的角色，即客户端的流量会直接发送给WAF，然后，WAF将过滤的流量单独发送到Web应用程序。这可以提供诸如IP掩蔽的附加益处，但可能引入诸如性能延迟等缺点。

商业产品

多数的WAF 商业产品都拥有差不多相似的特性，但是主要的差异通常是指特定环境中的用户界面，部署选项或要求。

软件套件

- Radware - AppWall
- Monitorapp AIWAF
- Barracuda Networks WAF
- Citrix Netscaler Application Firewall

- F5 Big-IP Application Security Manager
- Penta Security's WAPPLES
- Imperva SecureSphere
- Fortinet FortiWeb
- Positive Technologies, PT Application Firewall

云平台提供

- Radware
- AIONCLOUD
- Akamai Technologies Kona
- AWS WAF
- Cloudbric
- Cloudflare
- F5 Silverline
- QingCloud WAF
- Sucuri Firewall
- Imperva Incapsula

开源项目

web 应用程序防火墙的开源项目使用范围非常广。

- ModSecurity
- NAXSI

参考资料:

1. 维基百科的WAF
2. AWS WAF develpement guide
3. ModSecurity 官网