互联网安全防御之WAF (Web应用防火墙) 实现方案分享

产品名称	互联网安全防御之WAF (Web应用防火墙) 实现方案分享
公司名称	广州市微码互联科技有限公司
价格	.00/件
规格参数	
公司地址	天河区中山大道379号联合社区东区
联系电话	13480273125 13480273125

产品详情

WAF简介

WAF，即Web Application Firewall（Web应用防火墙），是一种针对Web应用层恶意请求的访问控制措施，是立体防御体系的组成部分和一种辅助性防御手段。

目前WAF的产品形态主要有：

(1)硬件产品

硬件WAF串行或旁路部署在网络上，通过Web界面进行管理和规则配置，价格较高，但部署方便，运维管理比较省心。

(2)纯软件产品

软件WAF以ModSecurity、Naxsi等免费开源软件为代表，部署在每一台Web服务器上，需要网络安全人员熟悉其配置规则，但服务器数量多了之后，这种单机模式安装的软件，维护管理很快就会变得不太方便，因为不同的服务器可能使用不同的规则。

(3)云WAF产品

以各类云加速+CDN类产品为代表，如国外的CloudFlare、国内的各种云加速等，对用户隐藏真实服务器地址，云WAF作为反向代理执行安全控制，是用户浏览器和真实服务器之间的中间人。应该说，云WAF是一种比较可行的模式，在商业上已有较多成功案例。但对于流量比较大、服务器比较多的大中型企业、或者涉及商业秘密等场景，可能就不太合适了。

(4)自研WAF产品

如果上述几种WAF无法满足业务的需求，则需要考虑自己开发定制WAF了。

WAF实现方案

笔者所在的公司，流量巨大、服务器很多，前面几种方案都不太适用。最终，我们决定自己开发WAF，主要需求有：

(1)能够通过服务器（云端）统一配置和下发策略；

(2)能够自动上报拦截日志；

(3)拦截黑客入侵行为，包括但不限于：SQL注入、跨站脚本、路径操纵、上传/利用网页木马、CC攻击等；

(4)规则要少，允许漏报，但不能误报。

关于第4点，我们一开始就将WAF定位为辅助性防御设施，根本性的防御措施还是放在安全流程、安全规范的落地和推行上。

我们的服务器操作系统统一采用Linux，Web服务器统一采用Nginx，这就降低了开发的难度，不用适配其它各种操作系统和Web服务器版本。