东北师范大学信息化管理与规划办公室

网站入侵防护系统（WAF）测试报告

测试时间：2013 年 10 月-11 月

测试部门：系统运行部

一、 前言

网站入侵防护系统（WAF）是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品。由于市场上网站入侵防护系统（WAF）型号众多，为了避免盲目购买，选择一款既能满足我校网站安全防护需求，又具备尽可能高的防护性能的产品，我们进行了本次测试，力求在满足性能要求的前提下，选择性价比更高的产品。

二、 测试产品选择

为了能够充分了解各个厂商的产品，通过网络查阅、兄弟高校咨询、自身了解，确定了三款测试产品，包括两个国内知名厂商以及一个国际知名厂商，分别为□□□、□□□、□□□。

三、 测试方式

本次测试主要通过实际部署到校园网中来对产品的防护效果进行测试，通过使用人员对后台进行操作来对产品的操作友好性、便捷性进行测试，同时结合我校网站的实际分布情况，对部署方式的合理性进行测试。

四、 产品部署方式

方案一：透明部署（串联模式）

透明部署方式，即将 WAF 防火墙串联到网络交换机之间，在所要防护的服务器群连接的交换机之前，如图 1 所示：

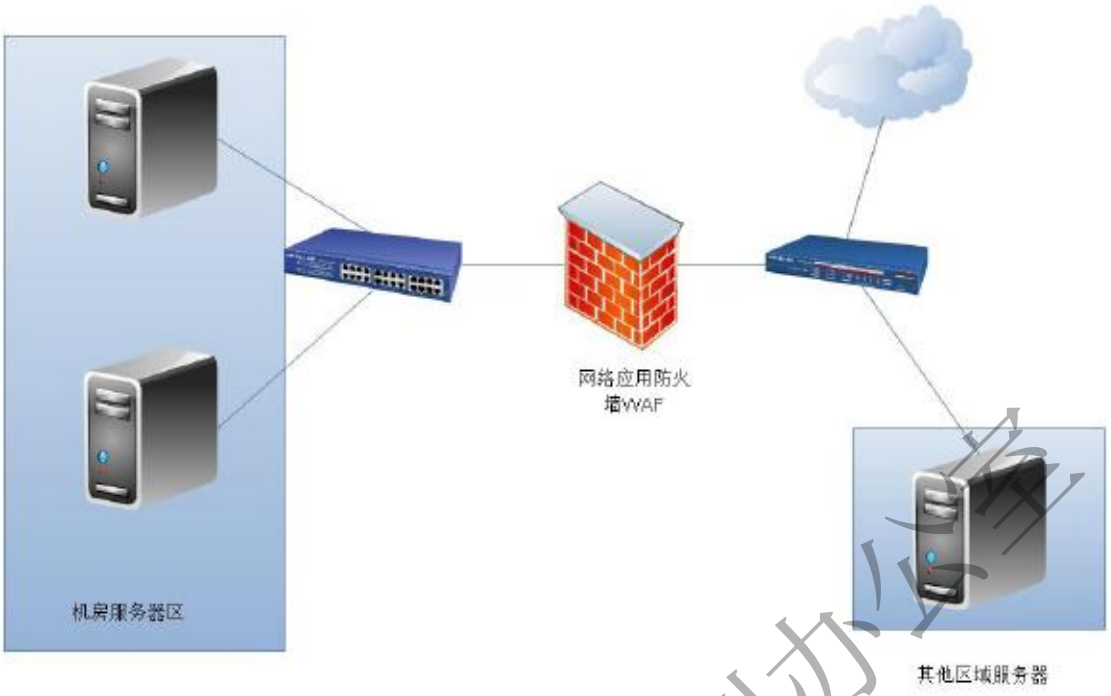

图 1

方案二：旁路模式（单臂模式、反向代理模式）

旁路模式，即将 WAF 防火墙直接连接到所要防护的服务器群的交换机上，对内外流量进行过滤，如图 2 所示：

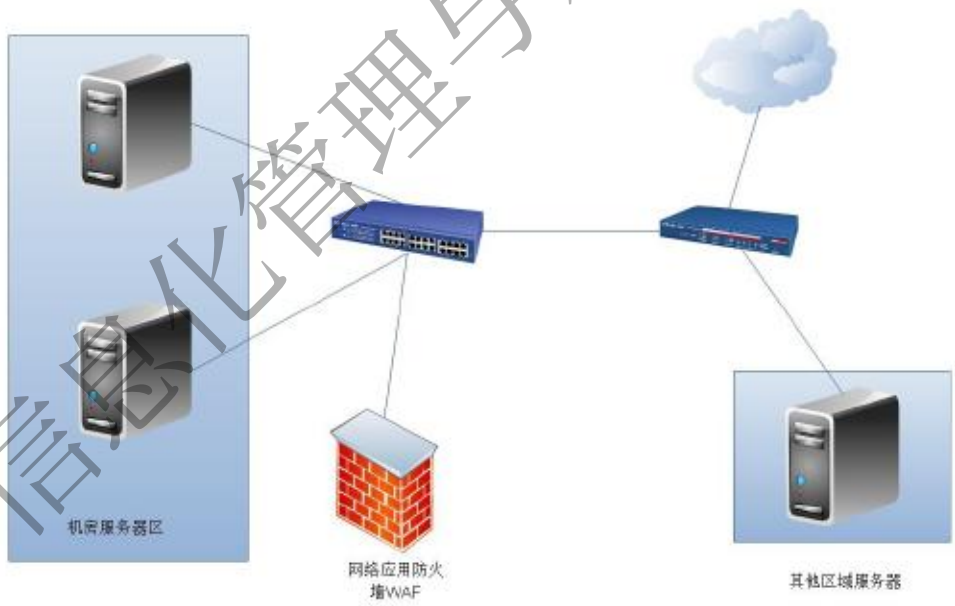

图 2

4.1 测试的部署方式

针对三种网站入侵防护系统各自所支持的部署方式的不同，以及测试选择的部署方式的差别，这里对比了各自部署方式的特点，如表 1 所示：

	□□□	□□□	□□□
支持的部署方式	透明部署模式、反向	透明网桥模式、旁路	单臂模式、双臂模式、

	代理模式和旁路模式	反向代理模式、路由模式、混合部署模式、虚拟化部署模式	桥接模式
测试选择的部署方式	透明部署：WAF 的入口接核心路由器端，出口接网站服务器区域，可防护服务器区域内的所有网站	透明部署：WAF 的入口接核心路由器端，出口接网站服务器区域，可防护服务器区域内的所有网站	单臂模式：直接将 WAF 的网口接到 9512 上面，通过修改域名将 http 流量引到 WAF，经 WAF 过滤之后，转发到真实服务器

表 1

4.2 两种部署方式

基于 WAF 防火墙的两种部署方案，在此对比了其网络架构、对外发布 ip 地址、多出口网站防护等部署的特性，如表 2 所示：

部署方式	透明部署	旁路方式
网络架构	串联到需要防护的网站之前，需要较小的改动网络架构	作为一个设备连接到交换机，不需要改动网络架构
对外发布 ip 地址	无需改变网站服务器对外发布 IP 地址	需要改变网站服务器对外发布 IP 地址
多出口网站防护	对学校主页这种多出口网站的防护不需要在交换机上做特殊配置	对学校主页这种多出口网站的防护需要在交换机，或者路由器上做地址转换配置
全校范围防护	则需要直接与核心路由器串联连接，有可能成为网络的瓶颈与故障点，尤其是有视频流经过的时候	只将对校内网站的访问通过配置引入到 WAF，其他流量不经过，不会造成网络瓶颈，但有可能成为单一故障点，需要通过双击热备的方式进行解决

表 2

4.3 旁路部署方式

旁路部署方式在三种 WAF 防火墙的各自部署中也各不相同，对于旁路部署方式的分析对比，如表 3 所示：

□□□	□□□	□□□
在路由器上面配置较多，每增加一台服务器的防护，就需要增加一条 nat 规则，不利于维护；或者按网段增加 nat 规则，这时非 http 流量的可靠性依赖于 WAF 自身的透传功能	在交换机端口上面做修改，比较方便；其余在 WAF 上面配置虚拟接口，实现不同 vlan 之间的数据传输和代理，配置方便，便于维护	测试时间短，未知

表 3

五、 防护功能测试

考察 WAF 防火墙的最重要的性能在于其防护功能是否完善，对于各个类型的网络入侵，对三种品牌的防护能力、防护效果进行了对比分析，如表 4 所示：

	□□□	□□□	□□□
基本功能	1.HTTP/S 支持 2.规则系统+自学习白名单建模的安全模型 3.Web 服务器漏洞 4.Web 插件漏洞 5.爬虫防护 6.跨站脚本防护 7.SQL 注入防护 8.LDAP 注入防护 9.SSI 指令防护 10.XPath 注入防护 11.命令注入防护 12.路径穿越防护 13.远程文件包含防护 14.CSRF（跨站请求伪造）防护 15.Cookie 安全防护 16.HTTP ACL 扫描防护 17.信息泄露防护 18.非法上传防护 19.非法下载防护 20.正则表达式规则匹配	1.SQL 注入攻击（包括 URL、POST、Cookie 等方式的注入） 2.XSS 攻击、CSRF 攻击 3.Web 常规攻击（包括远程包含、数据截断、远程数据写入等） 4. 命令执行（执行 Windows、Linux、Unix 关键系统命令） 5.危险存储过程执行 6.缓冲区溢出攻击 7.数据库信息窃取、泄露 8.网站挂马 9.扫描器探测 10.恶意代码 11. 自学习特征建模的防护 12. 基于过滤输出的防护 13. 扫描器扫描防护 14. DDOS 攻击 15. CC 攻击防护 16. 关键字过滤 17. HTTP SSL 安全加密、攻击过滤	1.SQL 注入 2. 跨站脚本攻击 3.Cookie 或表单篡改 4.表单元字符有效性检查 5.自适应安全策略 6.网站隐藏 7.响应控制 8.外出数据威胁保护 9.信用卡号码 10. 自定义特征匹配(regex) 11. **HTTPS 证书导入** 12. URL 参数控制
其他功能	1. 防护各类带宽及资源耗尽型拒绝服务攻击 2. 智能补丁应急响应 3.应急 ByPass 功能		1. 可针对 slow client 端攻击、僵尸网络攻击（CAPTCHA）的攻击进行有效防护. 2. GeoIP 过滤功能，当用户遇到大规模 DDOS 攻击可以开启此功能防护 3. 流量优化功能（缓存和压缩） 4. 集成了服务器负载均

			衡功能 5. URL 转换、请求重写、响应重写、BODY 重写功能 6. 具有 XML 防火墙功能，可以 XML、WS-I、WSDL、SOAP 验证 7. 对于上传文件有病毒扫描功能 8. 隐藏日志中敏感参数的功能 9. 具有 Clickjacking 攻击防护功能 10. 具有会话跟踪功能（有助于防护 7 层的 DDOS 攻击） 11. 具有 FTP 命令过滤功能 12. 可支持多种认证服务集成（LDAP、RADIUS、SITE MINDER、RSA SECURID、KERBEROS）
测试防护网站	对学校主页、一台 Asp 托管网站服务器进行防护效果防护	对一台 Asp 托管网站服务器进行防护	对一台 Asp 托管网站服务器进行防护
拦截防护效果	在测试期间，学校主页、托管网站服务器无安全事件发生，并且能在系统后台看到大量被拦截的攻击	无安全事件发生，能在系统后台看到被拦截的访问	无安全事件发生，能在系统后台看到被拦截的访问，对于不产生破坏行为的访问不进行拦截

表 4

六、 后台管理

后台管理可以方便管理者对于 WAF 防火墙策略的部署和调整，后台管理的便捷与否、功能展示明确与否同样影响着管理的效率。这里对三种产品的防护规则配置、报表展示等方面进行了比较，如表 5 所示：

	□□□	□□□	□□□
防护规则配置	配置方便	规则配置较方便	规则配置过程较复杂，需要细化配置
报表展示	实时显示防护效果，利用图形进行展示，界面友好，方便观看，展示效果好	实时显示须手动刷新，无图形展示界面，须手动导出，展示效果一般	实时显示防护效果，利用图形进行展示，界面一般
规则库升级	自动升级	手动升级，暂时无自	自动升级

		动升级	
修改配置界面响应速度	快(1s)	较快（3s）	较慢（3——5s）
防护网站数量限制	无限制	无限制	无限制
其他			在配置了之后，发生过两次配置自动消失的情况，代理商解释为测试机器多次试用，被摔坏了的原因

表 5

七、 售后服务以及后期费用

针对三种产品售后服务的费用和方式，下表也进行了详细的阐述，如表 6 所示：

	□□□	□□□	□□□
售后服务方式	有长春本地办事处	在沈阳和哈尔滨有办事处	在沈阳有办事处
售后服务费用	服务费用每年一收，根据型号不同，费用不同，最多不超过 2 万	5 年服务期内免费，超过服务期之后费用为合同的 10%左右	一年为期限，基本上为合同额的 10%——20%之间

表 6