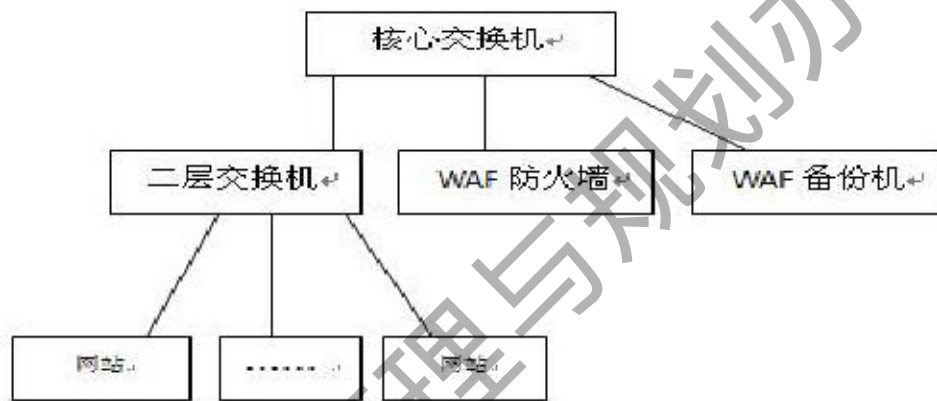


网站入侵防护系统（WAF）部署可行性报告

可行性报告背景：自从网站入侵防护系统（WAF）部署以来，对学校主页、信息化办主页进行了防护，在平稳运行三个月之后，对上述两个网站起到了很好的保护作用，阻止了大量的网络攻击，达到了网站防护的目的。但系统本身的硬件资源和负载是有限的，能否大规模的对东北师范大学所以信息系统和网站进行防护，需要根据硬件性能和防护运行情况进行估计，特形成此可行性报告。

一、系统部署拓扑

当前 WAF 防火墙的部署拓扑示意图如下：



硬件 WAF 防火墙直连到核心交换机 9512，同时有一个基于虚拟机形式的备份 WAF 防火墙，以备在硬件发生故障的情况下，可以临时使用，以免对校内网站的正常访问造成影响。

二、防护能力和效果

1. 可防御的攻击类型

对 cookie 中毒、跨站点脚本攻击、恶意浏览、SQL 注入、命令注入、参数（或表单）篡改、缓冲溢出攻击、目录穿越攻击、密码拦截、DOS 攻击等多种攻击类型。

2. 在试运行阶段防护的网站情况

目前对学校主页、信息化办、网上招聘系统、一卡通查询系统 4 个网站进行防护。在 WAF 防火墙防护之前，信息化办和学校主页的网站每天都有被攻击

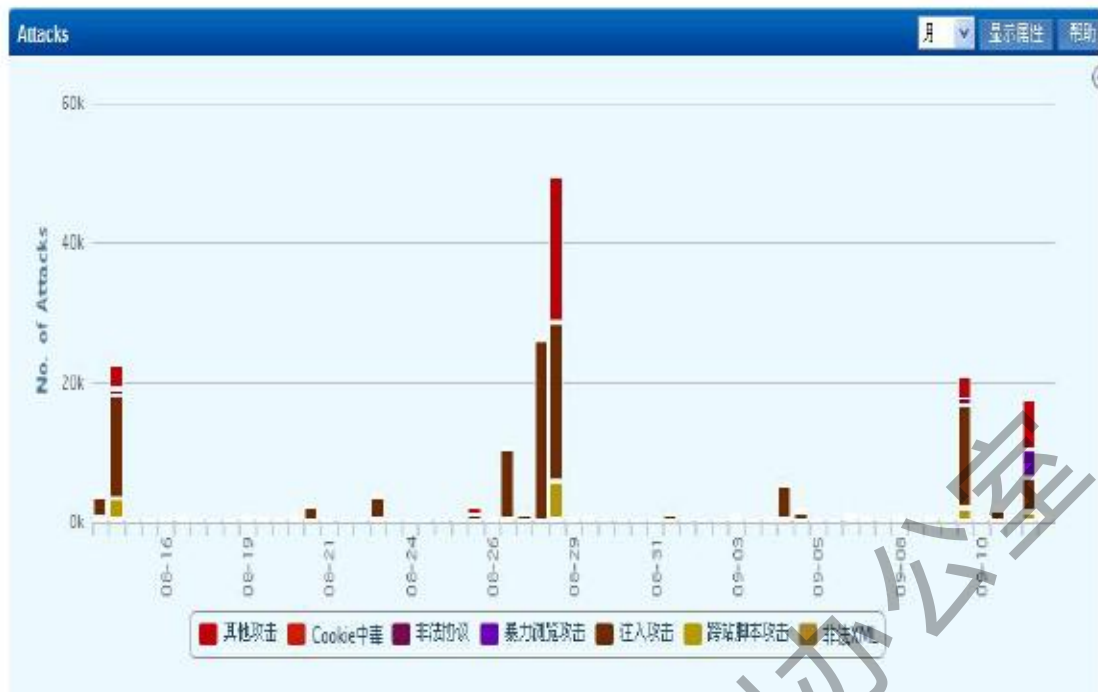
的记录，并有上传木马和垃圾网也的情况出现。部署 WAF 防火墙之后，WAF 防火墙对学校主页和信息化办的攻击行为拦截，如下图所示。

1)学校主页的攻击拦截记录

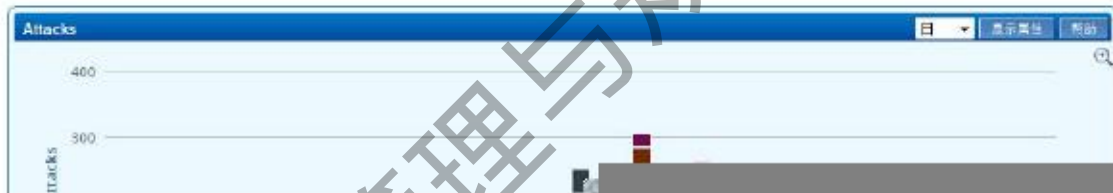
时间	客户端IP	服务器IP:端口	动作	严重性	URL	Method	攻击类型	详细消息	规则
2014-09-10 08:33:19...	222.210.85...	202.198.138.125:80	DENY	Alert	202.198.138.125/		Invalid Method		global
2014-09-10 08:31:05...	202.198.136...	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/uploads/	PROPFIND	Forbidden Method	Method="PROPFIND"	security-policy
2014-09-10 08:31:55...	202.198.136...	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/uploads/ta...	PROPFIND	Forbidden Method	Method="PROPFIND"	security-policy
2014-09-10 08:31:55...	202.198.136...	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/uploads/ta...	PROPFIND	Forbidden Method	Method="PROPFIND"	security-policy
2014-09-10 08:29:32...	101.228.68...	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/nenunew...	GET	远程文件包含漏洞	type="remote-f...	security-policy
2014-09-10 08:29:02...	202.24.2.189	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/nenunew...	GET	远程文件包含漏洞	type="remote-f...	security-policy
2014-09-10 08:28:04...	175.44.25.20	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/uploads/ta...	POST	远程文件包含漏洞	type="remote-f...	security-policy
2014-09-10 08:27:59...	202.198.142...	202.198.138.125:80	DENY	Alert	202.198.138.125/		Invalid Method		global
2014-09-10 08:26:17...	221.178.112...	202.198.138.125:80	DENY	Alert	202.198.138.125/uploads/123...	GET	Malformed Version	GET /uploads/...	global
2014-09-10 08:26:17...	221.178.112...	202.198.138.125:80	DENY	Alert	202.198.138.125/uploads/123...	GET	Malformed Version	GET /uploads/...	global
2014-09-10 08:26:17...	221.178.112...	202.198.138.125:80	DENY	Alert	202.198.138.125/uploads/123...	GET	Malformed Version	GET /uploads/...	global
2014-09-10 08:26:17...	221.178.112...	202.198.138.125:80	DENY	Alert	202.198.138.125/uploads/123...	GET	Malformed Version	GET /uploads/...	global
2014-09-10 08:25:34...	218.47.28.71	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/uploads/	PROPFIND	Forbidden Method	Method="PROPFIND"	security-policy
2014-09-10 08:25:34...	218.47.28.71	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/uploads/ta...	PROPFIND	Forbidden Method	Method="PROPFIND"	security-policy
2014-09-10 08:25:32...	218.47.28.71	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/uploads/ta...	PROPFIND	Forbidden Method	Method="PROPFIND"	security-policy
2014-09-10 08:25:32...	218.47.28.71	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/uploads/ta...	PROPFIND	Forbidden Method	Method="PROPFIND"	security-policy
2014-09-10 08:25:32...	218.198.105...	202.198.138.125:80	DENY	Alert	202.198.138.125/		Invalid Method		global
2014-09-10 08:25:14...	186.140.133...	202.198.138.125:80	DENY	Alert	ic3be.baidu.com/index.php?url...	GET	远程文件包含漏洞	type="remote-f...	security-policy
2014-09-10 08:24:25...	117.138.8.214	202.198.138.125:80	DENY	Alert	www.nenu.edu.cn/nenunew...	GET	远程文件包含漏洞	type="remote-f...	security-policy
2014-09-10 08:23:13...	113.57.188.70	202.198.138.125:80	DENY	Alert	202.198.138.125/uploads/123...	GET	Malformed Version	GET /uploads/...	global

2)信息化办网站攻击拦截记录

2014-09-09 18:17:06...	125.222.192...	202.198.138.125:80	DENY	Alert	xxhb.nenu.edu.cn/admin/upla...	POST	Deny ACL matched		www_xxhb_xxhb
2014-09-09 18:15:57...	125.222.192...	202.198.138.125:80	DENY	Alert	xxhb.nenu.edu.cn/admin/upla...	POST	Deny ACL matched		www_xxhb_xxhb
2014-09-09 15:38:58...	220.181.51...	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/ta/gonggao...	GET	Error response suppressed	code="403"	global
2014-09-09 14:54:11...	10.253.38.185	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/plaie/	GET	Error response suppressed	code="403"	global
2014-09-08 23:25:28...	61.147.193.21	202.198.138.125:80	LOG	Alert	xxhb.nenu.edu.cn/	POST	SQL Injection in Parameter	type="sql-injec...	security-policy
2014-09-08 23:01:18...	203.158.220...	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/plaie/	GET	Error response suppressed	code="403"	global
2014-09-08 23:01:18...	203.158.220...	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/plaie/	GET	Error response suppressed	code="403"	global
2014-09-08 22:19:25...	125.32.66.84	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/uploads/ta...	OPTIONS	Error response suppressed	code="403"	global
2014-09-08 22:19:24...	125.32.66.84	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/uploads/ta...	OPTIONS	Error response suppressed	code="403"	global
2014-09-08 22:19:24...	125.32.66.84	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/uploads/ta...	OPTIONS	Error response suppressed	code="403"	global
2014-09-08 22:19:24...	125.32.66.84	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/uploads/ta...	OPTIONS	Error response suppressed	code="403"	global
2014-09-08 22:19:23...	125.32.66.84	202.198.138.125:80	CLOAK	Notice	xxhb.nenu.edu.cn/uploads/ta...	OPTIONS	Error response suppressed	code="403"	global
2014-09-08 15:39:22...	115.238.225...	202.198.138.125:80	DENY	Alert	xxhb.nenu.edu.cn/admin/	GET	Deny ACL matched		www_xxhb_xxhb
2014-09-08 14:42:47...	61.235.158...	202.198.138.125:80	DENY	Alert	xxhb.nenu.edu.cn/admin/	GET	Deny ACL matched		www_xxhb_xxhb



2) 如果单看某一天的防护效果, 如下图所示, 受到的攻击次数在 1 千次以上, 主要的受攻击时间集中在 21 点和第二天凌晨 1 点之间, 受到攻击的主要类型为 SQL 注入攻击。



信息化管理与规划网

可见，自从 WAF 防火墙于 6 月 10 日部署以来，到目前为运行时间为 100 天左右，总共防御住的网络攻击数量为 99 万多次，平均每天防御攻击为 1 万次，有效的保障了其防护网站的安全。

三、运行状况

1. 硬件性能参数

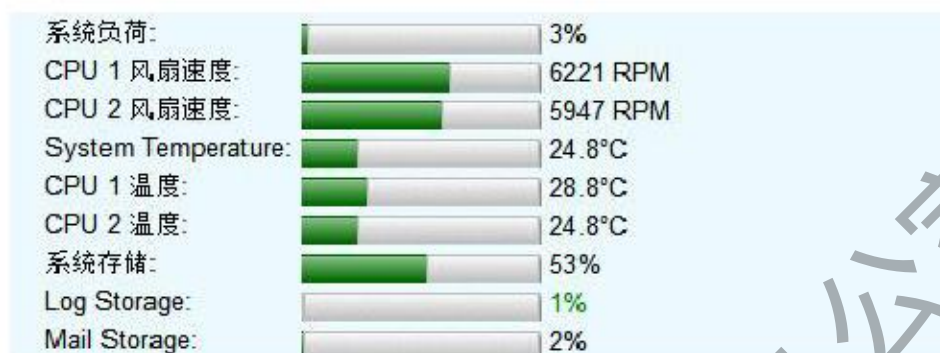
我校部署的设备硬件型号为 860，主要性能参数如下

名称	性能参数
	两个四核

信息化管理与规划办公室

硬件可以满足的最大 Web 流量 1G（据公司人员介绍，我校这种部署模式，由于存在 Web 访问的上行和下行，实际使用达不到 1G 流量），而目前校内网站、系统数量为 200 多个，4 个网站数量为 8M，按这种流量估算 200 个网站的数量约为 400M，硬件从 Web 流量这个性能指标上完全能够满足校内所有网站的防护需求。

3. 试运行阶段的系统负荷



在试运行阶段，系统负荷为 3%，但在网站多了之后的系统负载是什么情况，没有可以估算的理论算法，因此在这方面，需要在部署过程中，分批分阶段部署，每部署一批网站，观察系统负荷，如果系统负荷处于正常范围之内，就继续部署下一批网站的防护，如果系统已经无法负荷已部署网站，则停止部署。

四、被防护网站要达到基本条件

1. 不含有或调整后（将大文件内容迁移至非防护范围的服务器）不含有较大流量的在线播放和下载。

由于提供在线视频类服务和数据下载类网站对流量的占用过多，梭子鱼 WAF 需要对经过自身的数据包进行分解分析，如果这类型流量经过梭子鱼，会极大的影响硬件性能和效率，同时也有可能超过梭子鱼自身的流量限制，因此目前不能够部署视频类或者数据下载类型的网站。

2. 信息系统或网站最大并发数小于每秒 300 次。

网站的访问量对 WAF 的承载能力是一个重要的影响因素。其影响因素包含

4. 已经对信息系统或网站安全状况进行过自查。

因为 WAF 无法对已经被上传木马或恶意程序的网页进行防护，会认为这些访问是正常的网页访问，因此在部署 WAF 防火墙之前，需要将网站服务器上当前的木马、恶意程序清除，须自行检查或找专业的公司有偿清除。

5. 加入防护之后必须开启防火墙，阻止 http 访问直达服务器

由于未开启防火墙的状态下，客户端的用户会通过 http 访问直接访问到目标服务器，会对服务器的安全构成威胁。因此需要开启系统防火墙，只接收 WAF 防火墙返回的客户端合法请求，从而避免了由用户直接访问目标服务器的安全隐患。

信息化管理与规划办公室