Web 应用防火墙需要知道的十个问题

1 一句话概括梭子鱼 Web 应用防火墙。

梭子鱼 Web 应用防火墙是应用级的网站安全综合解决方案，能帮助企业达到在线支付级的网站安全标准。具备十大功能，十大技术，是 web 应用防火墙的领导品牌：

十大功能	十大技术
网站隐身	反向代理
网站防篡改	应用层深度包检测技术
网站主动防攻击	基于规则的攻击模式匹配技术
网站防信息泄露	http 数据标准化技术
网站防 DDoS、CC 攻击	Cookie 加密签名及重放保护技术
网站负载均衡	IP 复用、缓存、压缩等加速技术
网站加速	认证授权代理技术
网站安全访问	数据窃取防护技术
网站安全审计	高可用性综合技术
网站安全合规	智能模式学习技术

2 梭子鱼 Web 应用防火墙与网络防火墙的区别

这是工作在不同层面两类产品：

第一代网络防火墙作为访问控制设备，主要工作在 OSI 模型三、四层，基于 IP 报文进行检测。其产品设计无需理解 HTTP 会话，也就无法理解 Web 应用程序语言如 HTML、SQL。因此，它不可能对 HTTP 通讯进行输入验证或攻击规则分析。针对 Web 网站的恶意攻击绝大部分都将封装为 HTTP 请求，从 80 或 443 端口顺利通过防火墙检测。

一些定位比较综合、提供丰富功能的防火墙，也具备一定程度的应用层防御能力，如能根据 TCP 会话异常性及攻击特征阻止网络层的攻击，通过 IP 分拆和组合也能判断是否有攻击隐藏在多个数据包中，但从根本上说他仍然无法理解 HTTP 会话，难以应对如 SQL 注入、跨站脚本、cookie 窃取、网页篡改等应用层攻击。

梭子鱼 Web 应用防火墙能在应用层理解分析 HTTP 会话，因此能有效的防止各类应用层攻击，同时他向下兼容，具备网络防火墙的功能。

3 梭子鱼 Web 应用防火墙与网页防篡改的区别

这是防护方法和防护功能有巨大区别的两种产品。

从防护的方法来说，网页防篡改产品着眼点在于“事后恢复”，可防止篡改的危害扩大。但是它不能防止攻击发生；并且他只有在攻击发生对网页篡改的行为时才能产生作用，而事实上多数类型的攻击并不篡改网页，如 DDoS 攻击、CC 攻击、溢出攻击、cookie 窃取、密码拦截、数据窃取等；还有很多攻击有可能产生篡改行为，但多数情况并不会篡改网页，如 SQL 注入、目录穿越等；即使是“事后恢复”，网页防篡改产品也存在工作原理漏洞、服务负载增加、检测机制绕开、连续篡改等安全问题。

梭子鱼 Web 应用防火墙是 Web 网站安全的综合解决方案，能够主动防御各种针对 web 网站的攻击行为，包括各种“篡改”行为。它是在攻击到达服务器之前就进行阻断拦截，能解决一揽子网站安全问题。

4 梭子鱼 Web 应用防火墙与 IPS 的区别。

这是防护技术和防护对象不同的两类产品。

相同点是，IPS 和 Web 应用防火墙都是为防止网络攻击而设计的。不同的是 IPS 采用的是特征匹配技术、使用“允许除非明确否认”模式，其防护对象是一段网络、以及网络中通用的设备或系统而不是特定的 Web 应用；

IPS 不能向 Web 应用防火墙那样进行主动防护，因此他不能防止“零日攻击”，也无法防止针对某个应用特制的攻击，如针对某个网站的命令注入或 SLQL 注入攻击；IPS 事实上也不会去理解 HTTPS 协议中的程序代码或报头设定，由于 Web 网站往往是特定开发的，IPS 往往无法针对性的进行防御。

5 梭子鱼 Web 应用防火墙与绿盟 web 应用层防火墙。

这是功能上有着巨大差异的同类产品。(宝马和 QQ 的差别):

1 防攻击的颗粒度天壤之别 绿盟针对 ip 地址、网站（域）、应用进行防护，梭子鱼不但可以对网站进行设置，还能对这个网站的某个目录下的甚至某个页面进行设置策略。甚至还可

以深入到 http 包头中对参数进行限定。

2 缺乏很多 Web 安全防攻击功能:如 cookie 加密、防信息泄露、网站隐身、认证授、SSL 卸载，IP 复用，缓存、负载均衡、…

3 安装模式，梭子鱼有串接（透明模式、路由模式）、旁路接入等多种方式，绿盟只支持串接（透明模式）。

4 主动防御的方式 梭子鱼在应用层上对 http 的代码标准化后进行代码分析，绿盟估计只有部分攻击是这样监测的，其他的依据特征。梭子鱼还能根据 web 服务器学习其参数及参数值并自动推荐策略。

5 绿盟内置漏洞扫描和网页挂马扫描；但他的漏洞扫描只能发现 SQL 注入和跨站点脚本两种。

6 防 DDoS 和 CC 攻击，特别是对 CC 攻击，绿盟语焉不详，在界面上只能看到对 IP 连接数的限制。而梭子鱼有多种途径。

7 日志比较简单（非互动式日志），记录访问 IP 和网站及攻击事件十几种；而梭子鱼的日志非常详细，分为 7 个安全等级，可以记录到对哪一个页面进行访问，而且攻击事件有 100 多种，并且**系统能智能推荐策略**，是互动式日志；

6 梭子鱼 Web 应用防火墙能够防止 DDoS 攻击和 CC 攻击吗?

所谓 CC 攻击是利用大量代理服务器对目标计算机发起大量连接，导致目标服务器资源枯竭造成拒绝服务，是 DDoS 攻击的一种。高明的 CC 攻击会针对某个比较消耗服务器资源的服务进行攻击。梭子鱼具有防止 DDoS 和 CC 攻击的功能：

1 在网络层对连接进行检查和限制，防止半连接，限制并发连接数。

2 速率控制：限制对某个应用的请求数。

3 采用 cookie 认证：拒绝不真实连接；如果 CC 中也有 cookie，还可以使用 cookie+IP 等重放保护，拒绝不真实连接。

4 利用 Session 防止重复访问或不正常页面刷新。

7 梭子鱼 Web 应用防火墙能防止网页挂码或病毒吗?

通过防止各种产生网页挂马的攻击行为防止网页挂马或病毒。

1 首先是建立访问安全，例如 cookie 安全、SSL 访问、访问认证；

2 主动防止 XSS、SQL 注入、恶意浏览等各种可能篡改网页的行为。

3 禁止文件上传类型。

8 梭子鱼 Web 应用防火墙能防止恶意蜘蛛程序爬行吗?

通过对 robots.txt 的分析禁止恶意爬行。

如：百度

```
User-agent: Baiduspider
Disallow: /baidu
#######禁止百度爬行工具/baidu 目录######
User-agent: *
Disallow: /shifen/dqzd.html
#######允许其他爬行工具但禁止其访问/shifen/dqzd.html #######
```

再如 google：

```
User-agent: *     #允许任意爬行工具
Allow: /searchhistory/  #允许爬行目录
Disallow: /search       #不允许爬行的目录
Disallow: /groups       #不允许爬行的目录
Disallow: /images       #不允许爬行的目录
Disallow: /catalogs     #不允许爬行的目录
Disallow: /catalogues   #不允许爬行的目录
```

9 梭子鱼 Web 应用防火墙测试时是否一定要断网，或者一定要进机房？

1 梭子鱼有多种安装模式，透明模式和路由（反向代理）模式需要串接在网络中，需要短时间断网（几分钟，插拔网线的时间）；旁路模式是旁路接入不需要断网，也不一定要在机房。---不过这时只能模拟访问，但很难模拟各种攻击行为；而且我们无法针对您网站的实际情况进行安全分析及策略设置。

2 可以先用旁路模式熟悉 NC 的各项功能及策略设置；如果需要进行实际测试，可以将 DNS 记录改到 NC 上，或者进入机房，采用透明模式进行测试。透明模式支持 bypass 功能。

10 使用了梭子鱼 Web 应用防火墙都能有那些好处？

1 减少不安全造成的损失：

- 减少客户数据、商业机密、员工信息、财务信息及其他敏感数据泄露的可能性。
- 减少因泄露信息而产生法律诉讼的可能性。
- 减少因安全问题造成公司股价下跌、形象受损、客户信誉降低的可能性。
- 更早的遵从有关法规对企业网络安全的规定如： (SOX, GLB, HIPAA, CA SB -386)

2 加快应用的使用：网站可以更早投入使用，不必等到漫长的漏洞测试及修补结束才使用。

3 维护更简单

发现问题后，无需离线等待漏洞修复、补丁修复；

老的应用漏洞无需寻找当初的开发维护团队；

4 优化运营

补丁管理：无需守候补丁升级，只需按计划升级。

日志合并和管理：所有访问日志均合并到梭子鱼上，梭子鱼日志更为详细，且包括各种搜索方式，梭子鱼更具日志智能推荐配置。

隐蔽内部结构，易于发布应用。可将内部的目录转换为外部的访问地址。

安全策略管理更加有效：梭子鱼的策略可以复制，无需每个策略都重建。

5 SSL 管理

初始化更快：无需在每台 Web 服务器上启用，减轻 Web 服务器负荷。

证书授权及合并：内部系统无需单独购买。