梭子鱼Web应用防火墙

——Web应用交付融合解决方案

概 要

- 需求分析
- 梭子鱼Web应用防火墙功能与应用
- 市场竞争与分析
- 案例分享

近年来热点事件

攻击造成的危害

2010年中国大陆34854个网站被黑客攻击

2008 年数据为 656件；共被窃取285万笔资料，超过2004-2007的总和

外部占75%

内部占20%(Partner占32%)

94%以"Web攻击（HTTP协议）"方式入侵。其中79%使用 SQL 注入，64%使用多种攻击手段配合

35%受害者为商业或企业用户，7%为政府单位及军方

如果部署专业应用防火墙，就能防范这类攻击的发生

统计数据来源

CRCERC 国家计算机网络应急中心——2010 年报

IDG 新闻 —— 2009 年 1 月

Network World —— 2009 年 4 月

Computer World —— 2009 4

思考我们的安全意识误区

国内外行业法规遵从

1	银行业	《电子银行风险管理原则》巴塞尔委员会
2	金融行业	中国银监会：《中国银行业实施新资本协议指导意见》，《电子银行业务管理办法》
3	支付卡行业	PCI DSS(支付卡行业数据安全标准)
4	电信移动行业	《中国移动网络与信息安全总纲》
5	医疗行业	美国HIPPA（健康保险流通与责任法案）

国内WAF行业相关政策规定

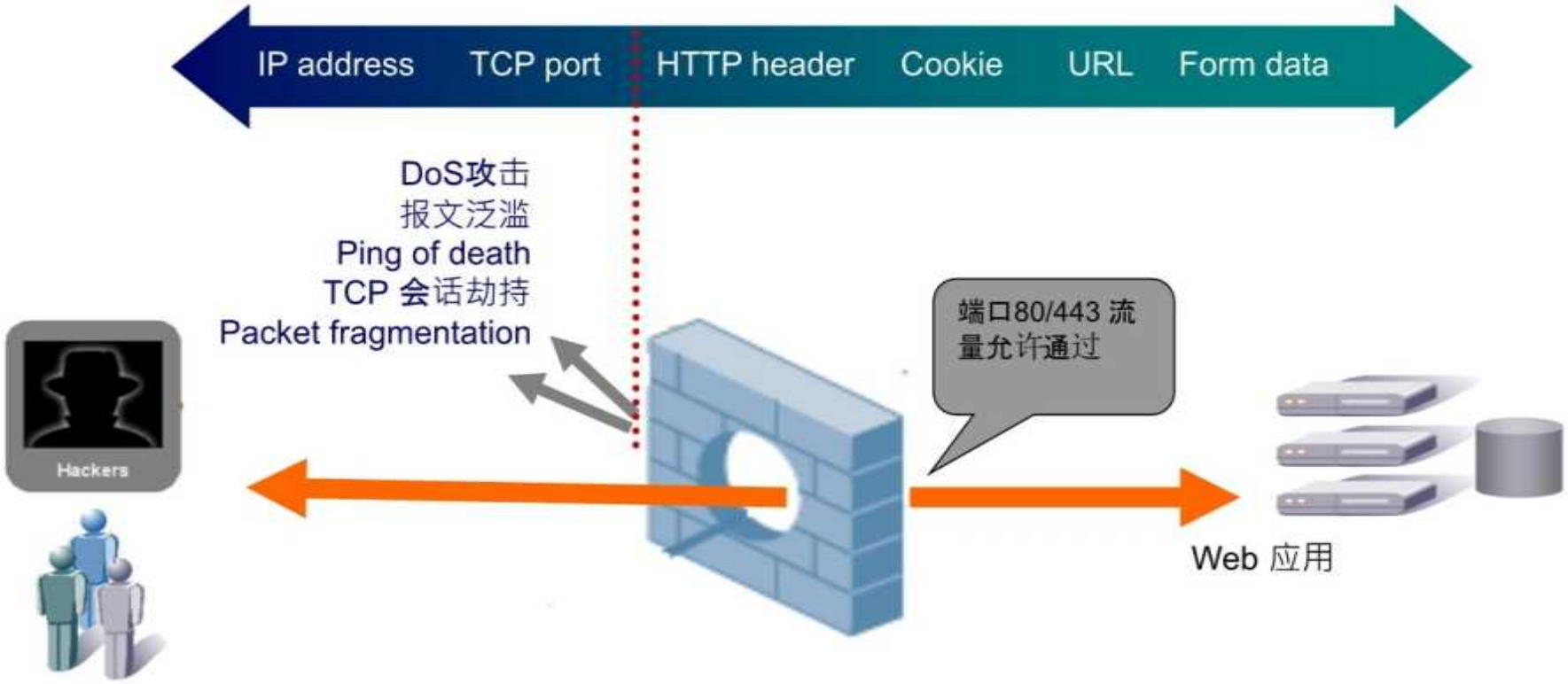
影响行业	相关法规	相关条例概述
门户网站、新闻网站、电子商务网站	互联网安全保护技术措施规定（公安部令第82号）	要求必须能够防范网站、网页被篡改
银行、运营商	互联网安全保护技术措施规定（公安部令第82号）	规定必须记录并留存用户登陆和退出时间、主叫号码、账号、互联网地址或域名

概 要

- 需求分析
- 梭子鱼Web应用防火墙功能与应用
- 市场竞争与分析
- 案例分享

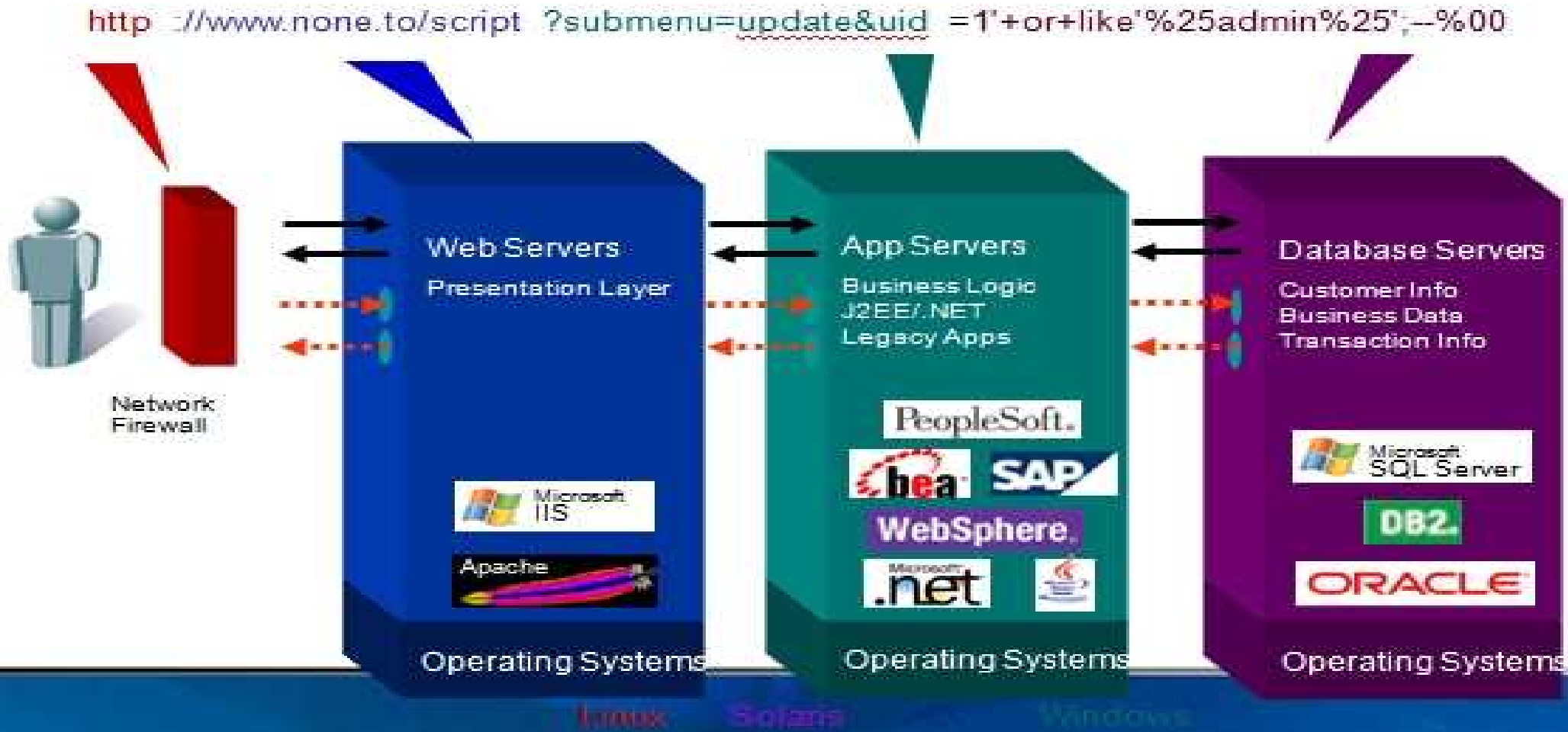
为什么传统防火墙不给力？

- **根本原因: 攻**击嵌入到正常业务流中，而这些业务流恰恰是防火墙允许通过的！



工作层次

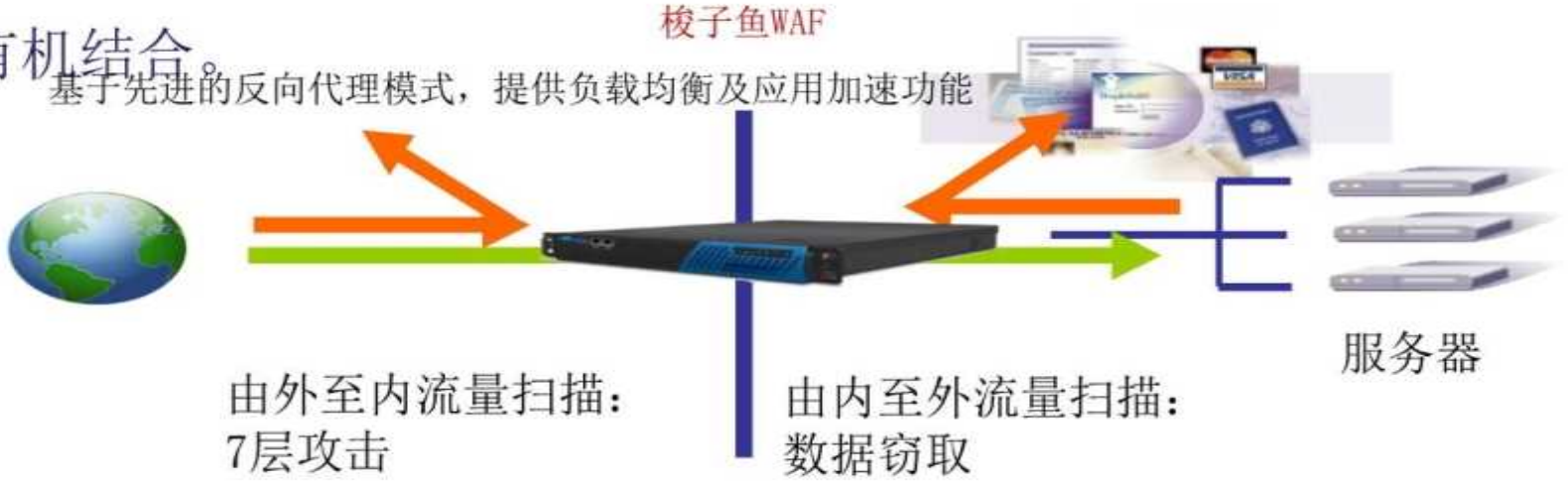
由于当今网络技术纷繁复杂，因此相应的攻击手法也层出不穷。但是“万变不离其宗”，所有的技术都是基于标准的OSI7层模型。因此，只要能够清晰地将攻击行为进行层次划分、精准定位，就能做到“对症下药”，防范于未然。



梭子鱼WAF产品理念 ： 安全防护 + 流量优化

Web应用防火墙通常工作在反向代理的模式下。能够进行TCP代理、NAT、SSL卸载、流量标准化等相关处理；同时，Web应用防火墙能够对HTTP请求和响应进行双向的扫描和过滤。

防护可以分为被动防护和主动防护。不同的防护模式考虑的角度不同，单一的防护模式无法对应用进行全面的防护，因此，完善的防护体系是被动与主动的有机结合。



被动防护：什么是危险的？

被动防护（黑名单防护）通常使用的更多。识别出一种危险的模式并且配置自己的系统阻断它。这个操作简单而有趣，却不十分安全。它依赖于人们对于危险的认识，如果问题存在，却没有被意识到（这种情况很常见），就会为攻击者留下可趁之机。

被动防护的核心是特征库，其防护质量完全依赖特征库的全面性和及时性。特征库过于庞大时，可能导致性能的下降；此外，特征库是已知攻击，无法防护未知攻击（零日攻击），最小的时间差也能导致攻击的成功入侵。

防护内容：已知的SQL注入、XSS（跨站脚本）、命令注入等攻击

被动防护的典型代表：IPS、IDS

主动防护：什么是安全的？

主动防护模式（白名单模式）是一种制定策略的更好方式，非常适于配置防火墙策略。在Web应用安全领域中，主动防护模式的核心就是为用户提供一个根据自身应用特性、完全自定义、颗粒度超细的策略配置模型。

主动防护也存在缺点，其最大的缺点就是需要花费时间进行策略的精心配置，但是防护效果佳。

目前Web应用防火墙通常都具有所谓的“学习功能”或“动态建模”，两者异名同理。学习功能属于主动防护，其工作原理就是在于Web服务器的通信过程中学习网站的参数，形成策略。优点在于能够与网站的变动保持一致，因为学习行为能够根据设定的时间间隔反复进行。

流量优化

流量优化功能并非锦上添花，而是保证业务持续可靠的强劲后盾。优秀的应用防火墙产品必须具备流量优化功能。

由于应用防火墙大部分工作处在第7层，因此需要更多的资源和时间进行数据包的分析和处理，这将加大延迟，为了弥补为了达到安全性而牺牲的延迟，必须使用流优化功能对增大的延迟进行有效弥补，甚至直接提升客户端的访问速度。

会话控制

- TCP 会话终止
- SSL 终止
- HTTP 协议恢复与遵从
- FTP 协议遵从
- HTTP 头文重写
- URL 地址翻译
- URL 速率控制

安全保障

- 应用程序伪装
- AAA 体系
- 白名单
- Forms 防护
- Cookie 防护
- 数据窃取防护
- 动态学习引擎
- SQL & OS CMD 注入攻击防护
- XSS 攻击防护
- 客户自定义黑名单

应用保障

- 缓存
- GZIP 压缩
- TCP 连接校验
- SSL 前段卸载及后端卸载
- Layer 7 内容交换
- 负载均很
- 服务器&应用程序健康检查，Failover 机制

代理技术 与 非代理技术：安全技术的本质差异

部署非代理技术WAF产品=将服务器操作系统和TCP 协议栈等直接曝露与Internet.

部署代理技术WAF产品：

- Web 地址翻译– 非代理技术无法重置地址信息
- 服务器伪装 – 非代理技术无法提供伪装
- SSL – 非代理技术的SSL速度缓慢
- Cookie 安全 – 非代理技术无法防护用户ID窃取
- L7 速率控制– 非代理技术无法防护DOS攻击
- 鉴权和认证– 非代理技术不具备AAA体系
- 防数据泄漏– 非代理技术无法对由内至外的数据提供掩护
- 响应报头加速– 非代理技术无法提供加速功能

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/577103002016006026