BARRACUDA NETWORKS

www.barracuda.com

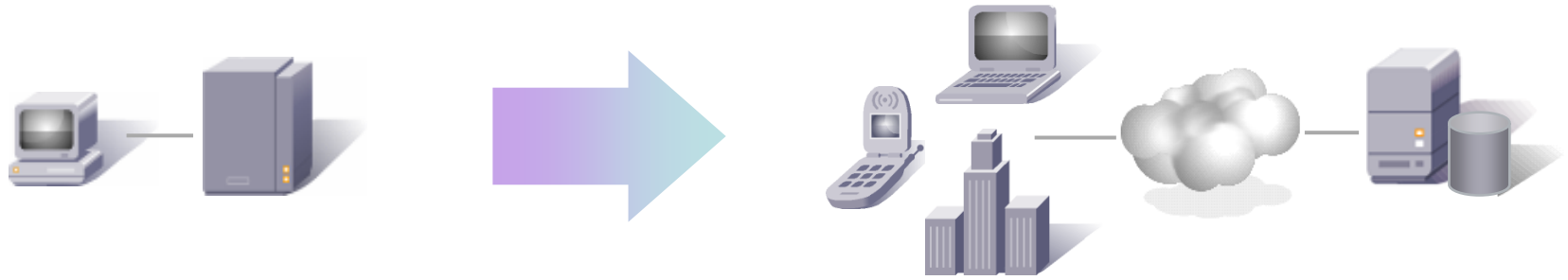
WEB应用访问安全案例剖析

梭子鱼网络（中国）

郑　爽

WEB应用究竟面临哪些威胁？

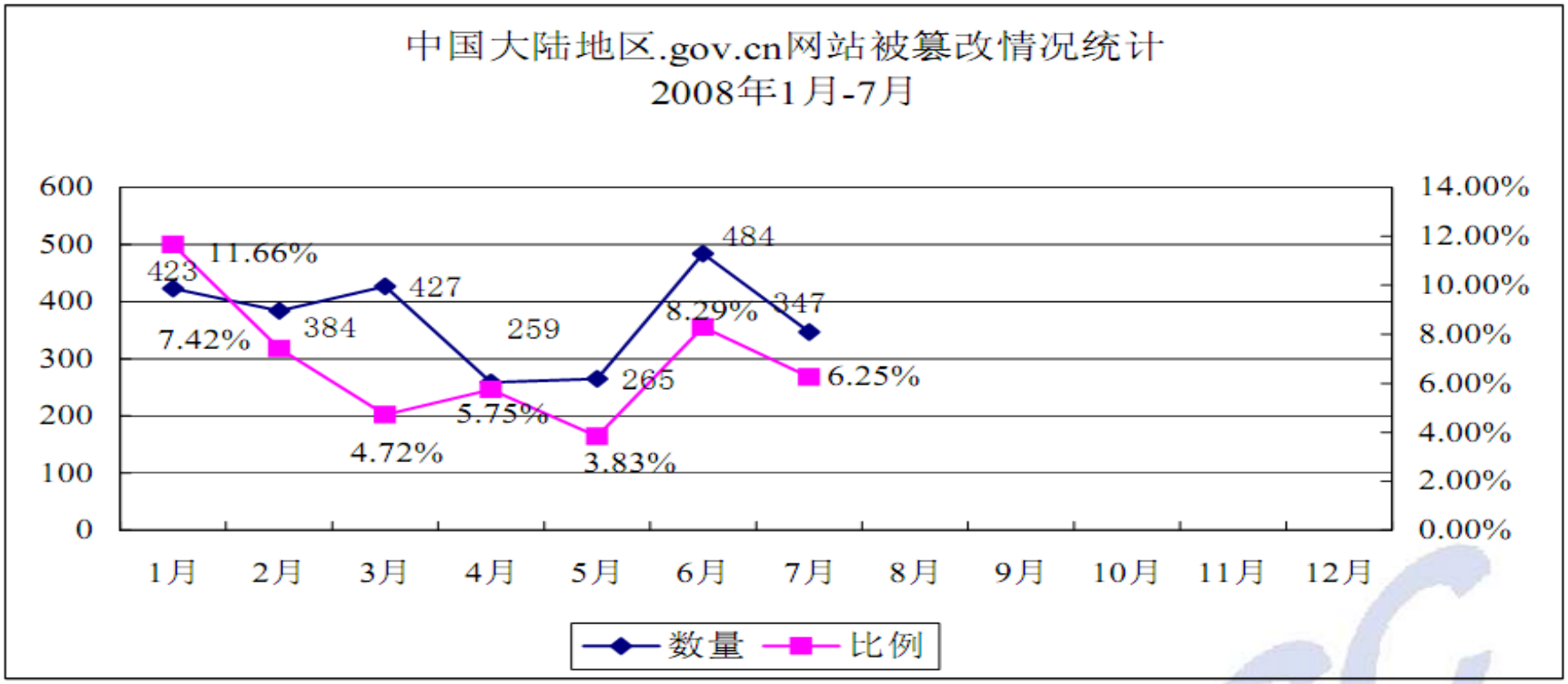
WEB 2.0发展趋势，催生黑客攻击从网络层转移到应用层



- web应用最为普遍
- 企业对外宣传、营销、甚至工作流程Web化
- 客户、员工、合作伙伴间通过web进行互动
- web网站的安全包括三个特质：保密性、完整性、可用性

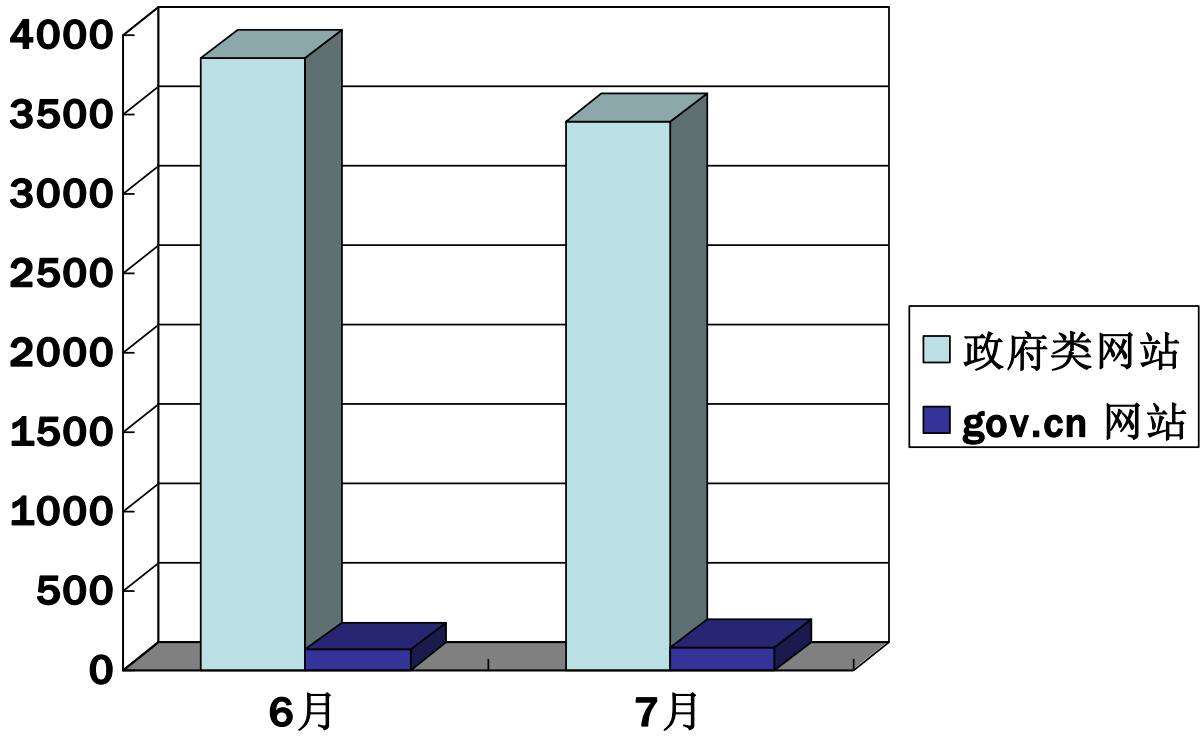
Web网站是当前最主要的安全威胁

- 75% 的攻击针对WEB应用(Gartner)
  - 2008-04 CNCERT/CC**国家互联网应急中心**监测到中国大陆被篡改网站总数达61,228个，比去年增加了1.5倍。（数据来源：CNCERT）



国家计算机网络应急技术处理协调中心

发布政府类网站被攻击数据6月（3854）、7月统计



看一个美国的统计

- 据最近的美国计算机安全协会（CSI）/美国联邦调查局（FBI）的研究表明：
- 接受调查的公司中有 52% 的公司的系统遭受过外部入侵，但事实上他们中有 98% 的公司都装有防火墙。
- 这些攻击为269家受访公司带来的经济损失——包括系统入侵、滥用 web 应用系统、网页置换、盗取私人信息及拒绝服务共计超过 1.41 亿美元。
- 美国总统奥巴马曾公开在电视媒体上讲话，每年由于黑客的恶意攻击，美国每年因此导致损失1000亿美金。

近期热点攻击事件

- 2008年6月，奥巴马竞选网站被攻击
- 2008年7月，美国某网站数百万客户资料被泄露
- 2008年10月，三鹿网站被改名为三聚氰胺网站
- 2008年，某著名网站被攻击，以校长名义发通告
- 2008年，中国大学生制作的反CNN网站被黑。
- 2009年2月，云南晋宁县政府网站被改为“躲猫猫”网站
- 2009年2月，法国驻华大使馆网站被黑。
- 2009年5月，上海车牌拍卖系统确实受到攻击
- 2009年5月，常州城市管理系统主页是城管、按摩女和黑帮的集合
- 2009年7月，新闻媒体播报的高校网页挂马问题等

为什么有这么多WEB攻击？

- 好奇心驱动

- 技术炫耀（技术学习、探索），如对政府类和安全管理相关类网站的攻击形式。

- 有组织利益驱动： 对中小企业，尤其是以网络为核心业务的企业，常采用有组织的分布式拒绝服务攻击（DDoS）攻击等手段进行勒索，从而迫使企业接受相应条件，影响企业正常业务的开展。

- 个人利益驱动 对于个人用户，攻击者更多的是通过用户身份窃取等手段，偷取该用户游戏账号、银行账号、密码等，窃取用户的私有财产。如利用网络钓鱼（Phishing）和网址嫁接（Pharming）等对金融机构、网上交易等站点进行网络仿冒，在线盗用用户身份和密码；通过恶意网页、社交工程、电子 邮件和信息系统漏洞等方式传播恶意代码；利用间谍软件（spyware）和木马程序窃取用户的私有信息，严重的可导致财产损失。

Web应用威胁都有什么呢？

员工

黑客

客户

- 窃取
- 中断
- 篡改
- 伪装

有哪些常见的攻击方式？

直接对象引用

直接利用开发人员疏忽，将目录 文件等关键对象信息获取

恶意文件执行

上传恶意代码，控制目标网站

攻击隐藏

黑客通常通过将他们的请求进行编码，以此来伪装自己的身份

Cookie 窃取

使用网络监听、篡改手段，盗取客户的登陆信息

目录穿越

攻击者能访问合法应用之外的数据或文件目录，导致数据泄露或被篡改

缓冲区溢出

破坏程序的堆栈，使程序转而执行其它指令。如获取系统管理员的权限

命令注入

将含有操作系统或软件平台命令注入到网页访问语句中以盗取数据或后端服务器的控制权

SQL注入

通过输入一段数据库查询代码窃取或修改数据库中的数据

跨站脚本攻击

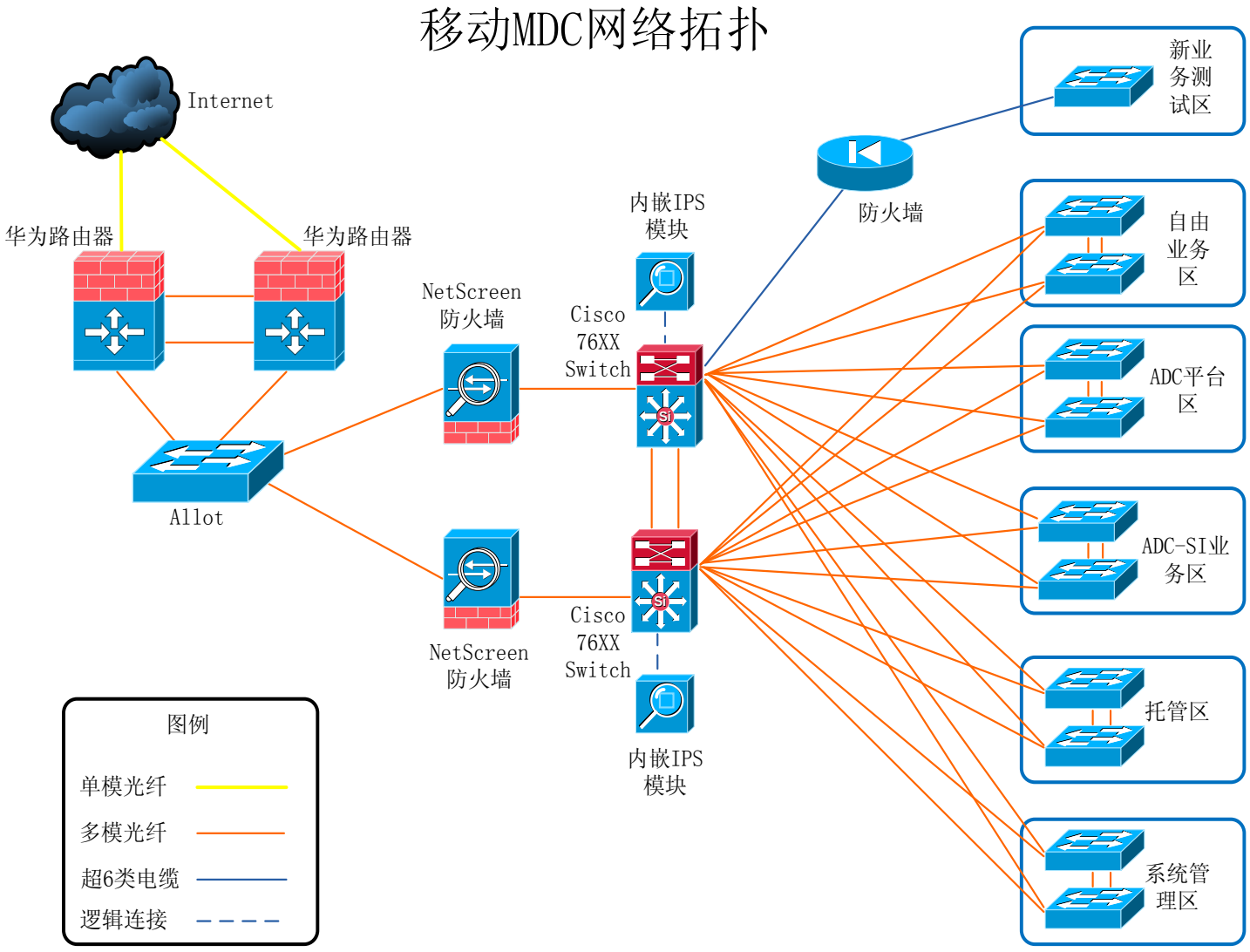
攻击访问该站点的用户，常见目的是窃取该站点访问者相关的用户登陆或认证信息

我们现有的安全部署能够阻止黑客对**WEB**应用攻击吗？

您是否已经开始有如下担心？

- 网站被攻击
- 网站被篡改
- 被OWASP 列举的前十位的攻击攻破
- 数据被窃取
- 怎么才能阻止下列攻击：
  - 跨站脚本攻击(XSS)
  - SQL 注入
  - Cookie 篡改
  - 缓存溢出
- 网站需要达到PCI标准

我已经有了防火墙、ips等防护设备已经安全了吗？



根据案例：移动MDC分析

- Allot流量控制设备，透明模式部署。
- NetScreen防火墙 ：

1）NetSreen防火墙是目前比较普及的防火墙，功能强大，性能好。

2）拦截大部分网络层攻击，例如网络层的蠕虫攻击，DDOS攻击

3)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

- 76XX交换机上内嵌IPS模块

4）完好的将ARP欺骗，2层的DDOS攻击阻挡

5）通过划分广播域的方法，将每个广播域的流量控制在本地，使病毒和非法流量不会扩散到整个MDC机房网络中

从OSI模型角度出发，4层以下的攻击基本上可以被目前网络中的安全设备完美的防御住。

IPS作用？

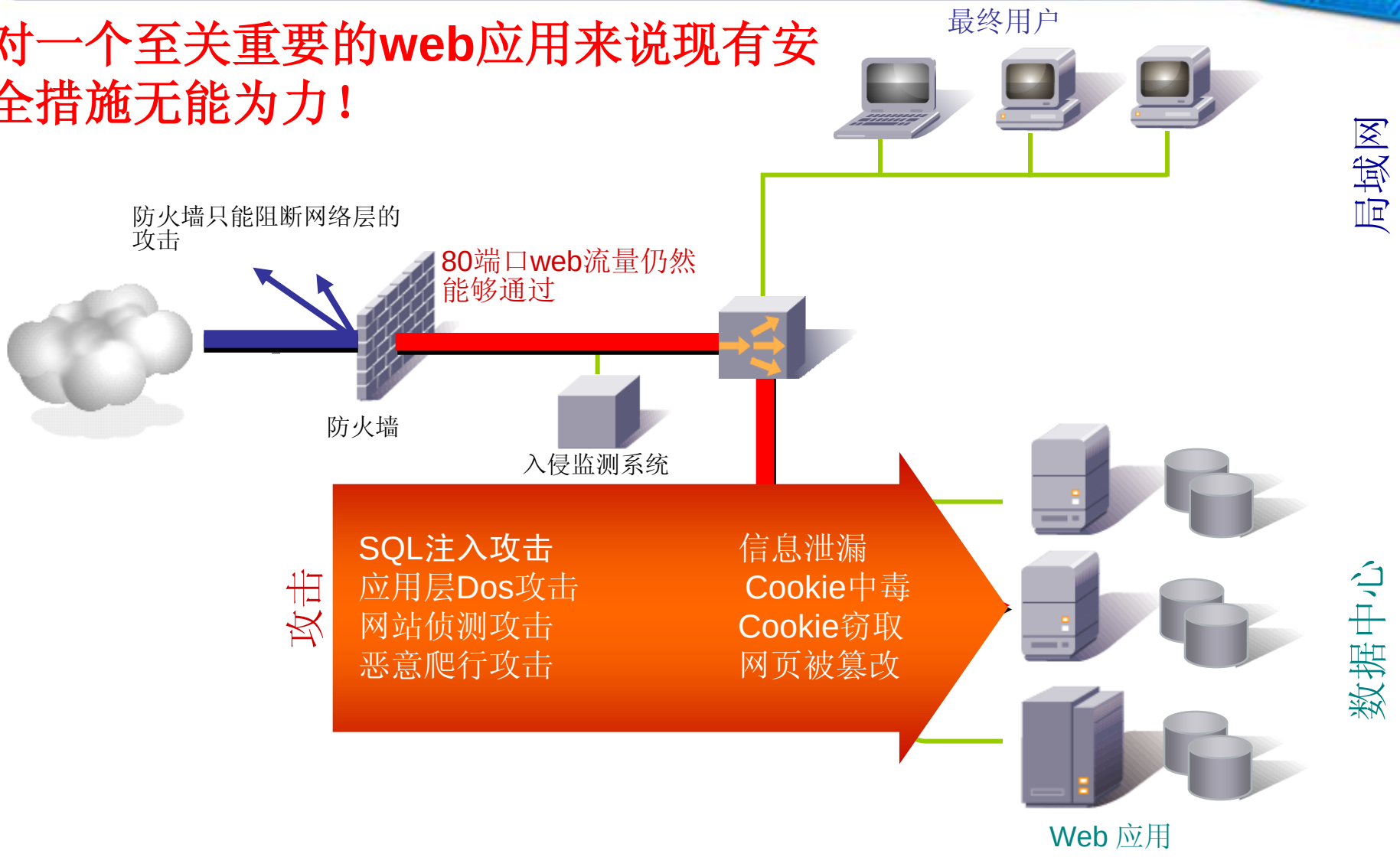
- 6）通过对数据包的7层检测来阻挡应用层的攻击；
- 7）通过特征匹配技术阻挡了大部分的主流攻击；
- 8）IPS能够阻挡“整个网络”的非法流量；

增加网页防篡改系统能够解决web服务器的安全威胁吗？

网页防篡改

9）它能够在web服务器的网页被篡改后再恢复的系统，能够保证网站的完整性

对一个至关重要的web应用来说现有安全措施无能为力！



为什么？

总结攻击特点：

- 大部分攻击在应用层
- 针对Web网站的恶意攻击绝大部分都将封装为HTTP请求
- 许多类型的攻击并不篡改网页
- 黑客往往将攻击隐藏在ssl内
- 攻击手段各种各样

传统防火墙：

防火墙工作在3、4层；

攻击从80或443端口顺利通过防火墙检测 ；

IPS入侵检测：

IPS不会对包括跨站点脚本攻击，SQL注入，命令注入，cookie密码窃取，URL编码攻击，cookie篡改，日志篡改等一系列攻击作出任何响应。

IPS最明显的缺陷在于它不能终止和处理SSL流量。

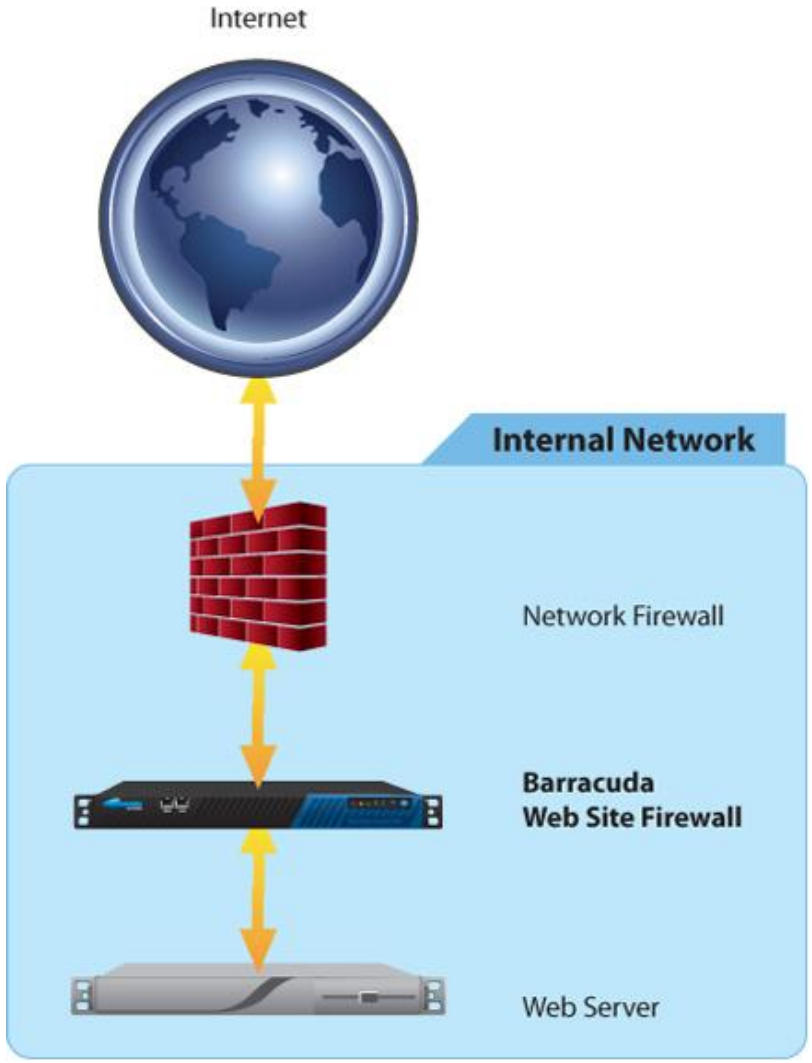
网页防篡改

对于攻击行为并不进行分析，也不阻止攻击的发生。

WEB安全是否应该交给专业的七层应用防火墙来进行策略防护呢？

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。
- 世界上唯一被ICSA在网络层和应用层上通过认证的产品



WEB应用安全功能概述

- **全面的WEB站点防护，降低商业风险**
  - 各种攻击
  - 非法访问
  - WEB站点伪装
  - WEB站点篡改
  - Outbound 数据窃取防护

- **应用传输加速**
  - 缓存 、压缩、TCP连接复用、SSL卸载和加速、负载均衡
- **审计及合规**
  - 帮助企业通过安全审计
  - 达到PCI（支付卡）应用安全规范要求
  - 美国萨班法案(Sarbanes Oxley)及其他合规性要求

PCI Requirements

	PCI 1.1 Requirements
1	Install and maintain a firewall configuration to protect data
2	Do not use default system passwords or other security parameters
3	Protect stored data
4	Encrypt transmission of cardholder data across public networks
5	Use and regularly update anti-virus software
6	Develop and maintain secure systems and applications
7	Restrict access to data by business need-to-know
8	Assign a unique ID to each person with computer access
9	Restrict physical access to cardholder data
10	Track and monitor all access to network resources and cardholder data
11	Regularly test security systems and processes
12	Maintain a policy that addresses information security

- 需求 6.5：开发安全的应用程序
- 需求 6.6：审核应用安全安全性
  - 选择 1：专业公司进行代码审核
  - 选择 2：部署应用防火墙

Web Application Security Consortium

Web Application Firewall Evaluation Criteria

Version 1.0 (January 16, 2006)

Table of Contents

- 厂商/咨询顾问的解决方案
- 作为RFI/RFP模版

十大功能、十大技术

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

技术原理

- TCP进程代理(TCP Session Full Proxy)
- Net防火墙
  - NAT, ACL, PAT
- 进程维护(Normalize Session)
- 协议遵从(Protocol Compliance)
- SSL加密 / 解密
- HTTP信头重写
- URL翻译

- 网站隐藏, 防爬行, Web地址转换
- AAA
- 应用防DoS
- SQL/命令注入
- DAP (Global and Session)
- URL ACLs
- Forms及Cookie窃取
- REGEX保护

- TCP Pooling
- 缓存, GZIP压缩
- SSL卸载, 重新加密
- 应用及服务器健康检查
- 内容交换(Content Switching)
- 负载均衡
- 记录、监控、报告

技术原理

- 识别并分析http会话；
- 策略防护
- 学习网站结构
- 加速
- 双向过滤

三步实现应用安全

1. 保护应用基础架构

- ✓ 隐藏
- ✓ Cookie 安全
- ✓ Web 地址转换

2. 根据应用强化安全

- ✓ 动态应用建模

3. 弹性安全策略

- ✓ 颗粒度极小，可高度自定义的Web 访问控制列表

超细颗粒度

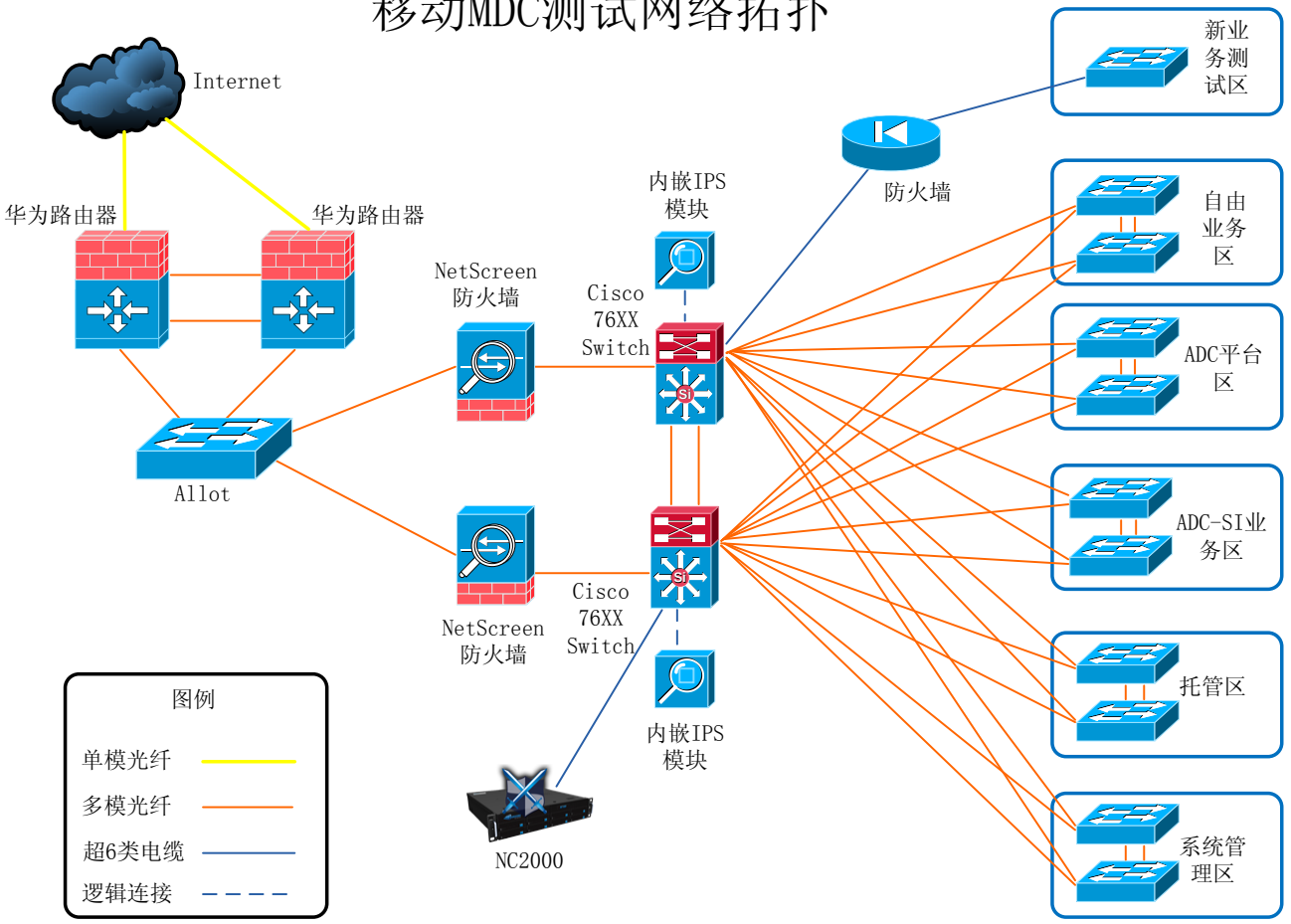
- 根据IP或应用设置安全规则（网络防火墙、某些UTM设备）
- 根据URL设置安全策略（web服务器、代理服务器）
- 根据HTTP报头设置安全策略（如请求方式、session、cookie各报头参数等）
- 根据页面参数（如表单参数、HTML元素、）
- 上述各等级颗粒度的组合策略。

流量优化技术领先

- 基于专利的NCOS操作系统，系统强壮，处理效率高。
- 综合采用TCP复用、缓存、压缩、负载均衡等技术，提高服务器响应速度，提升用户体验。
- 七层内容交换根据http报头进行内容分发。（也可以根据URL进行内容分发。）

针对MDC案例来看

移动MDC测试网络拓扑



保护服务器的类型

服务名称	服务描述	服务器数量	服务器类型
WAP	无线应用网站	1	WEB
Cai-ling	彩铃业务网站	1	WEB
Menhu	门户网站服务器	5	WEB
Pushumail	Pushmail服务器	2	WEB
Wireless	无线业务服务器	3	WEB
DNS	域名解析服务器	1	

防护策略

数据库防护： 针对wap客户信息数据，进行了SQL注入策略配置。

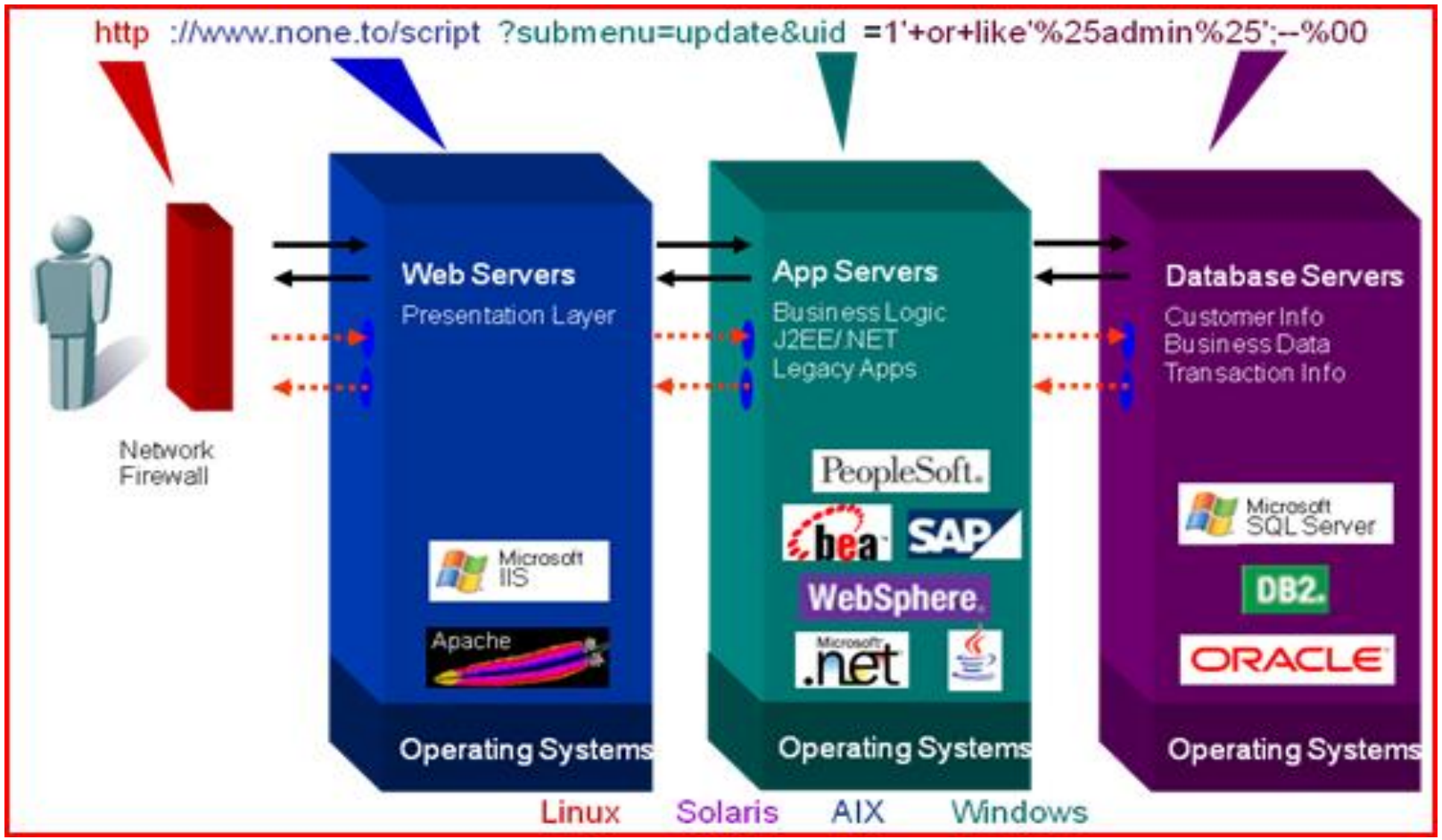
Cookie安全防护： 梭子鱼可以使用NC2000来对Cookie进行加密，在加密的过程中，NC2000会在Cookie中加入自己的标识位，这样黑客就算劫持到了会话也是无法解密的。如果黑客通过解密再加密的方式盗取Cookie，或者通过Cookie重放攻击，冒充用户本身的话，NC2000会通过IP地址进行Cookie来源的认证。

网站隐藏： NC2000可以开启Website Cloaking功能，防止黑客查看源代码中的服务器版本、Asp、.net版本

自动建模： NC2000具有强大的学习功能，可以与后台的服务器进行自动建模的操作，这个过程不需要人为的干预。学习完毕以后，NC2000上将有整个网站的架构和具体的URL。

应用层ddos防护： 通过识别Session，限制速率；对消耗服务器的同样访问进行时间/次数限制；对TCP－IP链接做各种检查

请求限制（Request Limits）



安全

标准化数据

d5opx;ÐÓGE]Ì€³óâ=
[ZÜ¾ç-Ù‰Vð„’‰<½
#Ôm]ëæoª5Zòˆ!0ˆÝ£kê
ØmtÈ ‘œín ‘k»A
H?>’5@Ì¿êÜ° Ýë;u
³7JMµ4[ø´Èò¾ø má¼

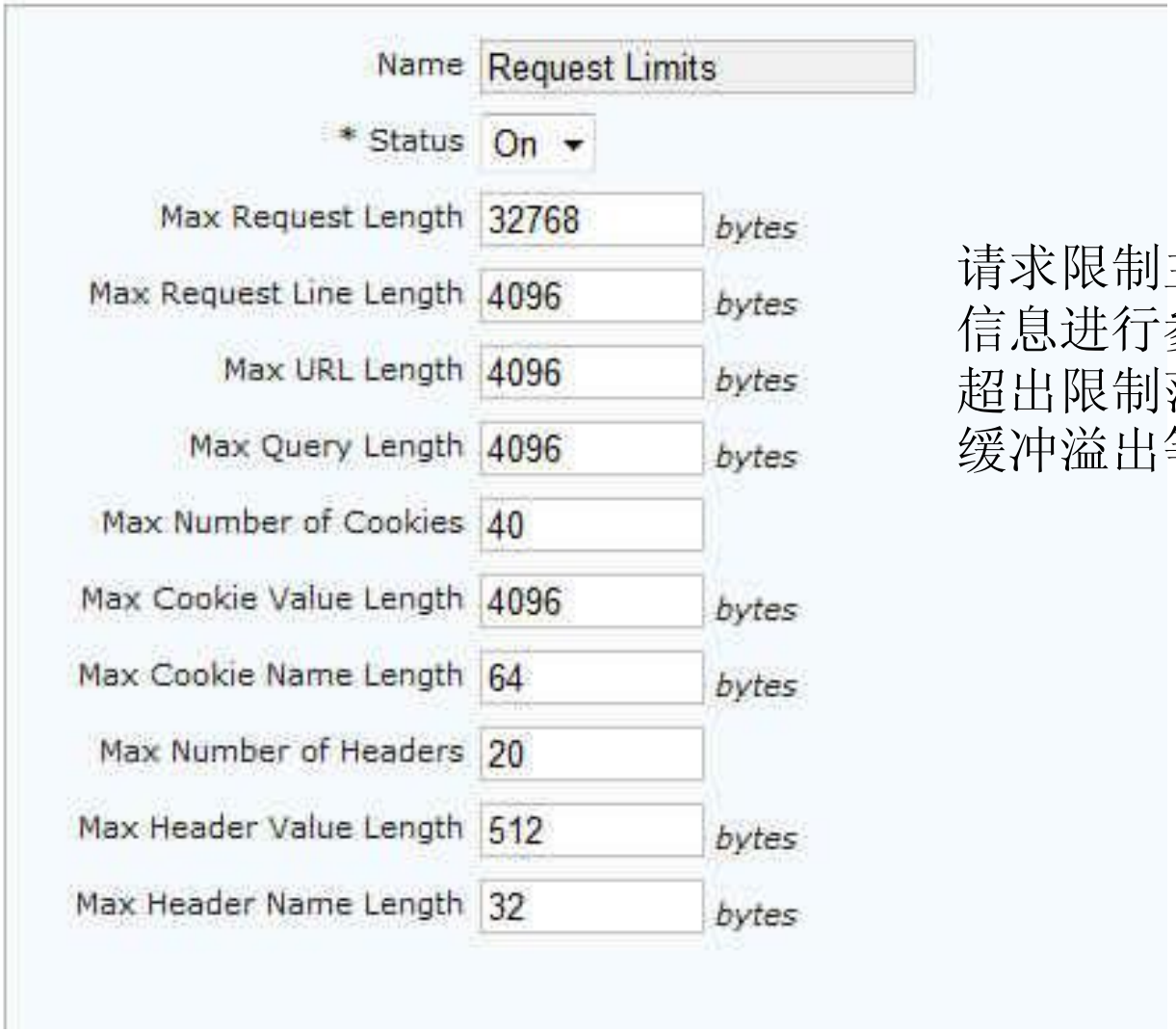
%2e%2e%2fpartners%2 ../partners/

%2ffinance%2frec%2f /finance/rec/

Decrypt SSL

Normalize

请求限制

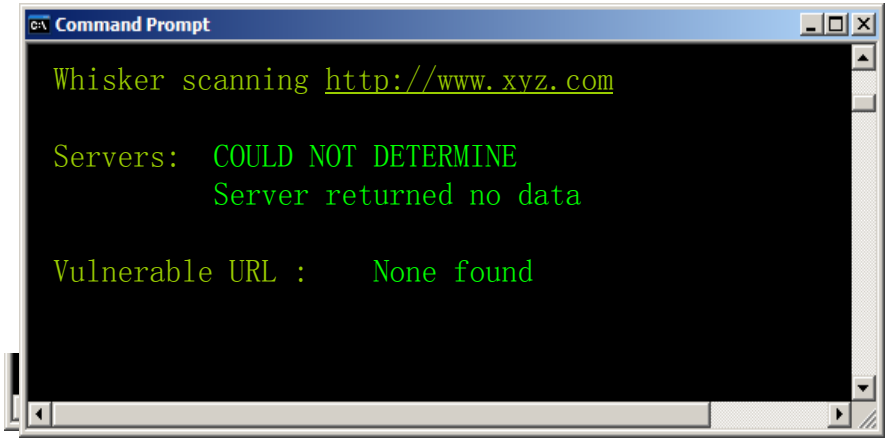


请求限制主要是对请求中的报头信息进行参数长度的限制，阻断超出限制范围的请求，保证免遭缓冲溢出等恶意攻击。

站点信息隐藏

黑客

应用防火墙



对外部访问隐身

Web服务器类型

应用服务器类型

操作系统

版本号

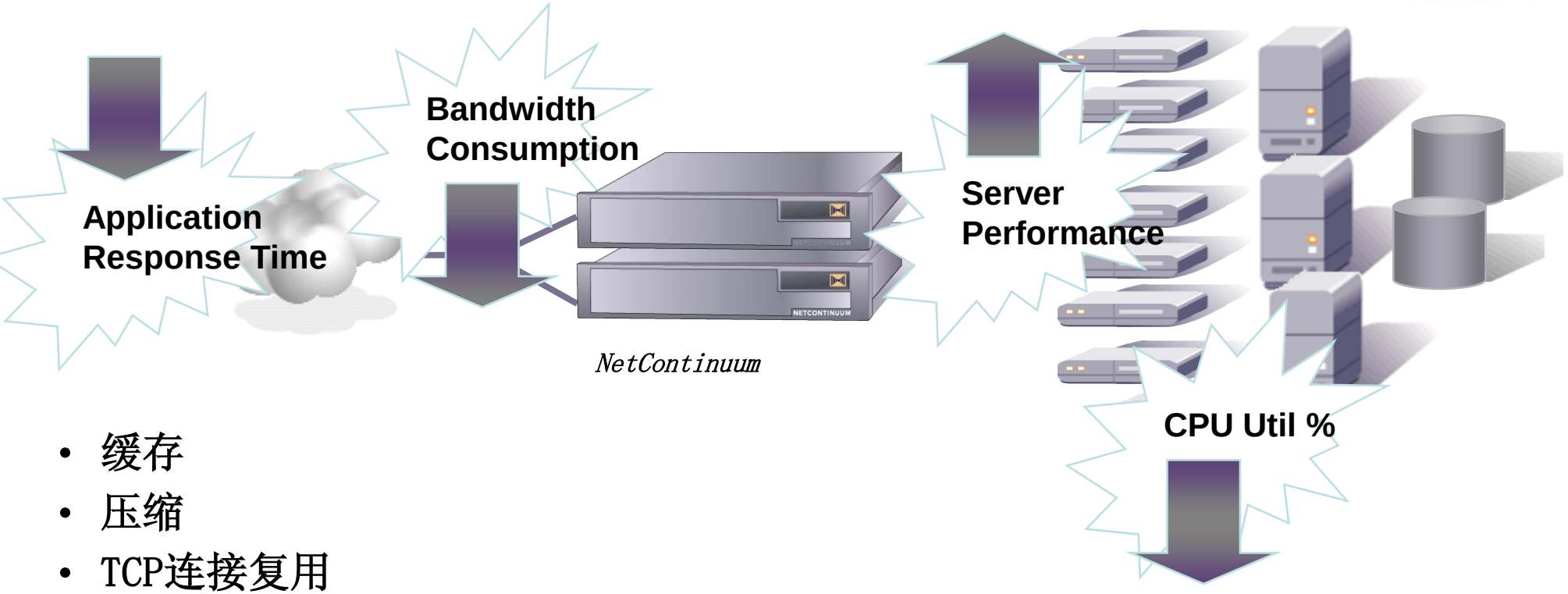
版本更新程度

已知安全漏洞

IP地址

工作站信息

加快应用的响应时间



- 缓存
- 压缩
- TCP连接复用
- SSL卸载和加速
- 负载均衡

30 – 400% 响应速度的提升以及完善应用安全

黑客攻击过程及梭子鱼防护

攻击对象扫描：端口、服务器类型、应用程序版本、数据库类型等	网站结构分析及文件目录探测	查找攻击点并尝试攻击，如SQL注入、跨站点脚本、溢出攻击等	偷窃或暴力攻击
网站隐身	URL全局防护，防止对文件或目录的非法访问	应用层攻击分析，主动防御攻击	Cookie防篡改，防DDoS攻击、防CC攻击、SSL安全访问等。

WEB应用防护优势

- **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)

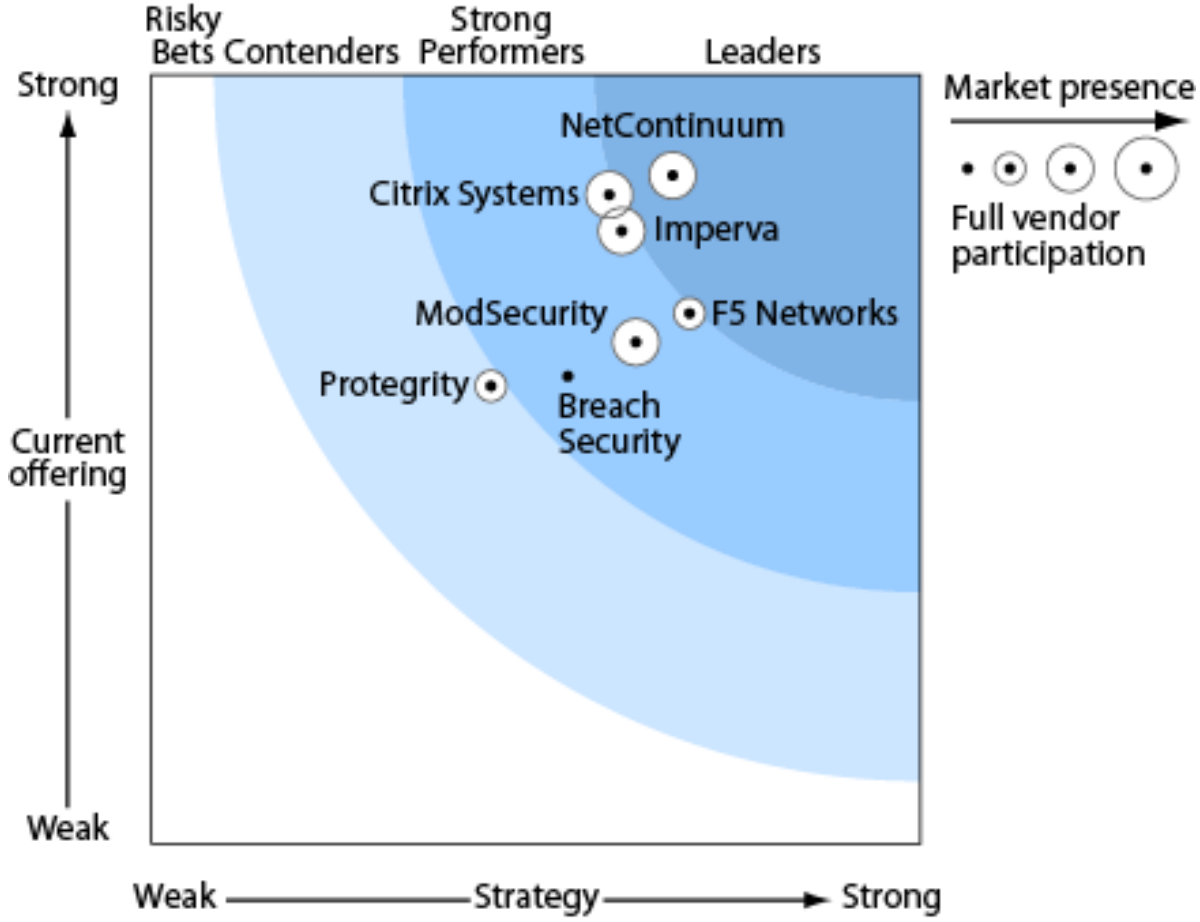
WEB应用防护优势

- 加快应用的使用
  - 网站可以提前发布，更早产生经济效益。
- 便于维护
  - 发现漏洞后，无须离线等待升级补丁。
  - 对于老的应用程序，即使维护团队不再，仍可以得到防护。
- 优化运行
  - 补丁管理
  - 日志合并和管理
  - 隐蔽内部结构，易于发布应用
  - 提高安全策略管理效率
- SSL管理
  - 初始化SSL更简洁，无须在应用程序中设定。
  - 证书授权&证书合并 ，无须在每台服务器上购买或设置证书

第三方评测： The Forrester Wave™: Web 应用防火墙评测

June 2006, Tech Choices **"The Forrester Wave™: Web Application Firewalls, Q2 2006"**

Evaluation Results For "The Forrester Wave™: Web Application Firewalls, Q2 2008"



Barracuda WAF 是Web 应用防火墙领导者

- Barracuda WAF可以用最小的配置达到最好的安全保护
- 对于以下的客户比较适合:
  - 有着最好的策略管理，阻止攻击和安全的特性的结合
  - 有着完整的登录，报告和双向的安全特性
  - 不需要企业级规模的配置
- 不同点:
  - 有最好产品管理的性能
  - 有最好的性能和加速功能

有哪些案例值得我们参考？

行业典型案例：

厦门移动	业务支撑中心WEB安全防护
辽宁移动	OA和业务支撑中心WEB安全防护
深圳全动科技	在线支付业务保护，满足PCI合规
大连工业大学	门户网站、学籍、学分等安全防护
中国农业大学	
网络教育学院	网站安全合规
格兰仕	网站认证安全
北车集团	解决SQL注入的困扰
上海市环保局	政府网站安全防范

一个值得信赖的厂商！

梭子鱼公司背景

成长

Los Altos, California
2002-2003
1,000 sq. ft.
4 phones

Cupertino, California
2003-2005
12,000 sq. ft.
50 phones

Mt. View, California
2005-2007
32,000 sq. ft.
160 phones

Campbell, California
Today
61,000 sq. ft.
230 phones

梭子鱼公司背景

发展历程

2008年累计客户达到80000家

收购Netcontinuum

年度销售超亿美元

2006年销售达到40,000台

06年推出负载均衡产品

推出WEB安全、IM安全产品

2005年销售达到20,000台，位居第一

2004年进入欧洲、日本、中国市场

2003年旗舰产品反垃圾邮件防火墙发布

2002年Barracuda Networks在硅谷成立

梭子鱼公司

- 远景
  - 开发易于使用及成本效益高的应用网络安全防护产品；
- 成立于2002年
- 梭子鱼邮件安全网关(垃圾邮件防火墙)2003年10月推出
- 梭子鱼web应用防火墙2007年1月推出（收购）
- 梭子鱼安全负载均衡机
- 总部在美国加州硅谷山景城(Mountain View)
  - 在英国、中国、加拿大、澳大利亚、印度、巴基斯坦、阿拉伯联合酋长国成立公司
  - 全球200+位以上雇员
  - 获得排名第一的风险投资Sequoia Capital及Francisco Partner 投资
- 中国区
  - 50多名员工
  - 目前除美国总部外人员最多
- 市场领导者
  - 全球超过80,000个客户

是美国最受关注的应用交付安全厂商之一

梭子鱼公司

客户横跨30多个行业

CBS.com
CATALOG.com
PRNewswire
PIXAR
The Salvation Army
Lockheed Martin
DM&S
Bridgestone Champ Car World Series
DREXEL HERITAGE
Jasc Software
CCC Commercial Contracting Corporation
Europcar
ARD Inc.
United Way
AKWireless
Navy
Coinstar
National Weather Service
WFP United Nations World Food Programme
IMMTECH Enriching lives with science
DATAMATION
The Seattle Times seattletimes.com
LOUIS VUITTON
American Red Cross
Caldwell consultants
Cabela's
MOORE STEPHENS INTERNATIONAL LIMITED
COMPUSA

梭子鱼公司

教育

UCLA

Washington State University

USC University of Southern California

MIT

Texas A&M

University of Delaware

UC Berkeley

Los Gatos-Saratoga Union High School District

政府t

United States Department of the Treasury

Department of Commerce

Department of Defense

NASA

Caltrans

City of Miami

OKC GOV Oklahoma City

金融

KPMG

ING

McDonnell Investment Management, LLC

Liberty Fund, Inc.

PlainsCapital Corporation

Austin Mutual Insurance Group

Wells Fargo

State National Bank

IT技术

Adaptec

IBM

SIEMENS

sgi United States

hp invent

集团

AAA

Bulova

Varian medical systems

Comcast

Loews Corporation

BARRACUDA NETWORKS

梭子鱼客户

SIEMENS

L'ORÉAL

GOODYEAR

DREXEL HERITAGE

YAMAHA

Pizza Hut

American Red Cross

CBS.com

Chevys FRESH MEX

PR Newswire
United Business Media

Panasonic

COMPUSA
THE COMPUTER SUPERSTORE

GMAC

LOCKHEED MARTIN

Forbes

JPL
Jet Propulsion Laboratory
California Institute of Technology

THE SALVATION ARMY

United Way

Comcast

Massachusetts Institute of Technology

WELLS FARGO

GUESS

Coinstar

FedEx

FORDHAM PREPARATORY SCHOOL
FOUNDED 1841

FOUNDRY NETWORKS

Century 21

FOOD4LESS

CITRIX

KNIGHT RIDDER

Canon

CABLE & WIRELESS

LOEWS CORPORATION

AKWireless

BOEING

The Seattle Times
seattletimes.com

adaptec

HUMANA

ING

AVIS
We try harder.

TOYOTA

PIXAR

MITSUBISHI

AAA

sbarro

Mercedes-Benz

梭子鱼公司

客户群体（包含国际知名公司）

UCLA

Mercedes-Benz

KPMG

IBM

Washington State University

hp invent

SIEMENS

verizon

McDonnell Investment Management, LLC

sgi United States

Georgia Institute of Technology

Liberty Fund, Inc.

NASA

PlainsCapital Corporation

ING

University of Delaware

UCBerkeley

State National Bank

VARIAN medical systems

MITSUBISHI MOTORS wake up and drive

Austin Mutual Insurance Group

LOEWS CORPORATION

梭子鱼产品获得的奖项

“(The Barracuda Web Filter is) an attractive proposition for the enterprise market, designed for simple administration and high throughput.”
-SC Magazine, February 2007

“Despite being heavy on the features, (Barracuda) Web Filter 310 remains easy to use and fully customizable.”
-CRN, June 2007

SC MAGAZINE RECOMMENDED

CRN TEST CENTER RECOMMENDED

网管员最喜爱的反垃圾邮件产品
Best Anti-spam Product Award

Best of CONNECTIONS 2007 Windows IT Pro WINNER

Windows IT Pro COMMUNITY CHOICE 2007 WINNER

Lotus ADVISOR AWARD EDITORS' CHOICE 2007

2007负载均衡技术创新奖
Technology Innovation Award

SC MAGAZINE AWARDS 2008 FINALIST Honored in the U.S.

Redmond MAGAZINE Best of the Best READERS' CHOICE Awards Winner ISV 2006

PRODUCT EXCELLENCE AWARDS LINUXWORLD CONFERENCE & EXPO

2006 Products of the Year SearchExchange.com

Network Computing Editor's Choice

谢谢！