Web一体化安全防护探讨

OWASP 中国

The Open Web Application Security Project

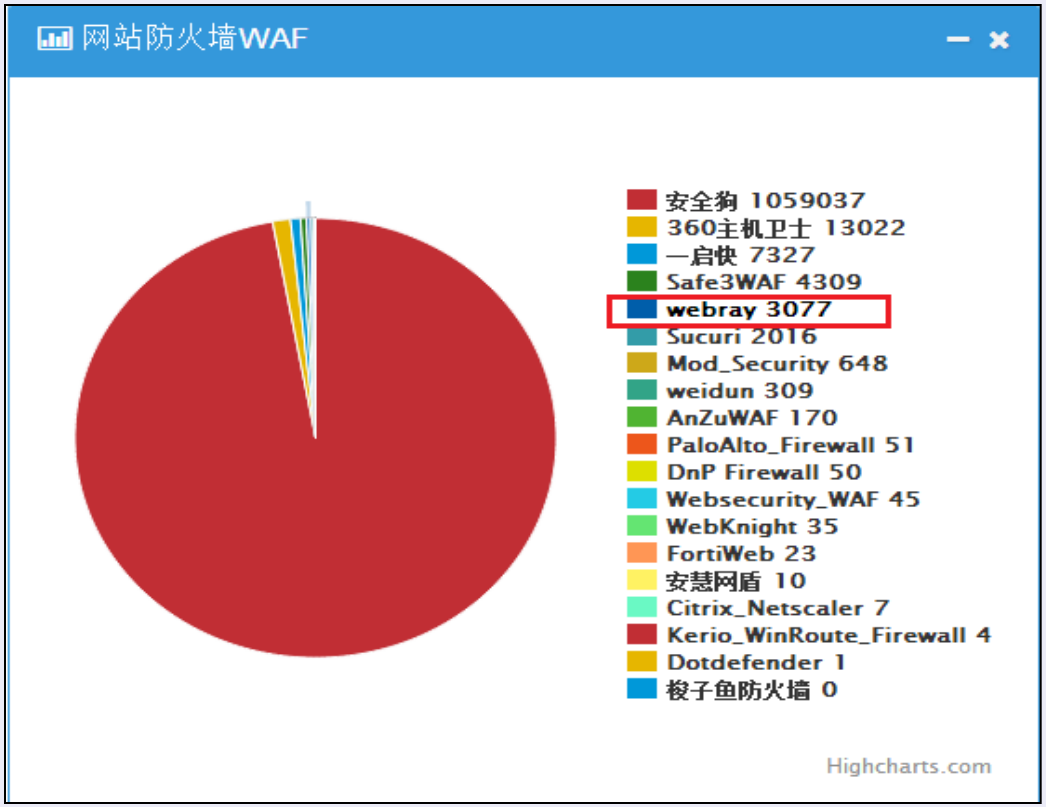
About Me

OWASP 中国
The Open Web Application Security Project

- 权小文
  - 13年安全从业经验，国企呆过，外企也混过。
  - 2009 创建WebRay公司，专做Web安全。我们发过免费Web扫描器，也做企业级WAF养家糊口。目前产品涵盖Web扫描、网站监控预警平台、Web防护墙、防篡改和异常流量清洗设备。
  - QQ: 40537240 M: 13811880491
  - www.webray.com.cn

JUNIPER NETWORKS

WebRAY



第三方检测机构fofa.so：检测的最新在线Web防护数量

大纲

OWASP 中国
The Open Web Application Security Project

第一部分 Web安全现状讨论

第二部分 一体化Web防护思路

第三部分 开放平台

OWASP 中国
The Open Web Application Security Project

第一部分 Web安全现状

- 安全事件浏览
- 现有安全防护措施讨论

OA系统


安徽新华学院
ANHUI XINHUA UNIVERSITY
数字校园 办公自动化系统
用户名(U)
密 码(P)
登录(L)
清空(C)
香港不宁！

管理系统

2014.9.3，中国东盟博览会前夕，桂林理工大学二级页面被黑。

10.18事件

事件回放：

1）2014年10月10日，外交部发言人洪磊主持例行记者会，会议上有记者提到黑客组织“匿名者（Anonymous）”，攻击中国政府网站，以表示对香港“占中”活动的支持；
2）2014年10月15日，Anonymous组织在国外Facebook等网站上公开发放攻击工具，公开招募攻击者；同时公布了攻击中国政府门户的名单，涉及147门户；

3）2014年10月12日9:30左右，首都之窗遭受来自国外的DDoS流量，大约1.2G，造成网络瘫痪30分钟；
4）2014年10月14日凌晨1:00左右，再次遭受800M左右DDoS攻击；

10.18事件

- 仍然被黑了… 这次不是Anonymous组织，是另外一个组织….

昨天晚上的故事

OWASP 中国
The Open Web Application Security Project

主　题：【WebRay监控中心】 一级警告：网站【http://kjc.njtu.edu.cn】被非法篡改 [举报垃圾邮件] [新窗口打开]
时　间：2014-11-05 20:34 (星期三)
发件人：mailsender@webray.ams [添加到通讯录] [邮件往来] [拒收]
收件人：(无)
附　件：./img/njtuB.JPG (266.29K) 下载

2014年11月5曰夜，拿下北京交通大学科技处。

http://kjc.njtu.edu.cn 北京交通大学科技处

Web攻击趋势

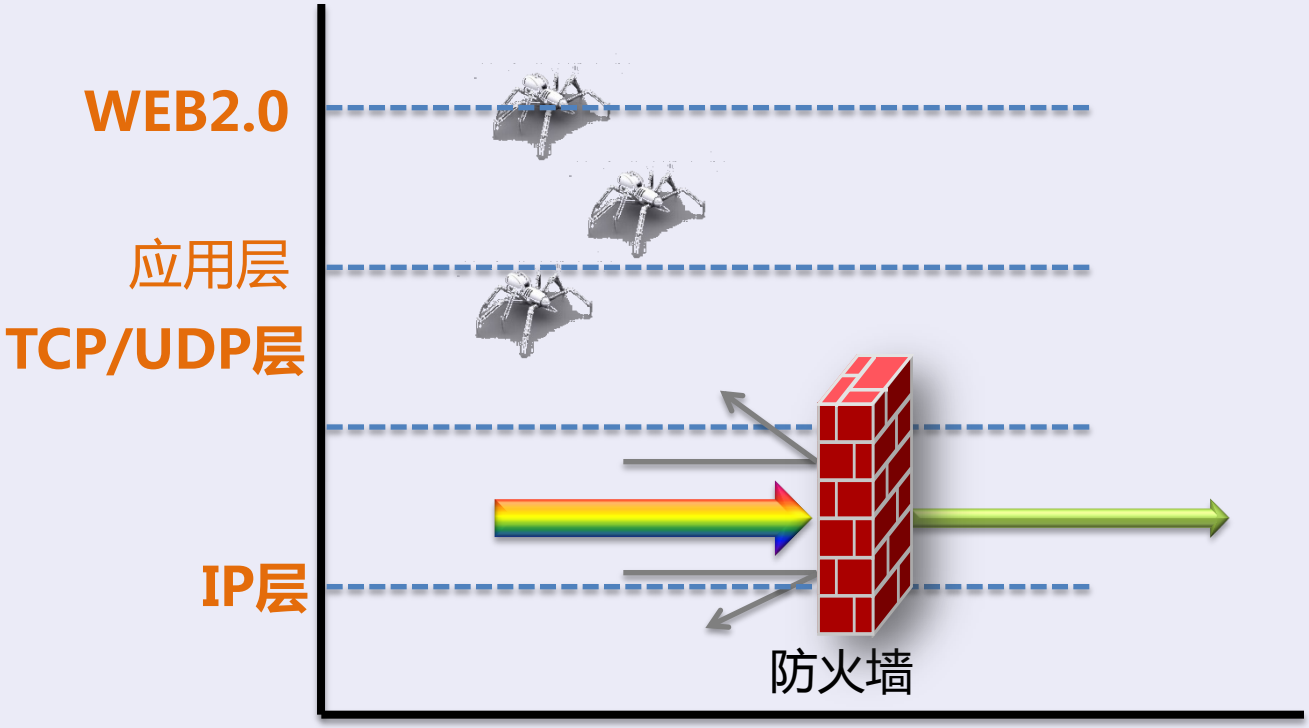
- 1. 二级站点攻击增多
- 2. WAP等面向移动的站点增多；
- 3. 英文等不常用网站增多
- 4. 安全属于长期的、此消彼长型对抗的过程，需要持续关注

- Web防护是一个长期持续的工作，不是一套设备就能解决的，需要考虑安全运维

答案在哪？

- 为什么部署了大量安全设备后，仍然不能降低风险？

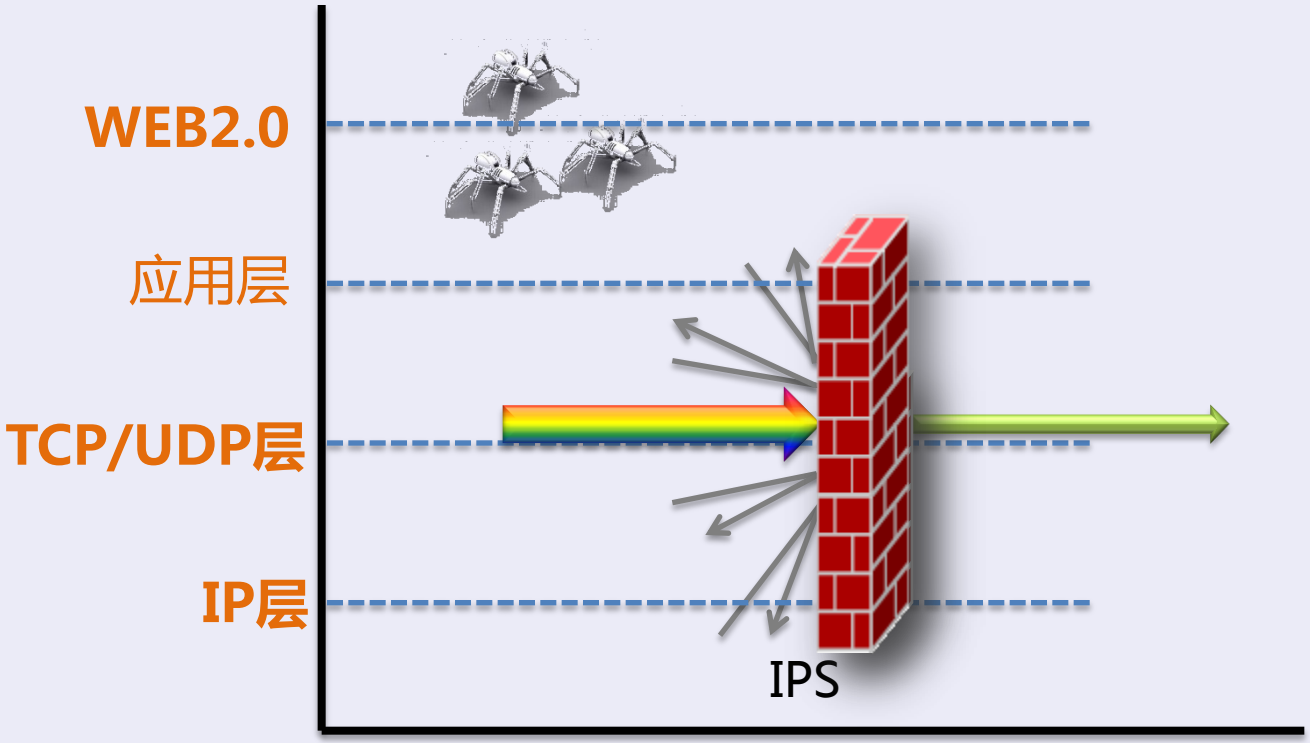
防火墙



- 检测网络层攻击
- IP地址、端口等
- 对Web层无防护

防火墙无法阻止从**内部**发起的攻击行为

IDS/IPS

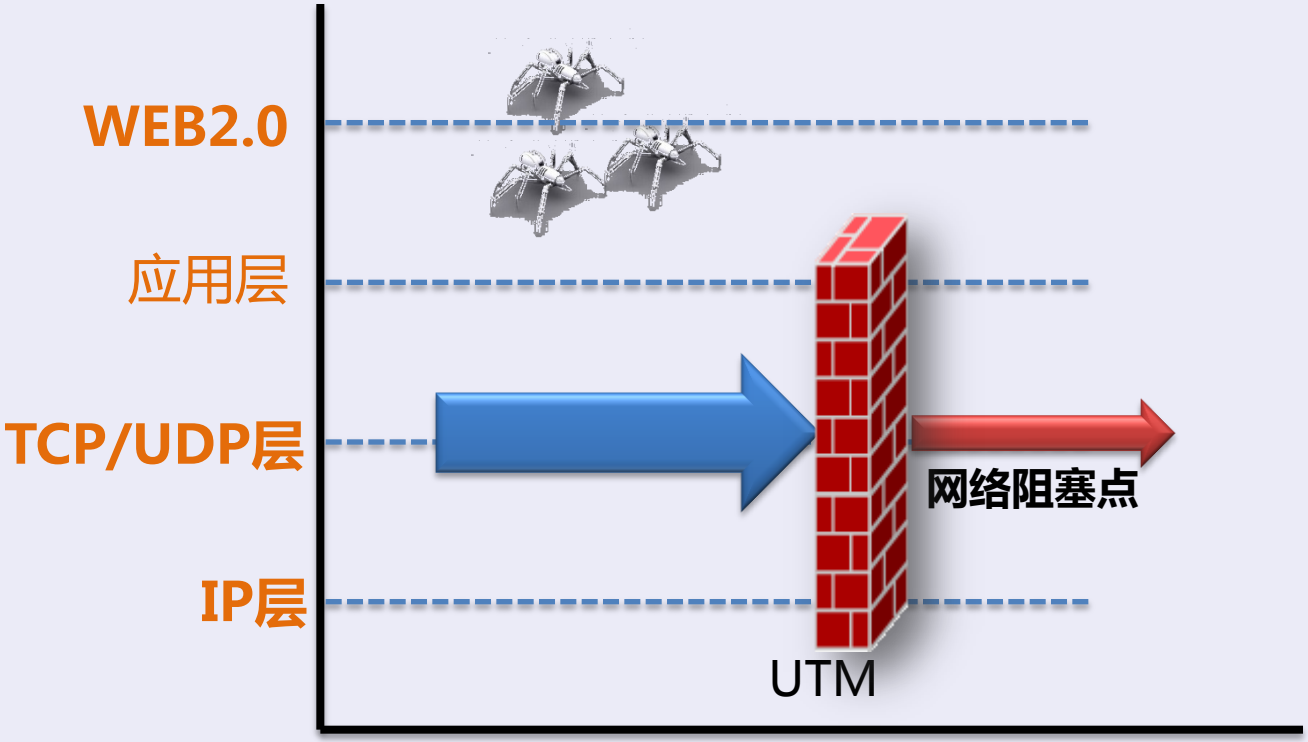


- 针对Web应用深度不够
- 只检测已知协议

IDS是单纯的入侵检测，负责**记录**入侵行为

IPS是入侵防御，可以抵御**部分**对WEB应用的攻击

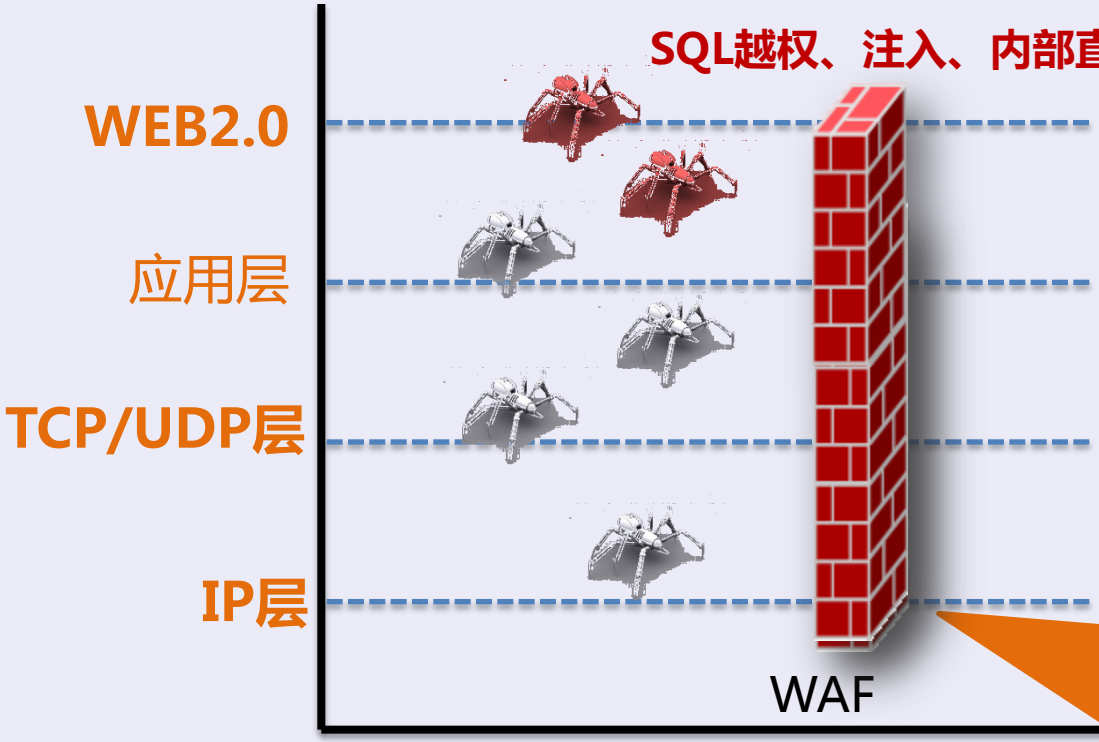
UTM



- 具备其他产品瓶颈
- 性能瓶颈

UTM是一种**宽泛**的防御，集成防火墙，IDS/IPS，VPN，网关杀毒，反垃圾邮件等多种功能于一身

NGFW



1. 能够阻止部分SQL注入攻击、跨站攻击
2. 无法阻止内部对数据库的攻击

正常： delete from table1 where name = 'John'
越权攻击： delete from table1
SQL注入： select * from stock where catalog-no = '' having 1=1 -- ' and location = 1

NGFW策设计

传统防火墙策略

应用层过滤

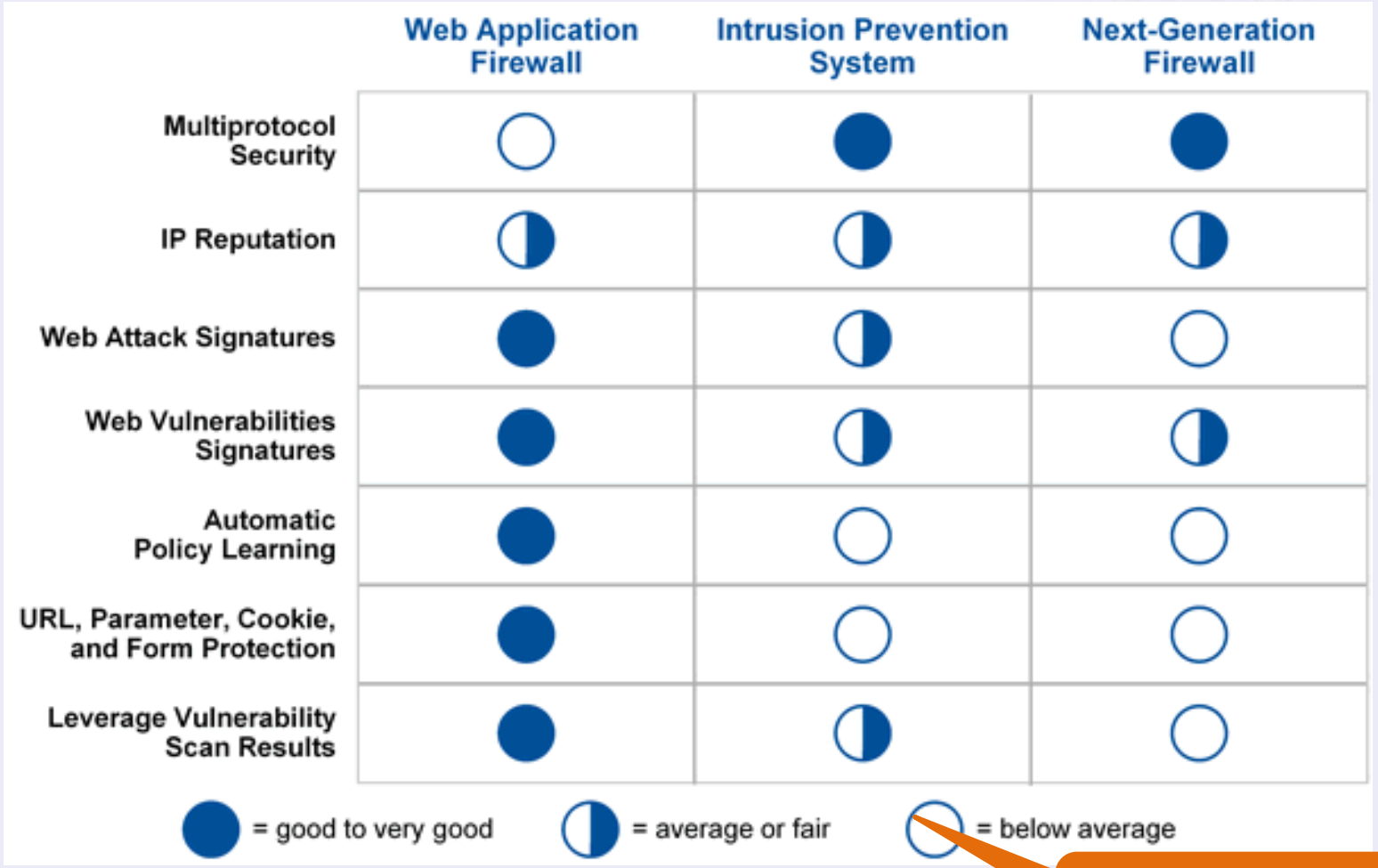
应用层防护

Source Address	Destination Address	Service	Action	AppFW	IPS	Description
Global Policy Pre Rules (0 rule)						
Device Rules (2 rules)						
Client-Network	Any	http	Permit + AppFW + IPS	P2P:File-Sharing Remote-Access:Tunneling Web:Anonymizer	Recommended	Allow outbound traffic on http-port, Block unwanted traffic and Protect against attacks to the clients
Any	My-Web-Server	http	Permit + AppFW + IPS	HTTP	Web_Server	Allow traffic to my web-server. Make sure that only HTTP is allowed Protect web-server against attacks.
Global Policy Post Rules (0 rule)						

基于黑名单应用阻断

白名单访问

NGFW-WAF-IPS



Gartner 2014报告

答案在哪？

从源头建立的第一道和最后一道防线

- 安全是个体系
- 不同视觉看看安全

OWASP 中国
The Open Web Application Security Project

第二部分 一体化防护思路

- Web安全生态链
- 一体化防护方案

OWASP 中国
The Open Web Application Security Project

Web生态图

网站入侵

WEB漏洞发现

暴力破解

DDoS

跨站脚本

SQL注入

攻击者

防火墙

信息窃取

网页篡改

网站系统

安全防护

WEB漏洞扫描和修复

双向流量的过滤与清洗

网页恢复

审计追查

非法入侵

网页篡改

信息窃取

Ddos

网站挂马

WebRay方案

产品

WEB漏洞扫描系统

抗拒绝服务系统
WEB应用防火墙

网页恢复系统
安全审计系统

服务

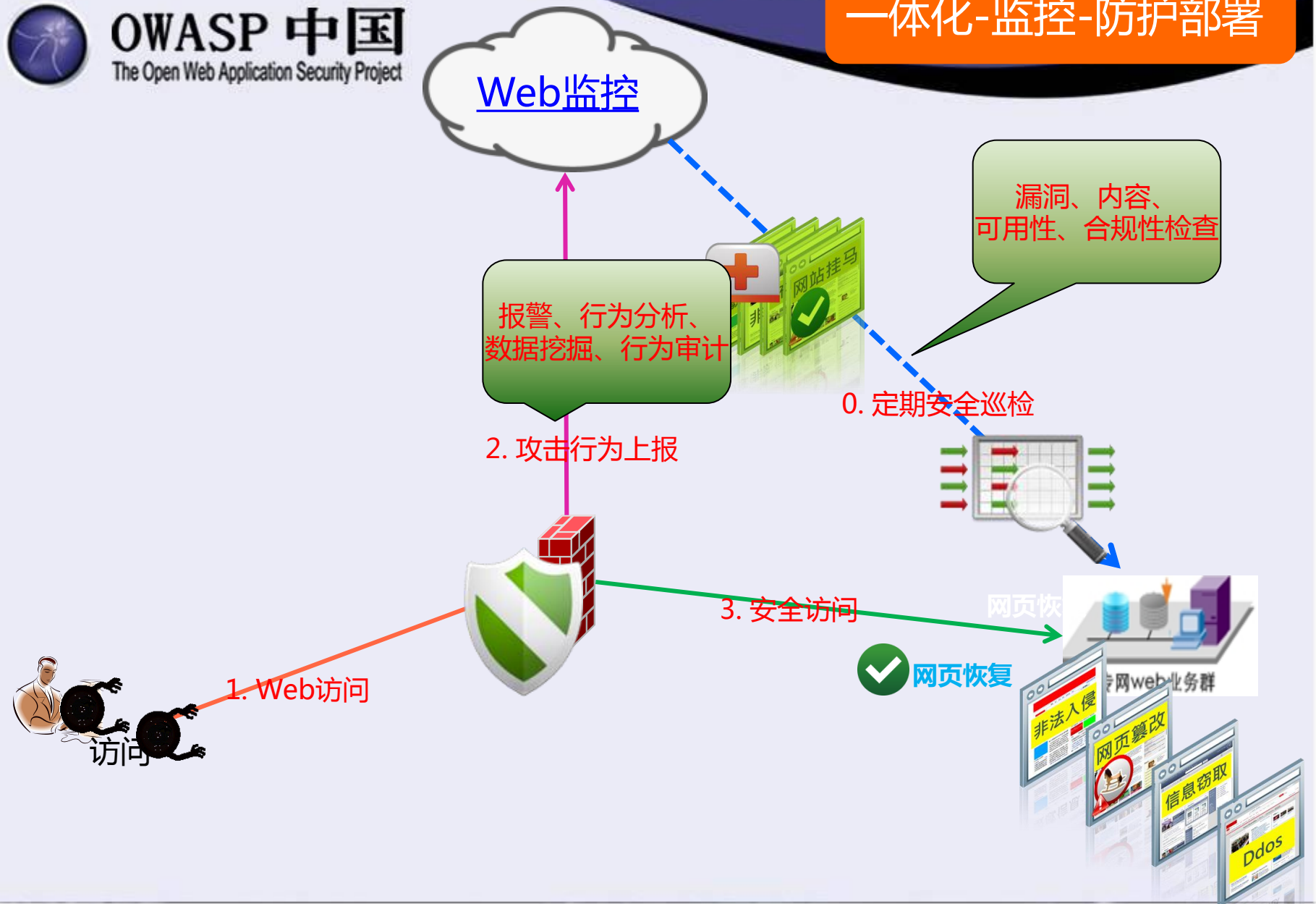
安全评估与加固
渗透测试

安全值守

应急响应
事件追溯


Web应用的集中监控
Web应用的管理
Web安全
Web应用的防护

一体化-监控-防护部署


Web监控
漏洞、内容、
可用性、合规性检查
报警、行为分析、
数据挖掘、行为审计
网站挂马
0. 定期安全巡检
2. 攻击行为上报
3. 安全访问
网页恢复
网页恢复
1. Web访问
访问
非法入侵
网页篡改
信息窃取
Ddos

过程分解

基于数据流防护

1. WAF&DDoS流量清洗
2. 网页防篡改防护

基于预防的防护

1. 定期安全巡检
2. 定期安全监控扫描
3. 数据流量总结、分析
4. 系统日志的挖掘和分析

老三样

事前

- Web扫描器
- 漏洞扫描器

事中

- Web防火墙
- 异常流量清洗

事后

- 网页防篡改
- 审计

监控预警平台

引子：
2014年10月21日20:22，首都之窗-，网站遭到非法篡改攻击，网页被篡改，因为四中全会

主　题：【WebRay监控中心】一级警告：网站【http://www.
时　间：2014-10-21 20:21 (星期二)
发件人：mailsender@webray.ams [添加到通讯录] [邮件往来] [拒收]
收件人：(无)
附　件：./img/bjipoB.JPG (110.73K)

2014年10月21日夜，拿下北京市知识产权局手机版。

http://www.bjipo.gov.cn/wap 北京市知识产权局手机版
曰的，开你玛逼的四中全会！"

oRay报警短信

我们的响应：
1）通知专利局值班人员，他们认为谎报
2）通知首都之窗总值班室，10分钟内网站关停

所有文件夹 >> **搜索结果** 已搜索到 15 封关键字为" **mailsender** "的邮件。

删除 | 举 报 | 导 出 | 标记为... | 移动到... | 更多...

发件人	主题
日期：昨天（1封）	
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://kjc.njtu.edu.cn】被非法篡改
日期：更早（14封）	
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://www.mgggzy.gov.cn】被非法篡改
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://www.thjdpx.com】被非法篡改
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://oa.axhu.cn】被非法篡改
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://www.lslushan.com】被非法篡改
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://www.bjipo.gov.cn/wap】被非法篡改
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://www.sclswsxx.cn】被非法篡改
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://www.naggzy.gov.cn】被非法篡改
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://www.zqgxczj.gov.cn】被非法篡改
mailsender	[收件箱] - 【WebRay监控中心】 一级警告：网站【http://www.syzwzx.com.cn】被非法篡改

我们的经验

逢重大事情
- 必有恶意网络攻击

有防护设备
- 请检查防护设备配置

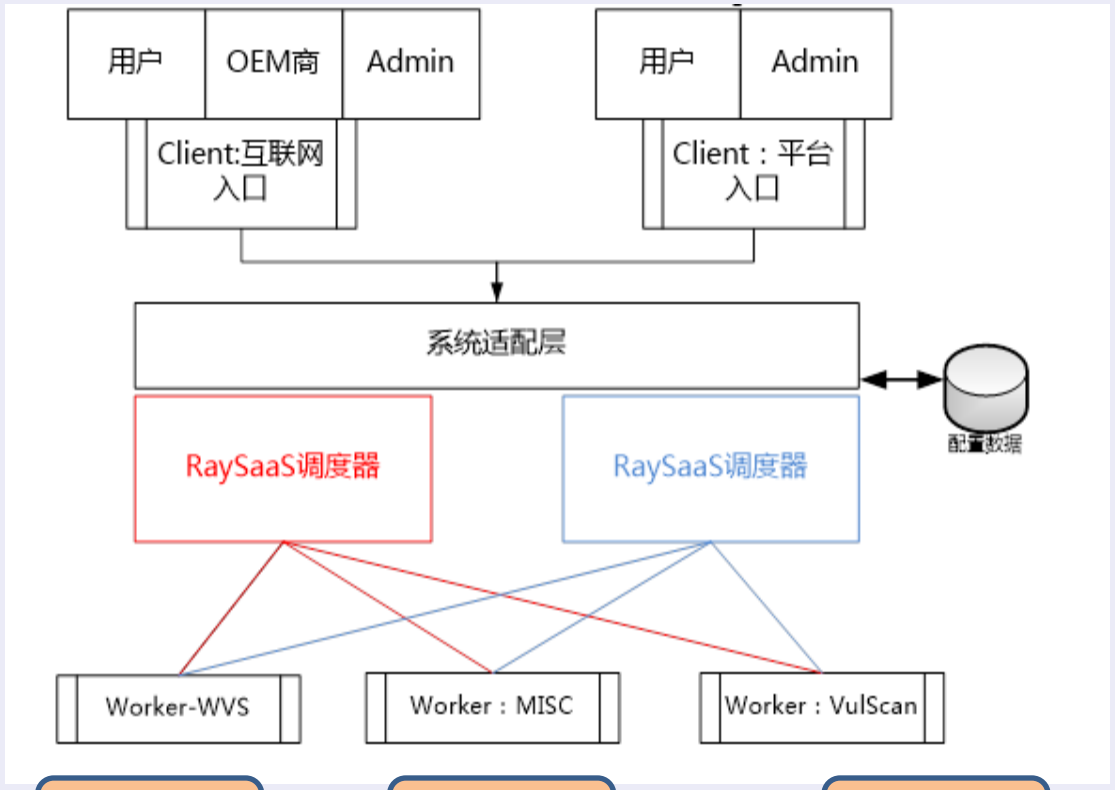
没有防护设备
- 做好前期预防工作

啥都没准备
- 最短时间内预警,及时处理，降低影响....

OWASP 中国
The Open Web Application Security Project

- 开放平台RaySaaS 欢迎合作开发

开放平台



主流语言均支持(Java、python、php、C/C++)

主流平台支持(Linux、Windows、Unix

互联接口就是一个配置文件(xml)

案例(端口扫描)

raycall -e nmap –c nmap.conf

OWASP 中国
The Open Web Application Security Project

网站监控预警平台

WebRay公司成立2009年，专注Web安全，解决服务器面临的安全问题。

基于具有**自主知识产权**的 RayOS安全系统开发：

①新一代高性能应用安全系统

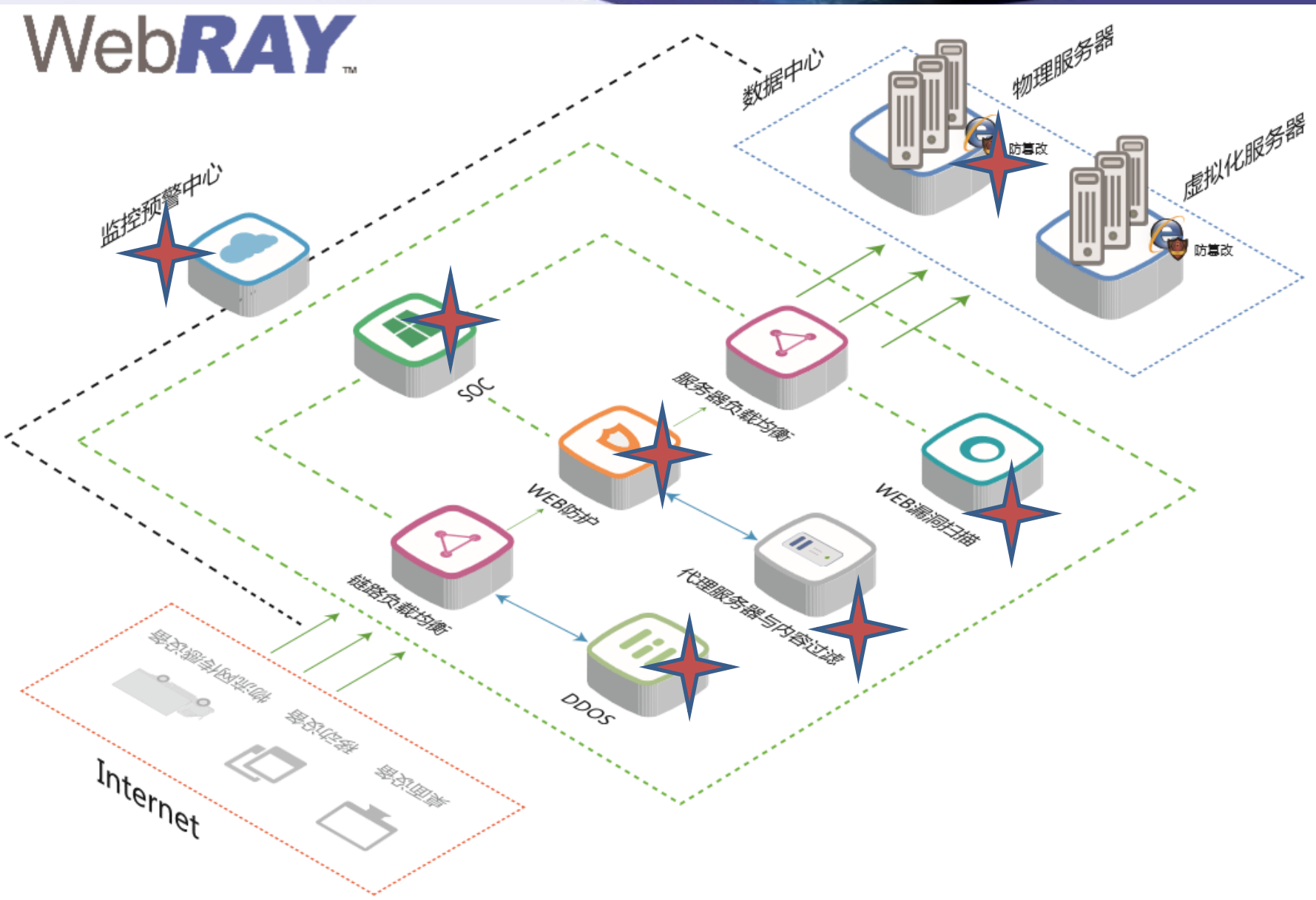
②安全检测类

③防护类（WEB应用防护系统、抗DDoS攻击、网页篡改防护系统）

④云检测与运营平台

实现“事前、事中、事后”的全方位多维立体安全的防护体系，构造基于企业安全的云运营平台。

主要产品


WebRAY
数据中心
物理服务器
虚拟化服务器
防篡改
防篡改
监控预警中心
SOC
服务器负载均衡
WEB防护
WEB漏洞扫描
链路负载均衡
代理服务器与内容过滤
DDOS
Internet

OWASP 中国
The Open Web Application Security Project

欢迎指正，谢谢！