



2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

电商企业网络安全现状及应对系统演进

我是王华侨，来自兰亭集势（外贸B2C）

个人称号：HonestQiao，乔楚

江湖称号：小乔，老乔，帮主，乔大妈

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

聊点什么

- 一次抵御网络攻击的切身经历
 - 攻击又来了
 - 穷尽办法应对
 - 有人敲诈
 - “累”就一个字
- 一个主动监测防御的系统
 - 上纲上线
 - 装在套子里的“人”

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

攻击来了

- 3月28日，内部邮件：

昨天晚上8:10至今天凌晨4:00，我们遭受到一轮非常严重的DDOS攻击

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

穷尽办法应对

- 来势凶猛
 - 晚上8:10 报警，网站连不上
 - SA登录服务器检查
 - 很快连不上硬件防火墙

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

穷尽办法应对

- 开始应对
 - 加入到TMS防御
 - 大量丢包，干扰部分正常用户
 - 改写访问地址，404错误

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

穷尽办法应对

- 进一步应对
 - 发现TCP flood和页面GET请求混合攻击
 - 重定向index.php的请求
 - 没有refer的请求，定向到静态页面
 - 切换IP
 - 切换到备用机房
 - 使用验证码

有人敲诈

[17:29:38] Emma: may I have that person's contact number?

[17:29:41] john: **he will pay me every month**

[17:29:48] john: **800\$**

[17:29:52] john: if i will stop ur site

[17:29:57] john: if **u will pay me 1000\$**

[17:30:00] Emma: where did you get this info, john?

[17:30:32] john: someone own a site

[17:30:35] Emma: how can I trust this, john?

[17:30:38] john: like urs

[17:30:39] Emma: can you tell me that site link?

[17:30:46] Emma: do you have the site name?

[17:30:50] john: i dont want troubles

[17:30:55] Emma: I understand

[17:30:57] john: if u will pay me

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

“累”就一个字

- 连续加班
- 疲于应对
- 精神恍惚

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

绝不能就这么完了

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

上纲上线

- 历史攻击状况和防御方式总结
- 网络攻击的种类
- 基本防御手段
- 我们要构建一个系统

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

历史攻击状况和防御方式总结

- 攻击水平在逐年提升
 - 2010年：频繁，但规模较小
 - 2011年：多次，成规模攻击
 - 2012年：规模化和智能化

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

历史攻击状况和防御方式总结

- 落后的防御手段
 - URL跳转
 - 人工筛选URL，Nginx配置跳转
 - 操作系统防火墙
 - 封禁IP地址
 - TMS 防火墙
 - 机房设置，操作滞后，容量有限，丢包严重

网络攻击的种类

- SYN/TCP flood
- WebServer的GET请求

SYN/TCP flood

- 恶意的数据包
- 防火墙过载
- WEB服务器网络连接数过多

WebServer的请求

- 伪装正常HTTP请求
 - 规模大
 - IP分散
- 动态页面请求
 - QPS瓶颈页面

基本防御手段


攻击种类	防御手段	效果	风险
SYN flood	防火墙	较好，对防火墙CPU要求高，带宽要求高	流量过大会误杀
TCP flood	防火墙	较好，对防火墙CPU要求高，带宽要求高	流量过大会误杀
http flood	Nginx 访问次数限制，验证码限制	快速，参数易于调节	限制越严格，约容易产生误杀。导致用户流失
iops	增强cache能力，采用验证码	性能提升，防御生效	带宽占用不减

我们要构建的系统

- 核心目的：**懒**
- 项目目标：
 - 实时数据采集分析
 - 预判是否存在攻击
 - 主动进行防御操作
 - 避免被动处理

我们可以用什么

模块	参数调整	自动?
Firewall/EthProxy	NO	NO- Always on
Firewall/Cisco	Yes	No- Always on
Nginx	Yes	Yes
Defence checkcode	Yes	Yes



All Defence – 全部加验证码
风险国家加验证码
红色级别限制访问
橙色级别限制访问
正常级别限制访问
IP白名单
手工加入白名单

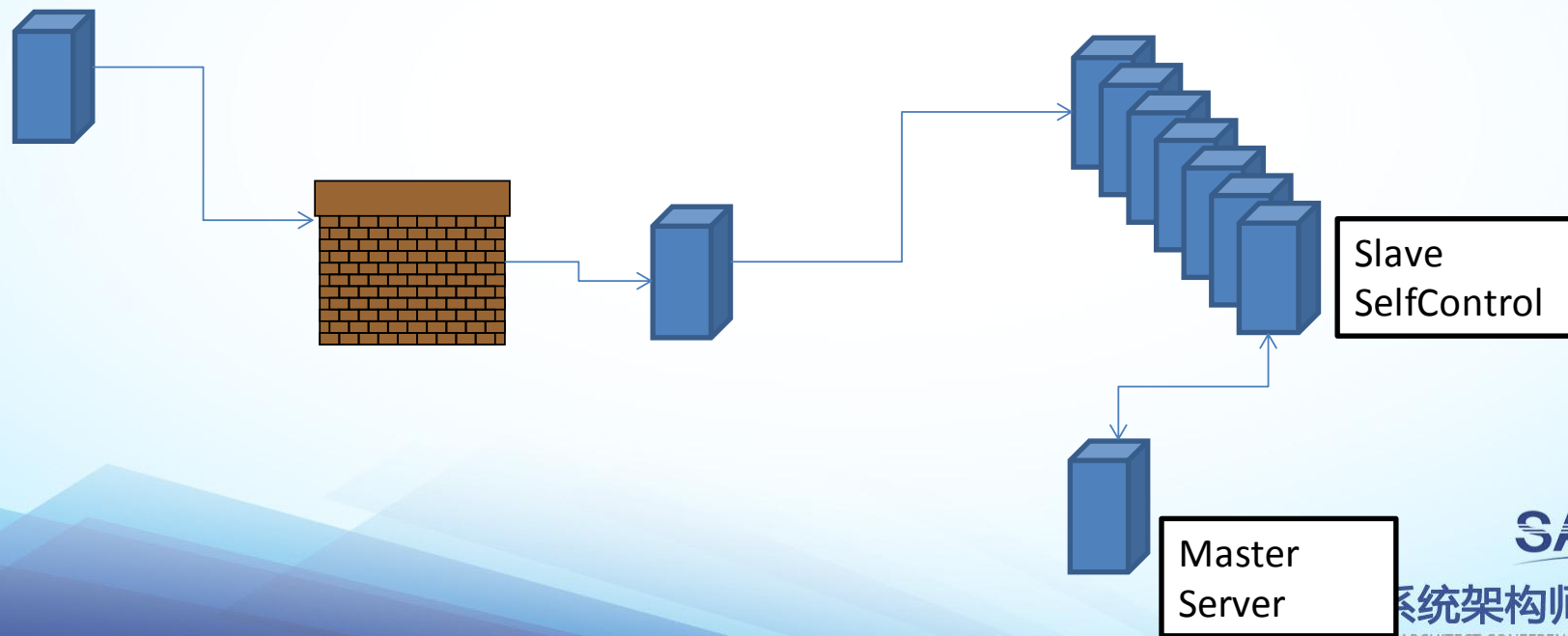
五彩石

基础数据收集

异常态决策

自动防御并报警

人工/自动升降级并解除



SACC

系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

系统架构M-S

■ Master:

- 从Slave收集状态数据
- 提供报警阈值，每天计算
- 提出报警，设置运行级别
- 邮件和短信通知

■ Slave :

- 定期发送状态数据给Master
- 从Master获取运行级别并设置
- 如Master无法响应，自行判断运行级别，进行邮件和短信通知

基础数据收集

- 网络连接数
 - netstat
- 网站PV
 - Nginx日志
- 网站UV
 - Nginx日志

基础数据收集

- check_ip.py 实时计算间隔时间内各IP访问次数及对应的级别，内容为：
 - 19/Apr/2012:21:31:0 P0 [('114.243.212.115', 144) ,('174.36.198.36', 1)]
- check_pv.py 实时计算间隔时间内PV及对应的级别，内容为：
 - 19/Apr/2012:21:41:1[0-4] P1 23
 - 19/Apr/2012:21:41:1[5-9] P0 81
- check_syn.py 实时计算间隔时间内SYN及对应的级别，内容为：
 - 19/Apr/2012:21:41:1[0-4] P1 10
 - 19/Apr/2012:21:41:1[5-9] P1 15

异常状态决策

级别	代号	数据特征
正常	正常	PV 每秒每台 < 100 SYN 每台 < 60 流量 < 100M
P2	正常	PV 每秒每台 10-200 SYN 每台 60-100
P1	橙色	PV 每秒每台 200-300 SYN 100-300
P0	红色	PV 每秒台 > 300 SYN > 300

自动防御并报警

- Master以Slave实时状态判定级别
- Slave结合自身的运行级别
- 按照最优先等级要求设置

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

自动防御并报警

■ Syn Flood

- 恶贯满盈：iptables，封禁，定期解锁

■ Nginx

- 嫌疑较大：limit_req，限制指定时间和每秒并发请求

■ 验证码

- 精准判断：PHP，达到当前级别为阈值，关小黑屋，需输入验证码解锁

■ 自动防御并报警

- stone_action.py

Stone项目中主要控制器，作用为升/降级和报警

All Defence – 全部加验证码
风险国家加验证码
红色级别限制访问
橙色级别限制访问
正常级别限制访问
IP白名单
手工加入白名单

自动防御并报警

Light **in** thebox.com



**We noticed you've been clicking on the same link a LOT
and our other pages are getting a little lonely!**

To get back on track, please click the input box and type the code you see in the image.

<input type="text"/>		<input type="submit" value="Submit"/>
----------------------	--	---------------------------------------

Copyright © 2006-2010 Light In The Box Ltd. All Rights Reserved.

SACC

勾师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

| 懒了

	root	• • Add IPs from block list to White List	07-23 03:02
	root	• • LITB_Web4 DDOS defense level is set to P2	07-21 16:43
	root	• • LITB_Web2 DDOS defense level is set to P2	07-21 16:43
	root	• • SYN Flood attack in FrontEnd_Master	07-21 16:39
	root	• • SYN Flood attack in FrontEnd_Slave	07-21 16:39
	root	• • LITB_Web4 DDOS defense level is set to P1	07-21 16:38
	root	• • LITB_Web2 DDOS defense level is set to P1	07-21 16:38
	root	• • Web2 Attack is coming in one second	07-21 16:38

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

事情还没有完

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

装在套子里的“人”

- 不是为了保守
- 而是为了保护

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

流量类攻击

- 带宽耗尽
- 硬抗

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

Cisco设别

- 功能有限
- 流量大也处理不过来
- 还是会堵死

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

TMS

- 机房可即时操作
- 流量大，丢包严重
- 重定向网址，影响正常访问

EthProxy

- 省钱：
 - 出现问题时操作
 - 滞后于攻击
- 花钱：
 - 持续接入
 - 不划算
- 流量清洗的问题：
 - 流量大，丢包多
 - 部分正常用户会误判

Global DNS

- 根据洲或者国家设定IP指向，反应滞后
- 越发达国家，攻击流量越大

最终选择

- Akamai Kona Site Defender
 - 只有HTTP和HTTPS通过
 - 震慑敌方
- 隐藏IP
 - 仅对Akamai Kona Site Defender暴露IP
 - 所有服务都在内网，VPN隔离保护
 - 多个机房备用
 - 非重点服务暴露在公网

Q&A

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算