

www.qconferences.com

www.qconbeijing.com



QCon北京2014大会 4月17—19日

伦敦 | 北京 | 东京 | 纽约 | 圣保罗 | 上海 | 旧金山

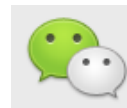
London · Beijing · Tokyo · New York · Sao Paulo · Shanghai · San Francisco

QCon全球软件开发大会

International Software Development Conference



@InfoQ



infoqchina

软件
正在改变世界!

特别感谢 QCon上海合作伙伴





弹性计算云安全

——现状、反思以及展望


阿里巴巴 魏兴国（云舒）

2013年10月




关于我

- ➡ 04年离校 国贸专业
- ➡ 05年绿盟 渗透测试
- ➡ 06年雅虎 IDC、Office安全
- ➡ 08年阿里
 - ➡ 2008 - 2010 集团系统、网络安全策略
 - ➡ 2010 - 现在 云计算安全



目录

- 弹性计算的新风险
 - 阿里的解决方案
 - 现状的反思
 - 未来云安全的展望
- 



弹性计算的新风险

- ➡ 传统安全域被打破
 - ➡ 不同用户混杂
 - ➡ 不同业务混杂
 - ➡ 来自内部的攻击



弹性计算的新风险

- ➡ 传统手段失效
 - ➡ ACL无法控制VM间的流量
 - ➡ 无法统一监控全网的攻击行为



弹性计算的新风险

- ➡ 大规模带来的问题
 - ➡ 交换机CAM表容量不足
 - ➡ ARP广播、NBNS广播风暴
 - ➡ 全局性的ARP欺骗、以太网端口欺骗攻击
 - ➡ 更频繁的外部攻击、入侵尝试



弹性计算的新风险

➡ 虚拟层穿透

- ➡ 入侵宿主机等同于入侵了传统的交换机
- ➡ 宿主机功能更复杂，更容易被入侵



厂商的解决方案

➡ 网络虚拟化标准

- ➡ 802.1 Qbg (VEB, VEPA, Multi-Channel)
- ➡ 802.1 Qbh/802.1BR (VN-Tag, VN-Link)



阿里的解决方案

- 为什么自己做？
 - 厂商方案本质是个网络模拟器
 - 定制化更灵活、高效、强大



阿里的解决方案

➡ 网络层架构

➡ 基于业务的分布式虚拟交换机

➡ 基于用户ID来分组虚拟机

➡ 控制策略下发到宿主机，随VM迁移而迁移

➡ 完备的安全功能



阿里的解决方案

➤ 访问控制策略

➤ 固化不可修改的全局策略

- 不同组默认隔离

- 动态绑定过滤IP、ARP、Ethernet头部欺骗

- 带宽控制、广播风暴抑制

➤ 用户通过WEB API自定义策略

- 远程控制端口访问源列表

- 其它自定义策略



阿里的解决方案

- 云盾—服务器安全
 - DDoS防御系统
 - 主机入侵防御系统
 - 网站安全防御系统
 - 服务器健康扫描系统
 - WEB应用
 - 网页挂马
 - 端口与服务



阿里的解决方案

➡ 云盾的效果

- ➡ 每天100起DDoS攻击，最大流量80Gbps，10%的攻击超过5Gbps，99.99%自动处理
- ➡ 每天200亿次密码猜解，99.99%防御成功
- ➡ 每天1000万次WEB攻击，100%防御
- ➡ 平均每周捕获一个0Day（未公开漏洞）！



阿里的解决方案

➡ 业务安全

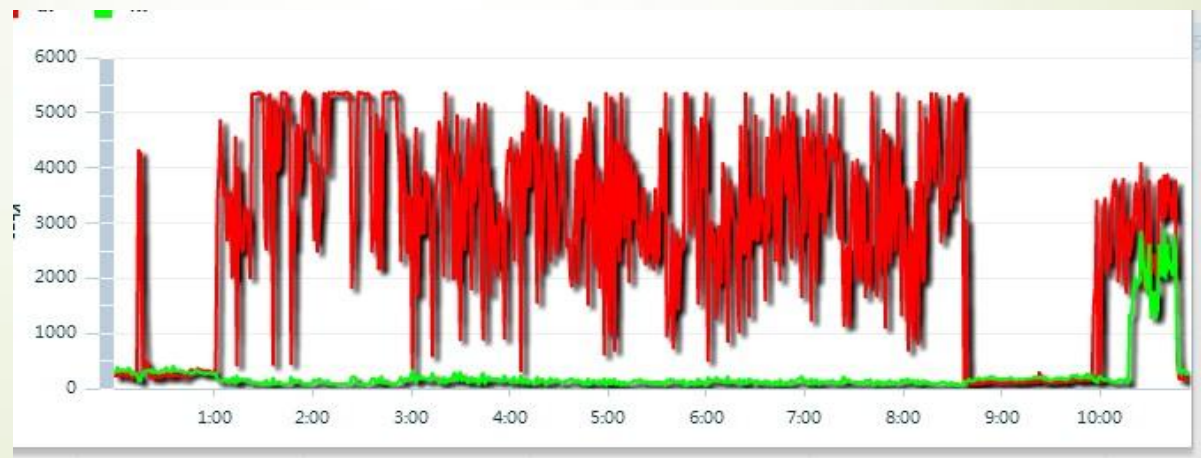
- ➡ 云服务器对外攻击检测
 - ➡ 过滤伪造报文
 - ➡ BPS、PPS、QPS、Connection检测
- ➡ 恶意行为检测
 - ➡ 对外扫描WEB漏洞
 - ➡ 密码破解
 - ➡ 垃圾邮件发送
- ➡ 黄赌毒应用的检查

阿里的解决方案

➡ 用户隐私问题

➡ 没有云服务器系统权限

➡ 不分析应用数据，只做宏观的统计测量





云安全现状的反思

■ 关于用户区域划分

- 三层隔离是最好的选择么？
- 多条防欺骗策略是否有损性能？




云安全现状的反思

- 关于分布式虚拟交换机
 - 能够支撑多少条自定义策略？
 - 宿主机规模达到10万的时候是否还可维护？



云安全现状的反思


- ➡ 用户群体继续扩大
 - ➡ 我们是否可以满足多样化的安全需求？
 - ➡ 能否方便的接入第三方安全提供商？



云安全的未来设想



➤ VPC虚拟专用云

- 不同用户网络在二层隔离
- 广播包在小范围内终结
- 无需大量防欺骗策略




云安全的未来设想

- ➡ VPC虚拟专用云
 - ➡ 基于image的自定义VM网关
 - ➡ IPS ? FW ? WAF ? UTM ?




再进一步？



云安全的未来设想

- 安全产品虚拟化、资源化
 - 将不同硬件抽象成统一的容器，安全功能剥离出来，开放接口给第三方安全厂商
 - 非模拟器的方式来集中部署控制策略
 - 所有安全产品服务都透明接入、透明变更



云安全的未来设想

➡ 两个条件

- ➡ 按需可得计算资源
- ➡ 按需变更的网络结构

云安全的未来设想

安全软件

硬件盒子




弹性VM

物理布线



SDN网络



云安全的未来设想

■ 云安全市场

- 用户绘制包含安全产品的网络拓扑图
- 用户选择各安全产品的提供商
- 云计算控制系统加载对应Image，基于SDN生成网络

云安全的未来设想

业务VM

业务VM

业务VM

云用户

Firewall
Image


IPS
Image

WAF
Image

众多安
全厂商

IAAS (基础架构即服务)

云提
供商



云安全的未来设想

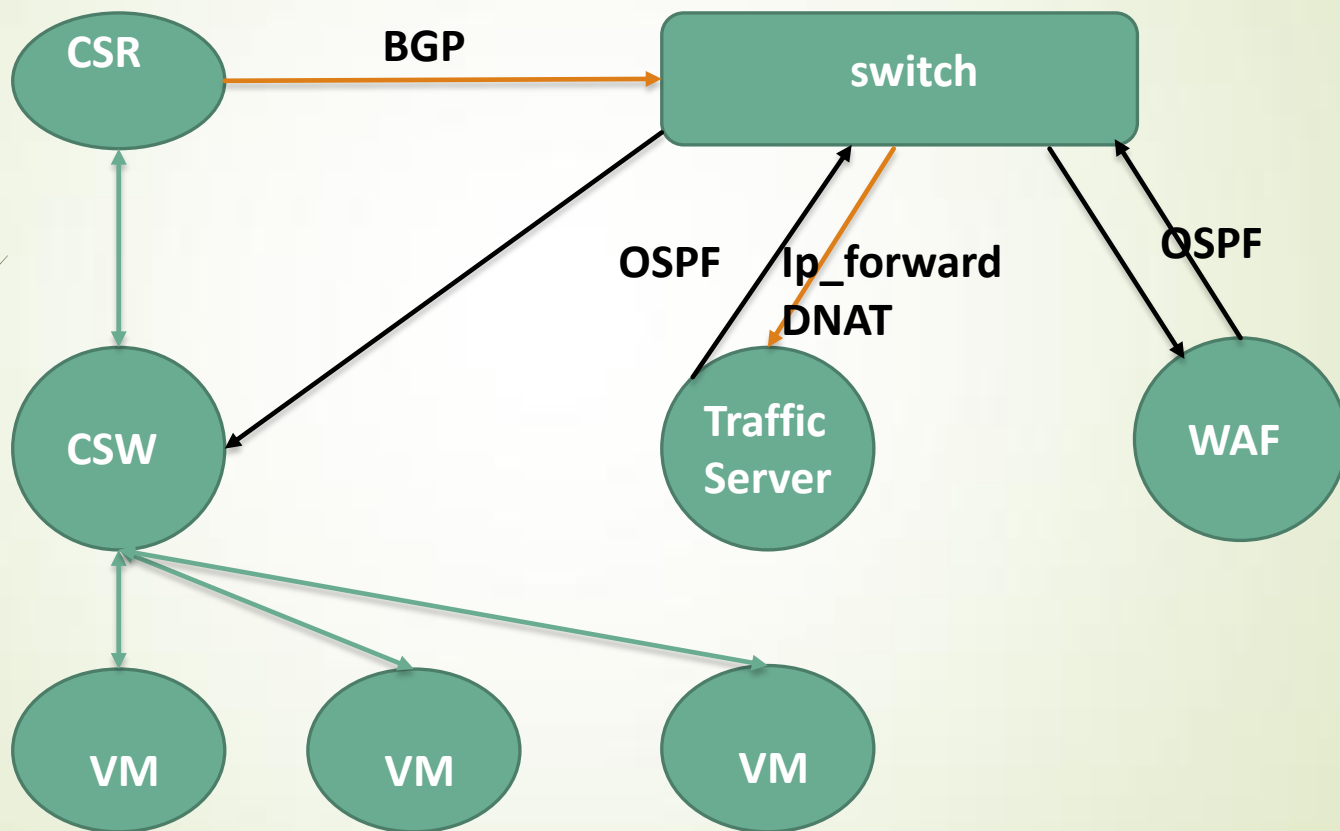
➡ 困难


- ➡ SDN迟迟不能得到应用
- ➡ 厂商对image中的代码、策略安全性存疑
- ➡ 这种模式是否可以发展起来？

云安全的未来设想

- 从透明接入WAF开始探索
 - 集中部署WAF，宿主机上DNAT
 - 宿主机上分布部署WAF，宿主机上DNAT
 - BGP引流OSPF回注，WAF上DNAT和路由转发
 - VM网关，自己掌控软路由
 - 更多其它方案.....

云安全未来的设想





总结

- ➡ 我们做的不仅仅是这些，欢迎加入
- ➡ 有问题请联系我
 - ➡ yunshu@outlook.com
 - ➡ <http://weibo.com/pstyunshu>