青云在数据与网络安全中的实践

王 煜 / William

Software Engineer

william@yunify.com

China Internet Security Conference 2014

2014中国互联网安全大会

青云在做什么

- 提供公有云服务
- IaaS 基础设施即服务
- 云端的计算、网络、存储和安全
- 交付稳定可靠的 IT 资源

云计算中的安全课题

ISC 2014

- 当我们谈论安全时我们在谈论什么？ Security & Safety
- 如何利用 SDN 技术构建安全的网络环境
- 在海量数据存储服务中，如何保证用户数据的安全可靠
- 如何利用自动化运维，保证系统从失败中快速恢复
- 用户在云计算环境中会遇到哪些安全问题
- 用户如何在云计算环境下构建高可用的服务架构
- 经验与哲学

QINGCLOUD青云

软件定义网络

- 用户层面与物理层面

  用户层，实现传统 IT 网络环境中的组网功能

  物理层，将控制和转发进行分离，将控制部分提炼到软件中实现，硬件路由设备退化为二层连通设备

- 基础网络 / 私有网络

  基础网络是用户加入的公共网络，二层连通，内网 IP 可发生变化

  私有网络与其它租户完全二层隔离，足够安全，且符合传统 IT 网络构建习惯

- 二层设备 – 交换机

  100% 二层隔离，更高的安全性

- 三层设备 – 路由器

  连接二层设备，端口转发，过滤控制，VPN，GRE 隧道

为什么构建私有网络

ISC 2014

- 用户需要 100% 二层隔离的网络环境

  常见的云计算提供商只提供公共的基础网络

  多租户的不同主机之间需要确保隔离

  大部分的攻击发生于网络内部多租户之间

- 自由组网，和传统物理世界拥有同样的网络拓扑

  将传统网络中的功能完整搬到云计算环境下，原来的实践经验依然适用

  用户可以通过控制台或者 API，随时修改网络配置，几秒钟生效

- 构建混合云，和已经部署的物理网络相互连通

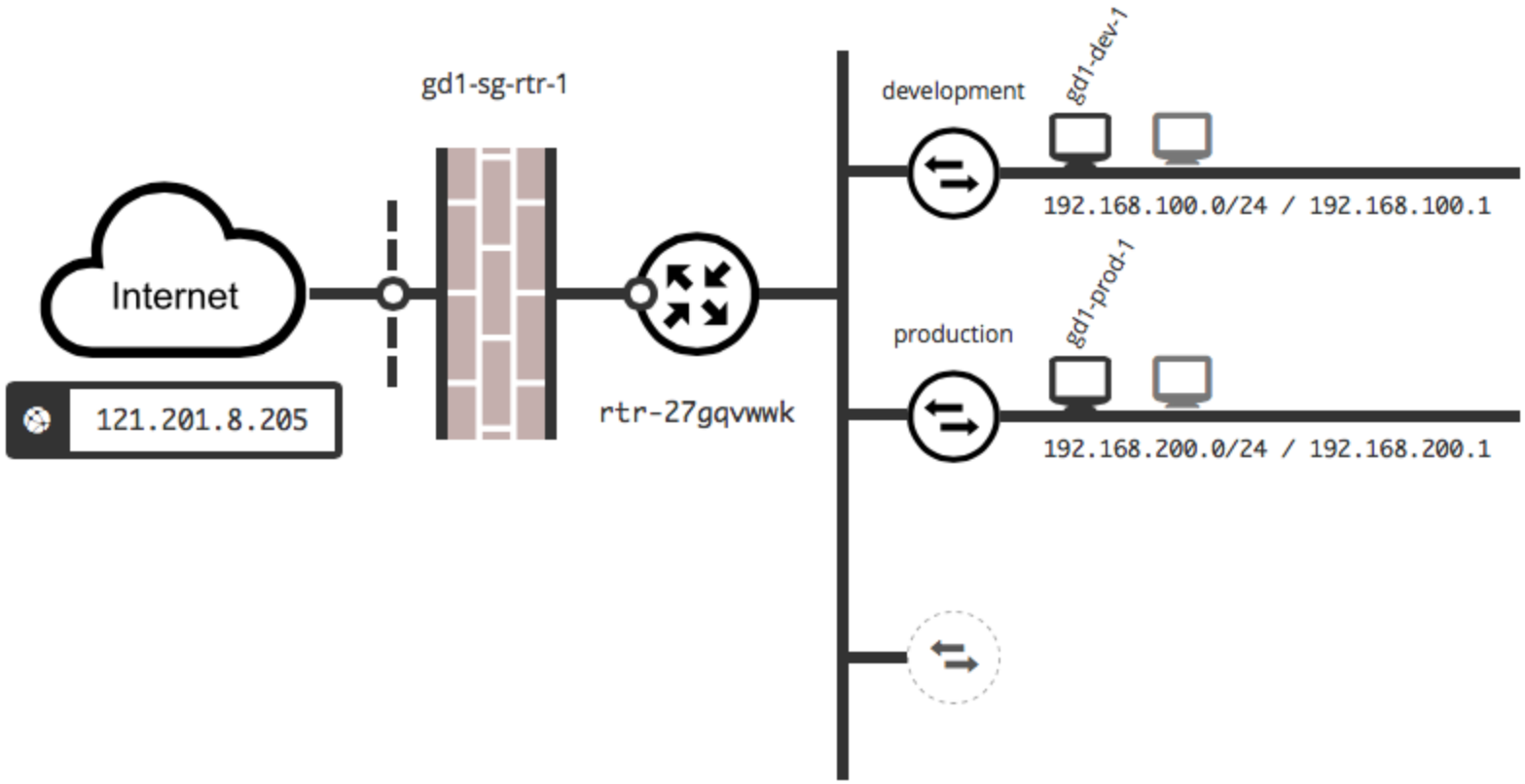
  用户将系统完全迁移到云端需要过程，这个过程中业务要一直提供正常服务

  通过青云路由器提供的功能，让云计算环境和传统网络环境完全相融

QINGCLOUD青云

典型的网络拓扑

完整的网络环境包含：防火墙、路由器、交换机、主机、公网 IP



数据存储与安全

- 评价存储方案好坏的唯一标准，是否能满足用户的需求

  数据必须是可靠的，绝对不能丢

  对于频繁读写的在线系统数据，提供足够好的读写性能

  对于离线或备份数据，提供足够大的空间和低廉的价格

- 青云的分布式存储

  性能性硬盘，85000 IOPS，128 MB/s 足够快的速度

  容量性硬盘，0 - 5T，足够大的存储空间和低廉的价格

- 实时副本与灾难恢复

  数据的写入只有在多个副本上都完成后才成功返回

  至少有一份不在同一个物理磁盘上

数据备份与恢复

- 数据备份

  块设备级别的备份与恢复

  捕捉硬盘在某一个时刻的状态，未来可以随时恢复到这个状态

  可以同时对多张硬盘做备份，也可以对正在运行的主机做在线备份

- 备份链

  每条备份链包括一个全量备份点以及多个增量备份点

  每次做全量备份都会产生一个新的备份链

- Snapshot 与快照

  快照只是在原有数据上打标签，这会破坏原有结构

  青云将每次变化的数据取出来，离线存放，不影响原有数据，这样做更安全

自动化运维与机器人社区

- 自动化运维

  云计算真正考验运维能力

  人是最昂贵也是容易犯错的，所以要自动化一切，零运维

- 资源的安置策略

  机器人 bot 是系统中的 controller，负责调度和安置资源

  均匀化法则，根据当前的 workload 运行状态，哪台机器比较空闲就放在哪

  历史状态 和 Device Credit

  对设备运行状况的预测

- 故障恢复

  出错、损坏、故障是常态，对所有的错误都有应对的策略，设定 trigger

  快速将数据迁移到其它机器，SDN 发挥作用将流量牵引到新地址

云计算中的账号安全

- SSH 登录破解

  常见于开启了允许密码登录的情况

  禁用密码登录，改成使用密钥登录，并定期更换新密钥

  使用青云路由器构建私有网络，并开启 VPN 服务，将主机置于私有网络内

- 常用软件账号破解

  软件通常配置了默认账号和密码，用户忘记修改

  修改默认账号和密码，并且只监听特定的 IP 地址

  使用青云防火墙，应用到主机、路由器、负载均衡器等设备，只开启必要的访问端口

- 管理员账号

  青云控制台的主账号与子账号

  账号锁定功能，及 API 签名

云计算中的应用安全

- XSS 跨站脚本攻击
- SQL 注入攻击
- CSRF 跨站请求伪造
- 恶意爬虫
- 文件上传漏洞

传统 IT 环境下的安全问题依然存在！

云计算中的拒绝服务攻击

- Challenge Collapsar 攻击

  CC 攻击是最常见的拒绝服务攻击形式，攻击者模拟用户的请求行为，不容易分辨

  通常从两方面入手，一是识别攻击特征，屏蔽请求，二是提高服务响应速度

- SYN Flood

  开启 syn cookies，net.ipv4.tcp_syncookies = 1

  增大 syn backlog，net.ipv4.tcp_max_syn_backlog = 8192

  减少 syn ack 重试次数，net.ipv4.tcp_synack_retries = 2

- 慢速攻击

  可以将青云负载均衡器置于最前面接收客户端请求，并将 HTTP Timeout 设置为一个较短时间

云计算中的流量攻击

- 攻击者向某一 IP 发送大规模的数据包流量
- 目的是占满被攻击者的总入口带宽，使正常流量无法进出
- 通常由上层网络提供者发现和处理，云计算的终端用户无法直接干预
- 青云与数据中心合作应对大规模流量攻击

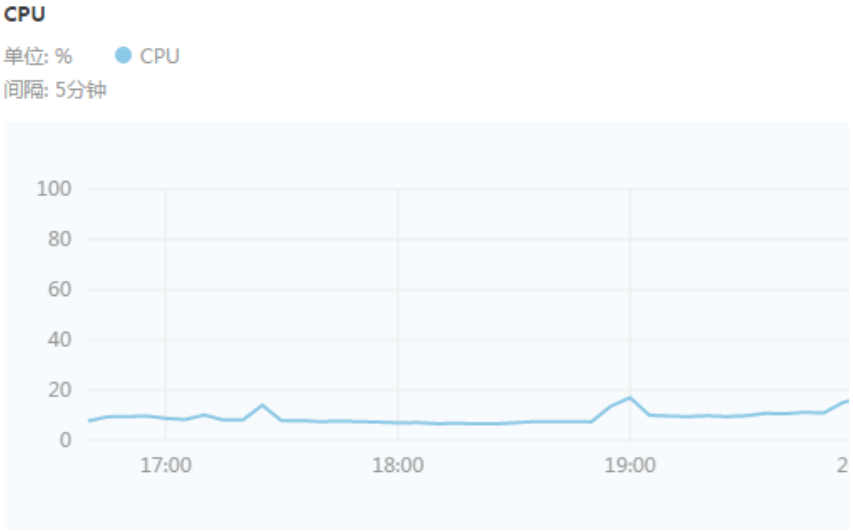
  动态修改被攻击对象的链路到隔离链路，避免影响全局

  广播 IP 路由到上联机房交换机，将流量牵引到黑洞清洗设备

构建高可用的服务架构 I

- 监控告警服务

CPU 利用率 / 内存利用率 / 磁盘使用量 / 网络流量



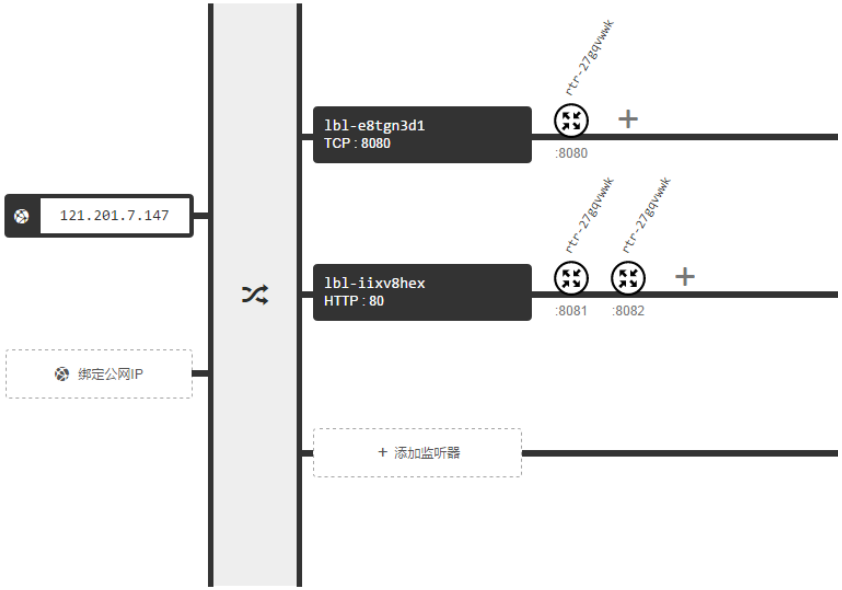
构建高可用的服务架构 II

- 负载均衡器

  完整的功能，七层负载 HTTP / TCP，后端状态检查

  负载方式，轮询 / 最少连接

  转发策略，域名 / URL



构建高可用的服务架构 III

- 防火墙

  青云为每个用户提供了一个缺省防火墙，用户也可以自己更多的防火墙

  防火墙可以应用于主机、路由器、负载均衡器等后端资源

- 完全开放的 API 接口

  对于资源的操作全部开放 API 接口

  青云的控制台 console 就构建在 API 接口之上

  完善的 API 文档，和 SDK 工具

  编写系统脚本，自动化运维

  例如，流量高峰和低峰，通过 API 增减资源

经验与哲学

- 推出的每一项功能都必须是出众的，和别人做的一样就没有任何机会
- 人是最容易出错的，所有能够被自动化的事情，都需要被自动化
- 对代码质量的极致追求，不断地 Refactoring
- 一切出错都应该控制在局部范围内，避免影响全局
- 系统的任何部分都应该是可水平扩展的
- 逻辑可以是复杂的，架构一定是简洁的

加入我们

如果你具备以下一个或多个技能，欢迎加入我们：

Linux / Python / C

Web / JavaScript / HTML5

计算机网络 / 虚拟化技术 / 分布式系统 / 数据库技术

我的邮箱：william@yunify.com

QingCloud-IaaS

青云QingCloud

www.qingcloud.com

QINGCLOUD青云

Thanks!