360

www.360.cn

云时代的ddos

胡振勇 huzhenyong@360.cn

2014年4月

- DDOS攻击的发展形势
  - PC肉鸡发起的攻击变少
  - 服务器肉鸡发起的攻击变多
  - 未来可能出现发自手机的ddos攻击

- 反射攻击
  - NTP攻击
  - DNS攻击
  - SYN FLOOD攻击

几种ddos攻击方式和防护手段

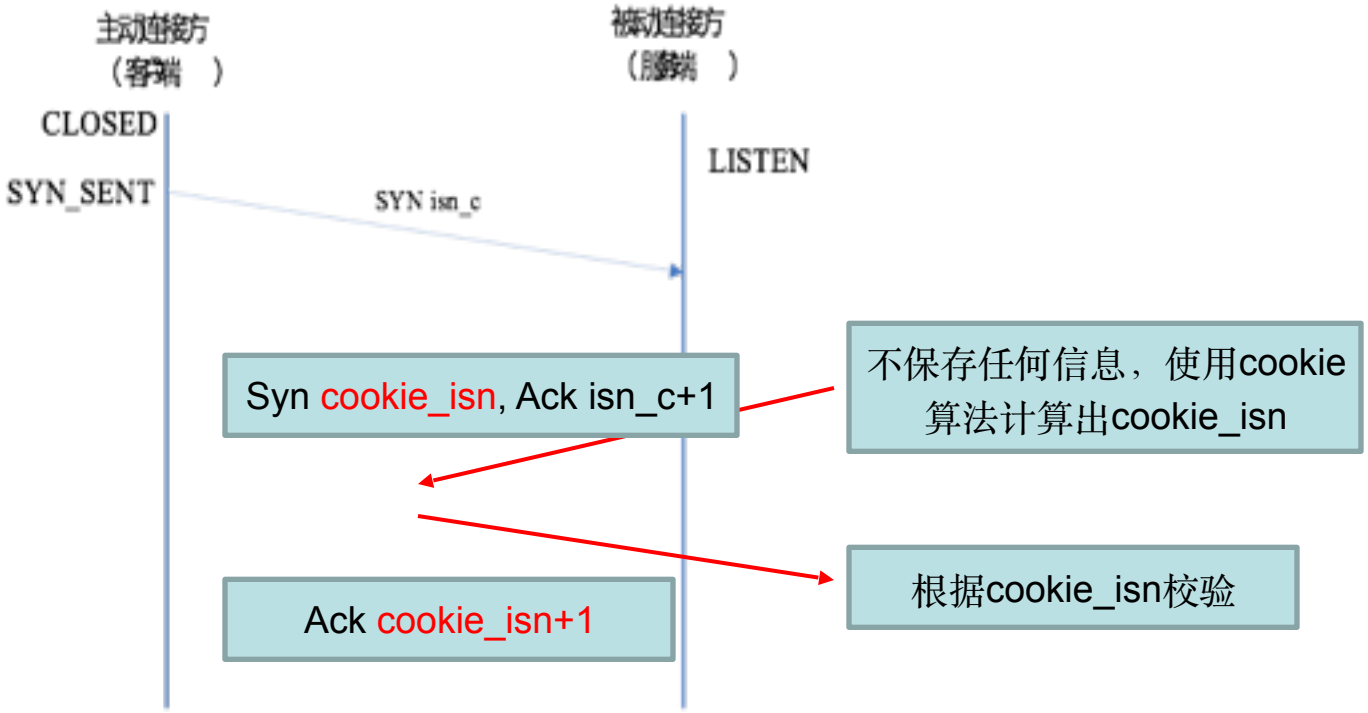
DNS 攻击

- 现状
  - 攻击带宽峰值超过100Gbps
  - 攻击目标私服为主
  - 大部分攻击为泛解析攻击

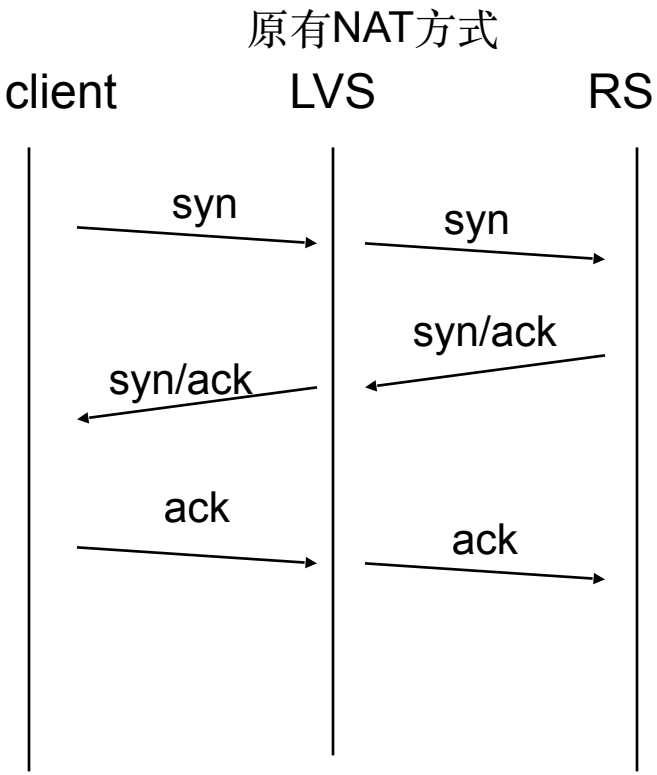
- 解决办法:
  - 单域名查询限速
  - 强制缓存
  - 递归DNS加白
  - 极端情况非白即黑

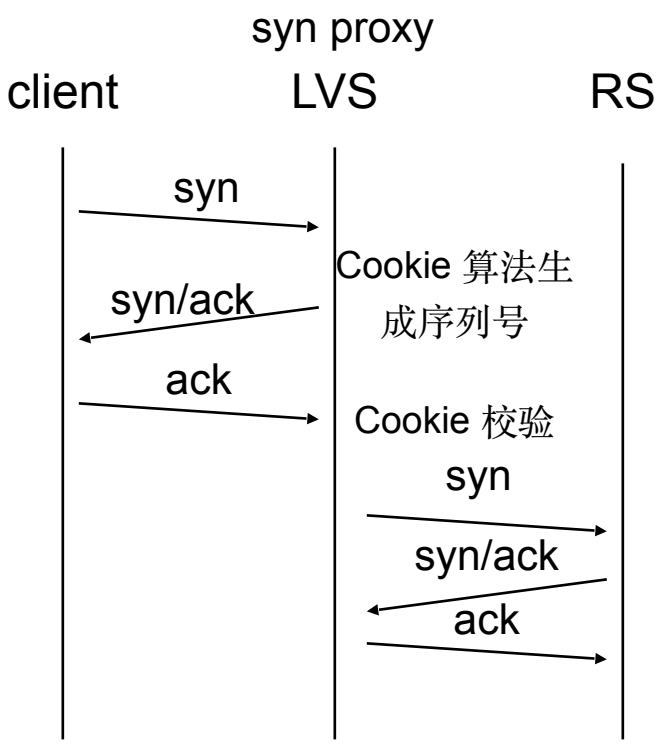
SYN Flood攻击

SYN Cookie

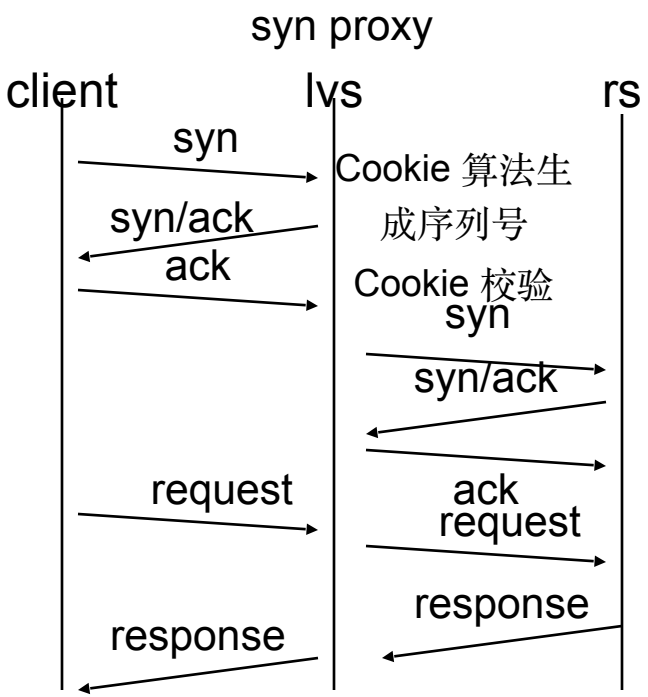

主动连接方
（客户端）
被动连接方
（服务端）
CLOSED
SYN_SENT
SYN isn_c
LISTEN
Syn cookie_isn, Ack isn_c+1
不保存任何信息，使用cookie算法计算出cookie_isn
Ack cookie_isn+1
根据cookie_isn校验

LVS防御SYN Flood攻击





syn proxy只是修改了三次握手的过程，后续的数据包过程完全没有变化，不会缓存数据



- 目前主流的服务器:
  - E5-2630 CPU*2
  - 64G RAM
  - Intel万兆网卡
- >9Mpps
- >4Gbps

- 问题

  和VIP同网段的client访问不通VIP

  原因：

  同网段机器之间通信需要知道对方的MAC，而VIP的MAC Client是学不到的

- 解决办法

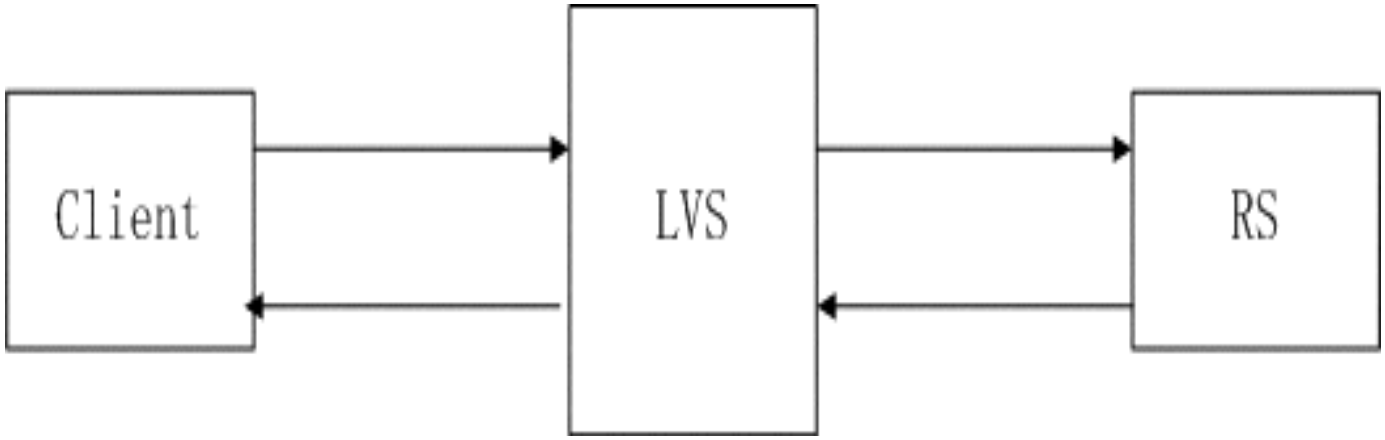
  运维规范避免:

  - VIP使用独立的网段
  - 设置特殊路由

问题：

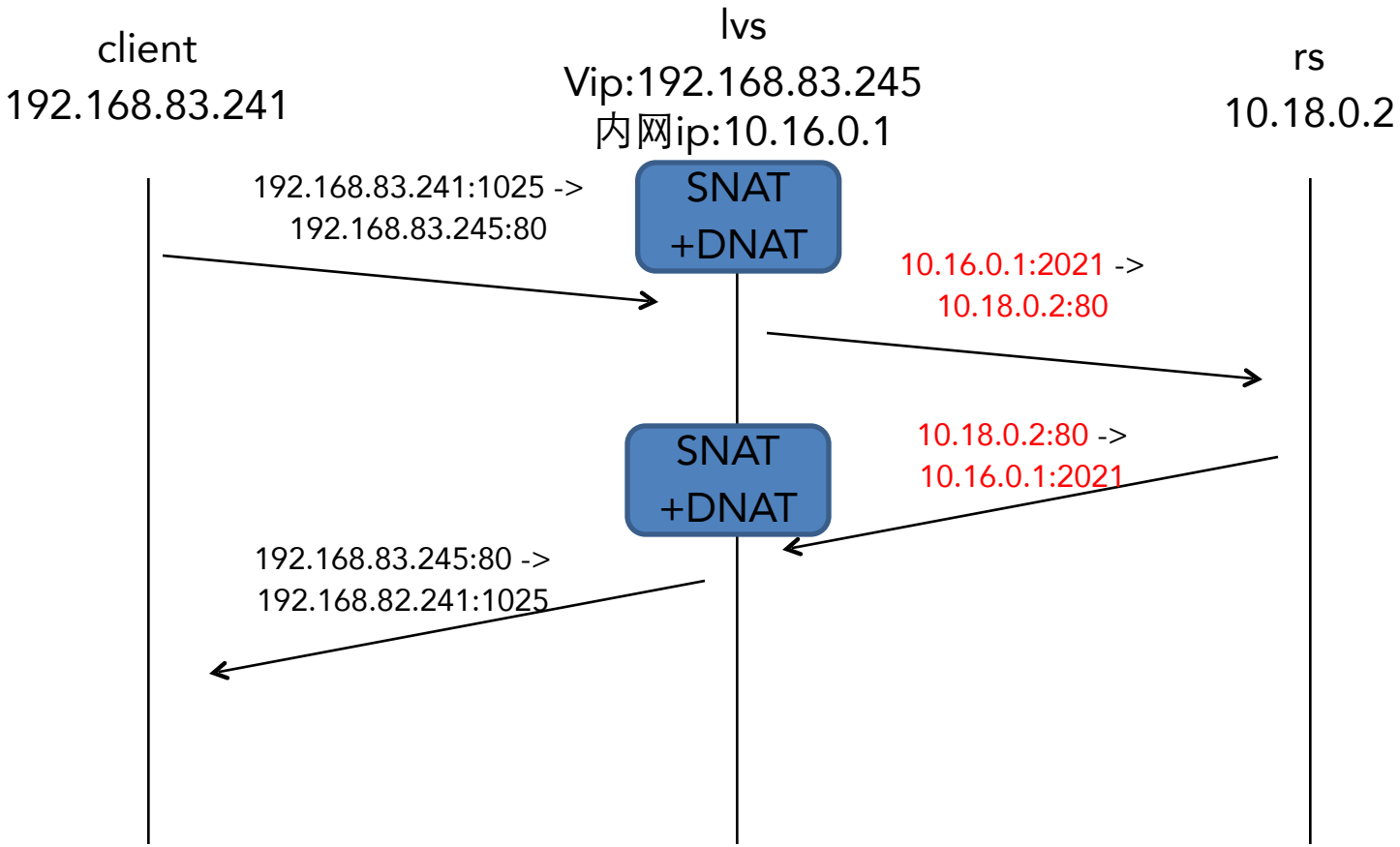
LVS与RS只能位于同一网段的问题

- NAT模式

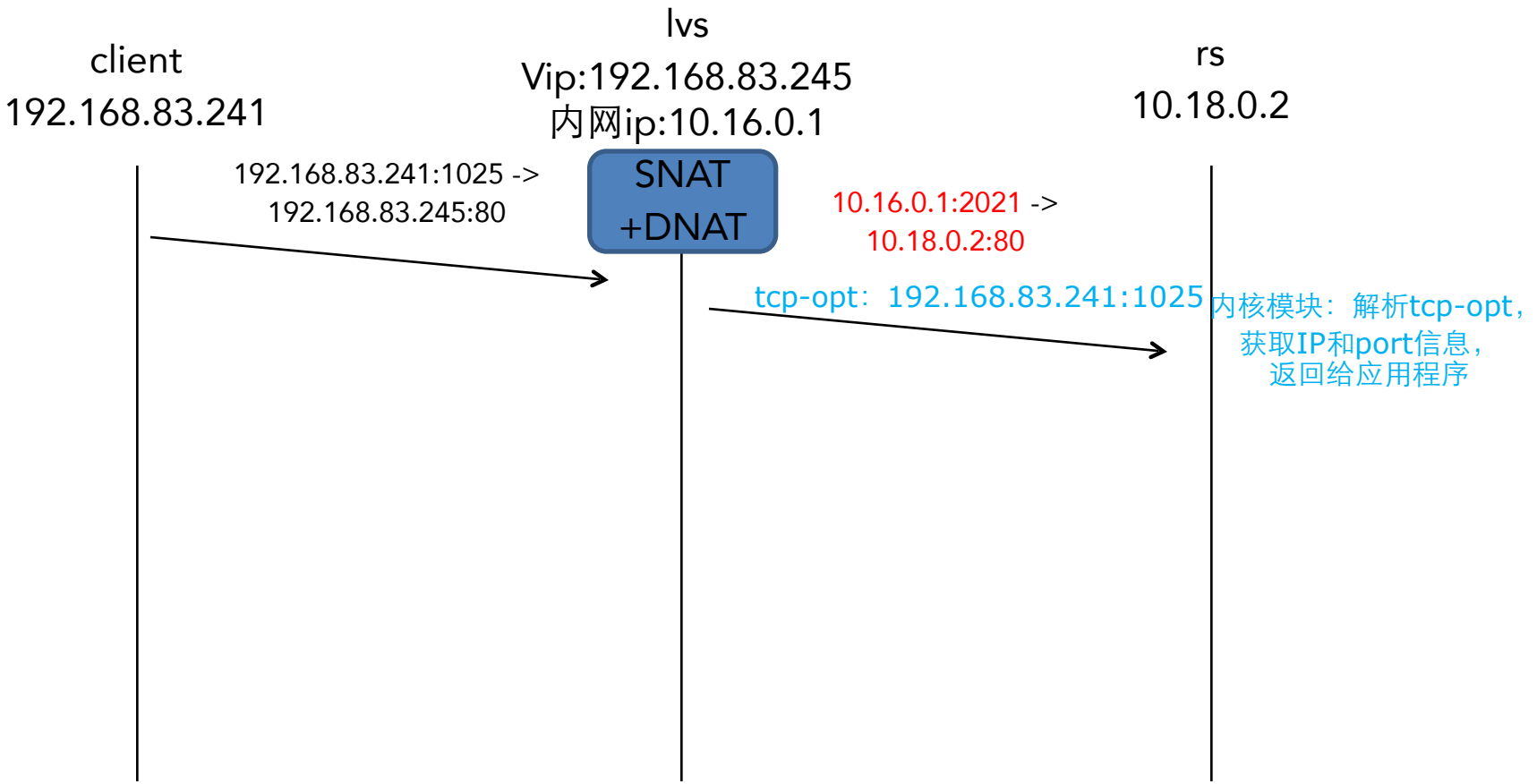


跨网段引入的问题：

- RS上的应用看不到client的ip

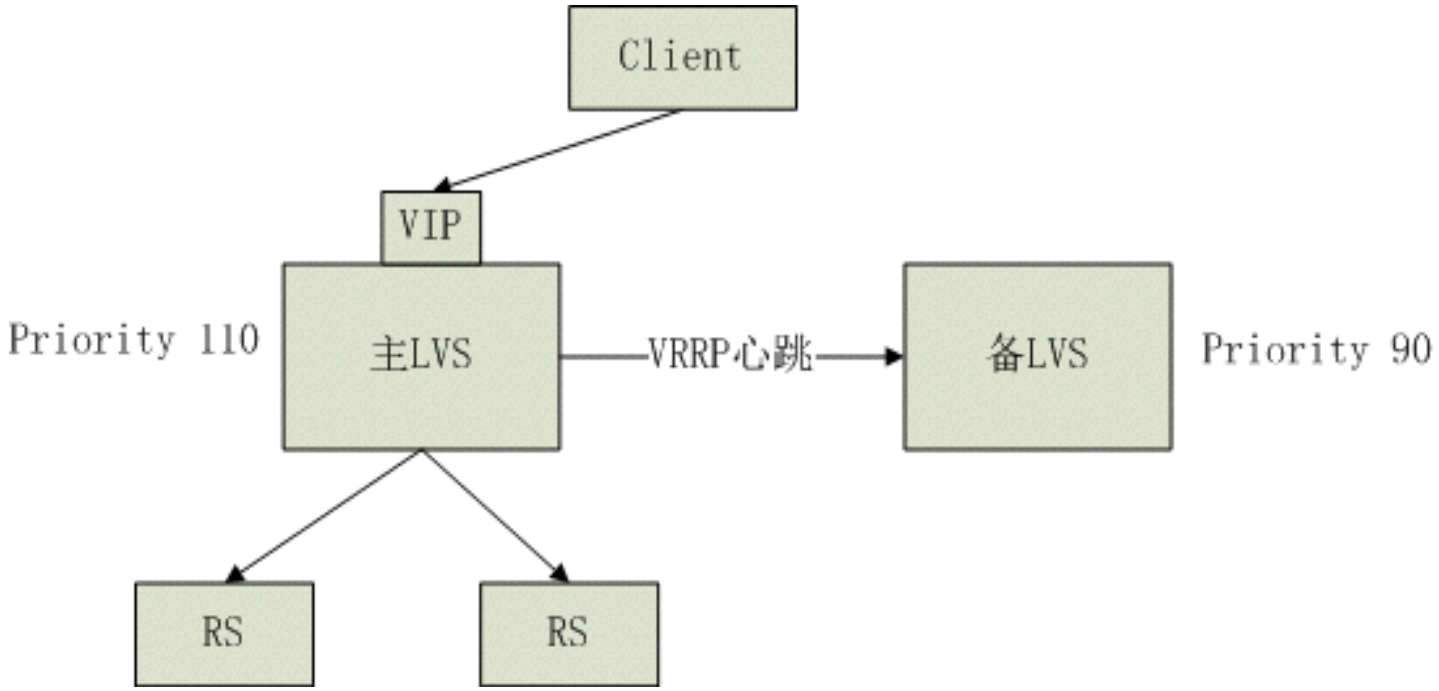


- 获取client ip的解决办法

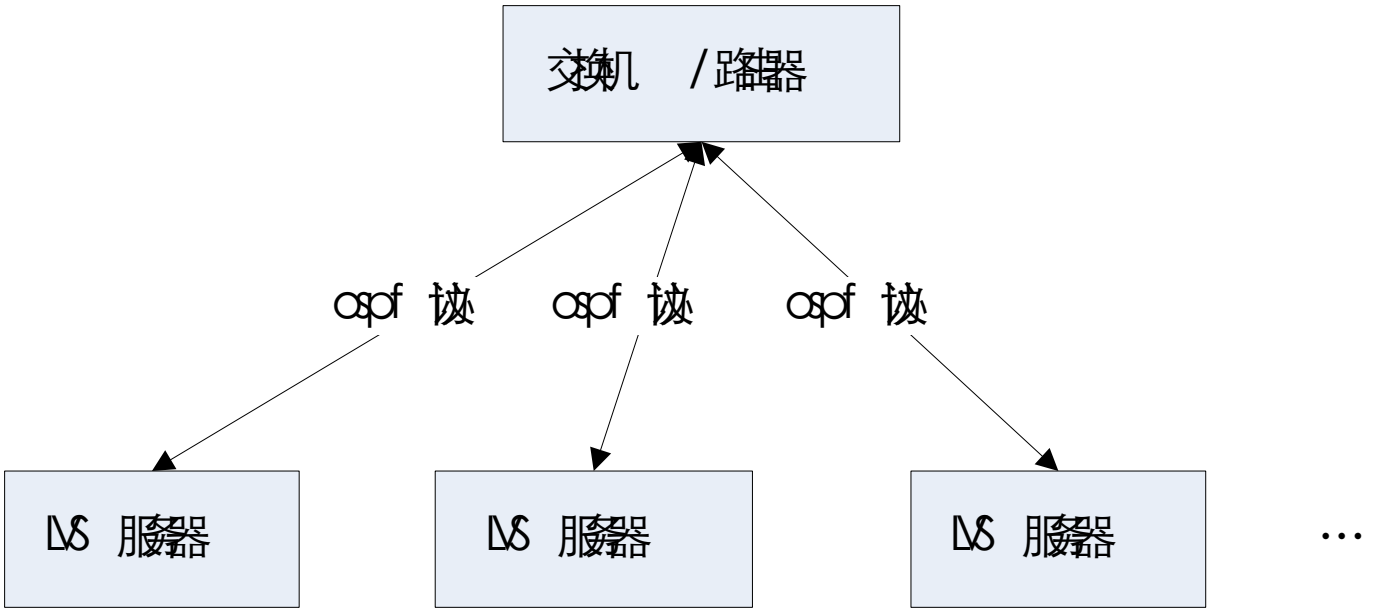


- 横向扩展的困境

  一个VIP只能在一台LVS上



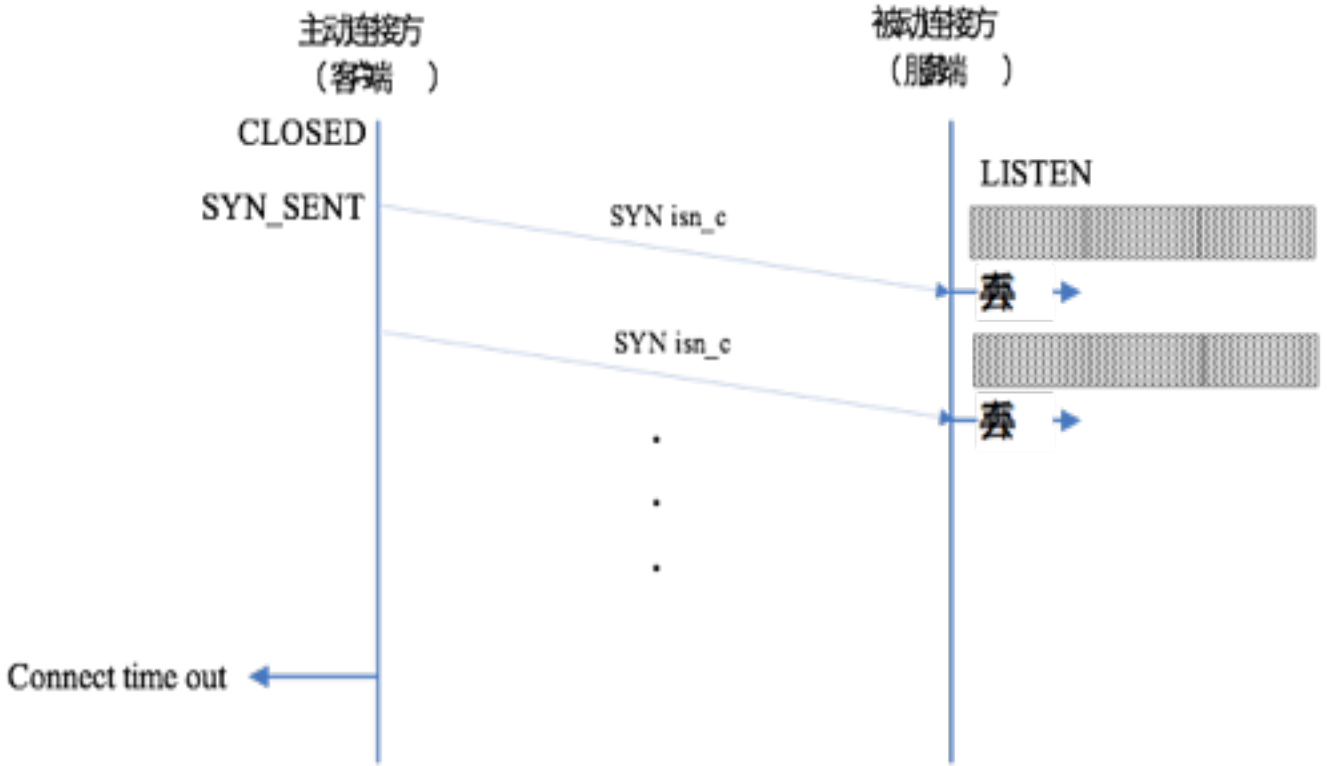
- LVS集群



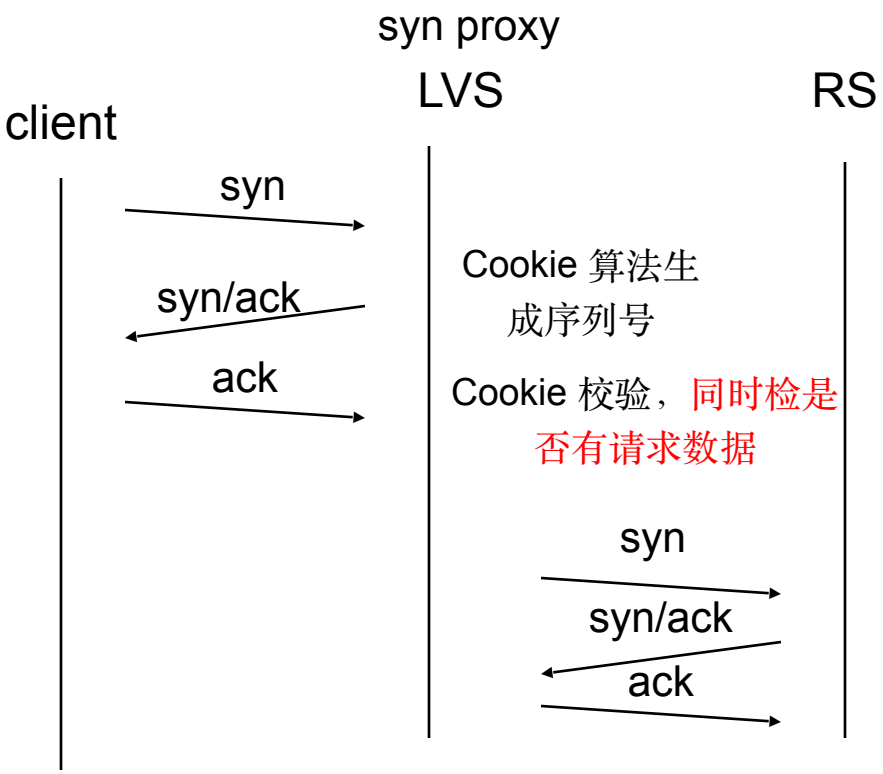
慢连接攻击

慢连接攻击

- 攻击者建立连接后，延时发送请求
- 服务程序接收到连接后，等待接收请求，导致连接累积，最后不能Accept新连接



防御慢连接攻击


syn proxy
LVS
client
RS
syn
syn/ack
ack
Cookie 算法生
成序列号
Cookie 校验，同时检是
否有请求数据
syn
syn/ack
ack

攻击方式的演进

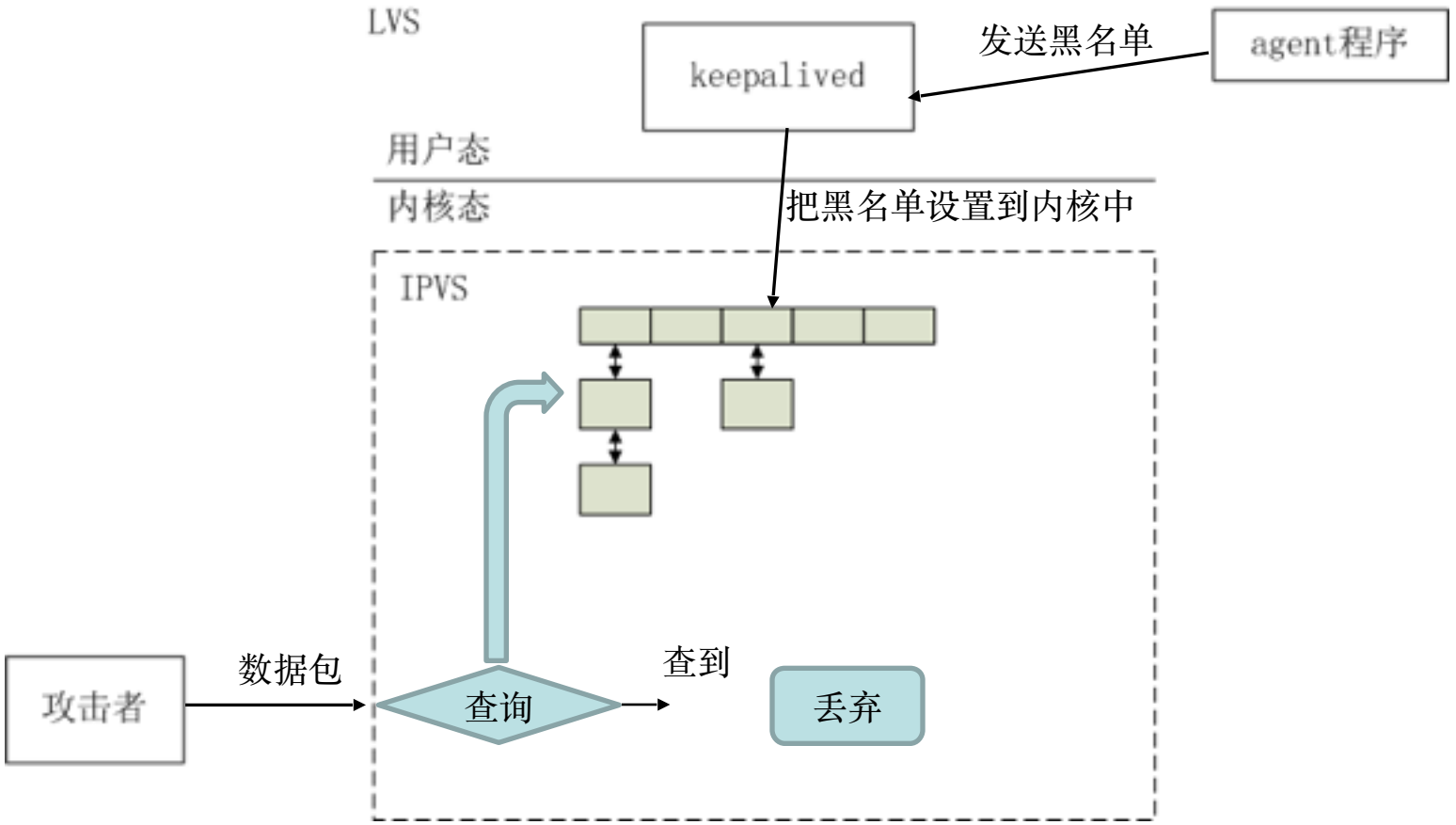
- 攻击者建立连接后，每xx秒（小于http服务器的ReadTimeOut）发送一个字节的请求
- HTTP服务器的默认TIMEOUT设置是60s
- 但是没有人会有耐心等待一个60s才能打开的页面

- 缩小HTTP超时时间
- 配合临时封IP的机制

分布式连接攻击

防御分布式连接攻击

把攻击者IP保存在黑名单hash表
用户数据包到达后，查询是否在黑名单中，在就丢弃



分布式攻击客户端的识别

- Cookie验证
  - 通过客户端IP地址、时间等因子计算Cookie

对ddos脚本类的攻击有效

- 运行JavaScript进行测试
  - 进行较复杂的数学计算
  - 判断浏览器插件属性

对隐形浏览器或者内嵌页面有效

分布式攻击客户端的识别

- 访问行为分析
  - 短时间内访问同一个URL多次
  - 除了某个URL，不访问其他资源（如图片、css等）

对内置型、广告联盟的攻击有效

- 图片验证码
  - 要求访问者输入图片验证码
  - 不定期的更换验证码图片

用户体验较差，但是效果也最直接，不得已而为之

攻击方式的演进

- 多种防护方式的代价不一样
- 需要多种方式的结合

- 攻击客户端使用webkit完美模拟浏览器

防护平台的建设经验

- 防护能力要足够强
  - 多节点部署，分散攻击力
  - 单个节点的带宽储备充足
  - 单机的处理能力提高
  - 和运营商网络联动

- 防护方式要灵活
  - 方便进行调整
- 模块化的设计，灵活组合
- 不同用户/域名之间的配置独立
- 软件的灰度升级
  - 支持小范围的软件升级，可以在指定范围进行测试，即使有bug，范围可控

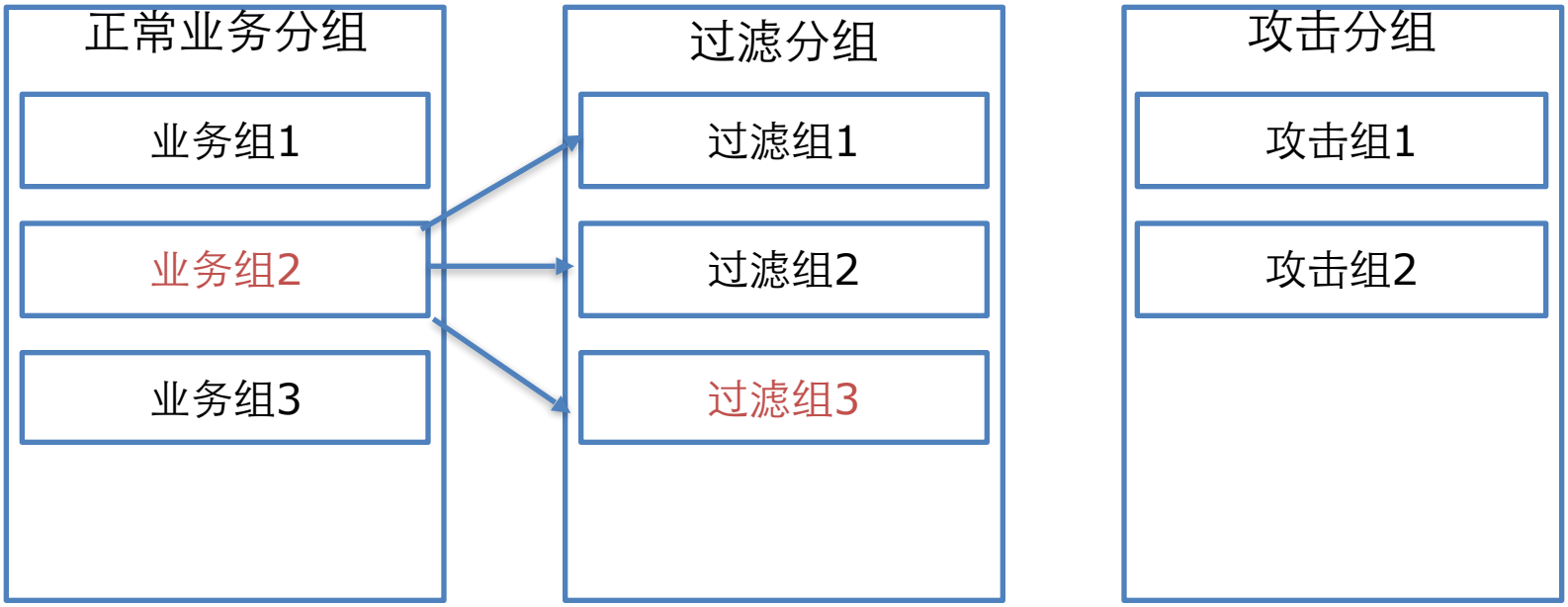
- 具备故障隔离的能力
  - 多点部署，单个节点故障不影响业务
  - 快速识别攻击目标，避免其他用户受影响

- 问题:

如何快速发现SYN Flood的攻击目标?

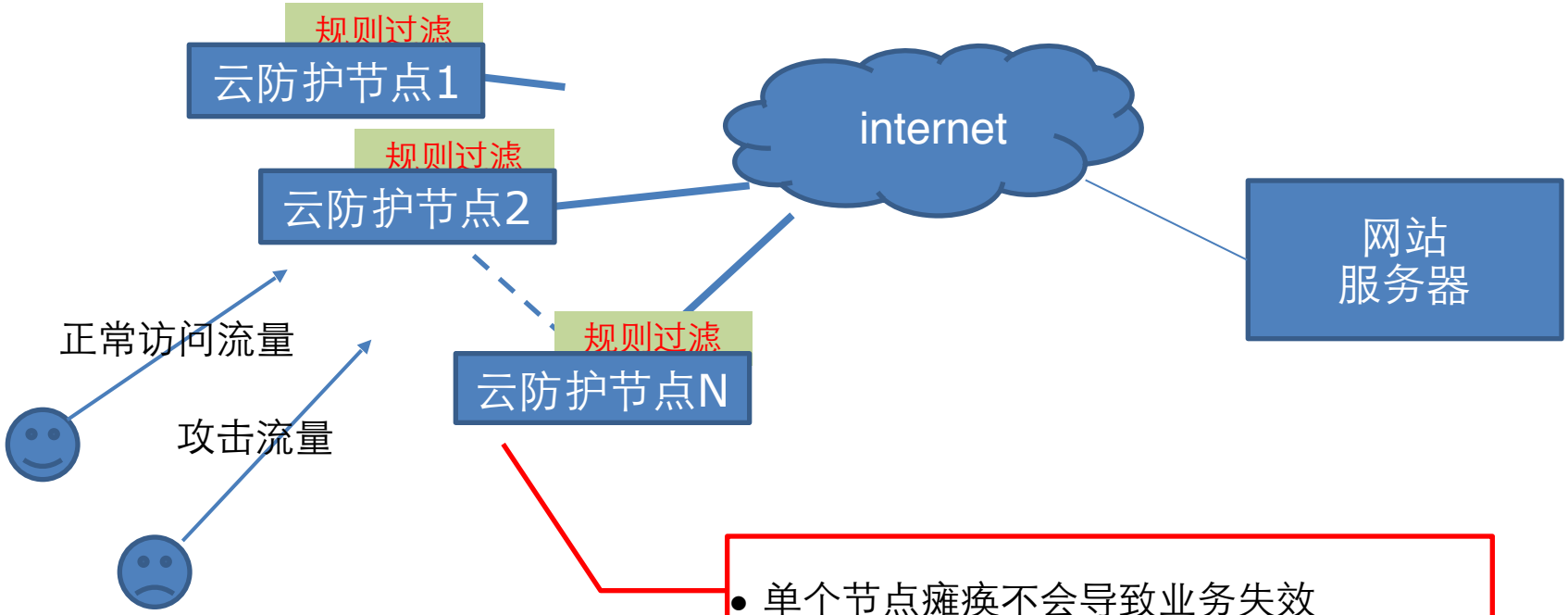
解决办法：

- 分组过滤



- 问题:

如果攻击流量太大怎么办（超过一个机房的总出口带宽）？



- 单个节点瘫痪不会导致业务失效
- 当一个节点攻击流量超过防护能力后，通过DNS将攻击流量引导到带宽储备高的节点

Q&A

革命尚未成功，同志仍需努力!

Thank You!
谢谢！