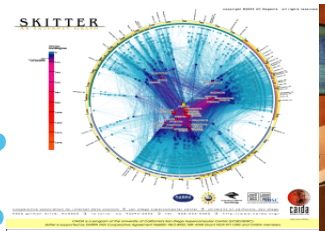
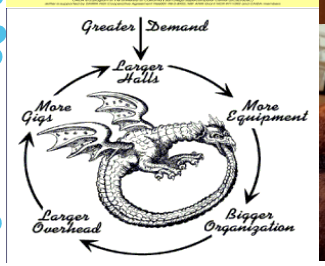
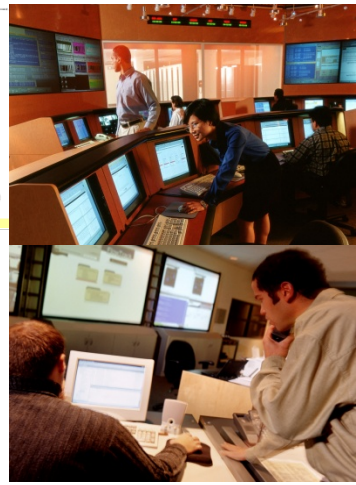
如何响应DDOS攻击（服务提供商版）







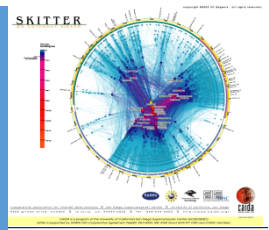
大纲

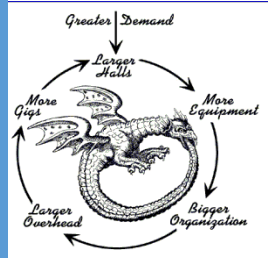
- 抵御拒绝服务攻击的背景原理
- 工具投入使用-DDOS攻击

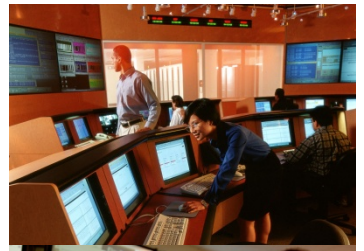
悠久的历史–在线培训

- NANOG 23 – ISP安全–现实世界技术II – by Barry Raveendran Greene, Cisco Systems; Chris Morrow, UUNET/Verizon; Brian W. Gemberling, UUNET
- NANOG 25 – BGP安全更新 – by Barry Raveendran Greene, Cisco Systems
- NANOG 26 – ISP安全–现实技术 – by Barry Raveendran Greene, Cisco Systems; Kevin Houle, CERT
- NANOG 28 – ISP安全：部署和使用污水池 by Barry Raveendren Greene, Cisco Systems; Danny McPherson, Arbor Networks
- NANOG 36 – ISP安全101入门 by Barry Greene, Cisco Systems and Roland Dobbins, Cisco Systems
- NANOG 47 – NSP-SEC十大安全技术 by Barry Greene, Juniper Networks
- NANOG 54 – 服务提供商“安全”工具套件 by Barry Greene, ISC (Part 1) & (Part 2)
- **MAAWG 26 – SP安全研讨会**
- CommunicAsia 2015讲习班

抵御拒绝服务攻击的背景原理





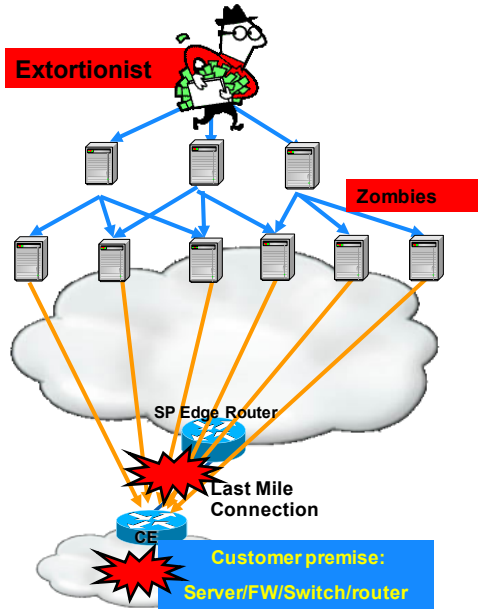


您如何真正阻止DDOS攻击？

- 管道清理，清理中心和其他“ Anti-DDOS”工具不能阻止DDOS攻击。
- 这些工具至关重要，但只能用于提供：

  选定任务关键服务的全面服务还原

  ✓ 是时候补救DDOS攻击



- 停止DDOS攻击需要具备以下能力：

1. 承受攻击，不屈服于勒索/威胁
2. 攻击源的可见性/追溯
3. 补救攻击中使用的工具（僵尸网络和反射器）
4. 回溯到用于发起攻击的C&C。
5. 对发起攻击的人员进行三角剖分。

拒绝服务弹性必备原则

为获利服务构建安全基础设施

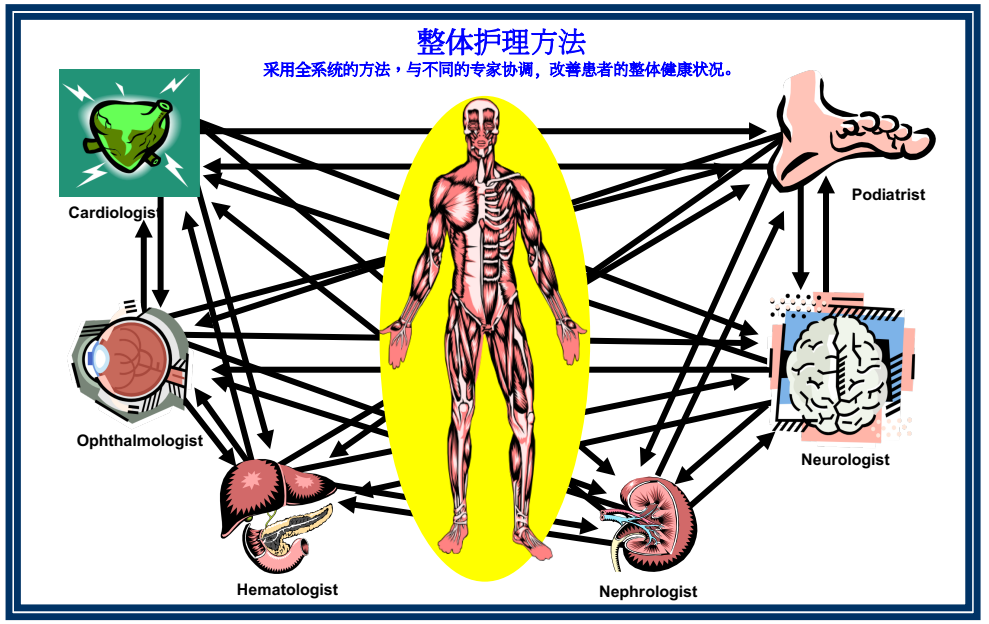
完全控制
网络中的所有流量

总可见度
在网络的各个方面 .

最大化可用性
所有服务。

可见性是什么意思?

- 可见性是电信行业的业务基础。
- 您需要了解客户在做什么，哪些应用程序在驱动网络，并了解业务的发展方向。
- 如今，大多数电信公司都无法使用 TCP / IP！

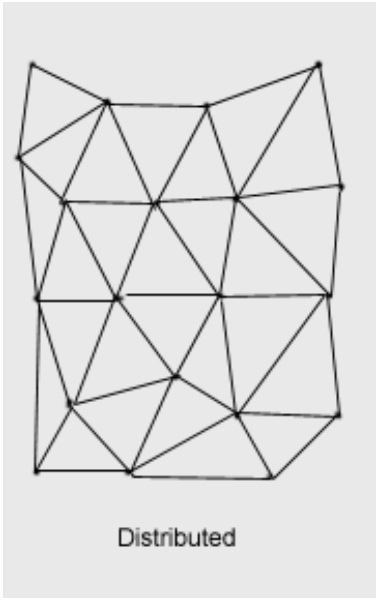


控制是什么意思？

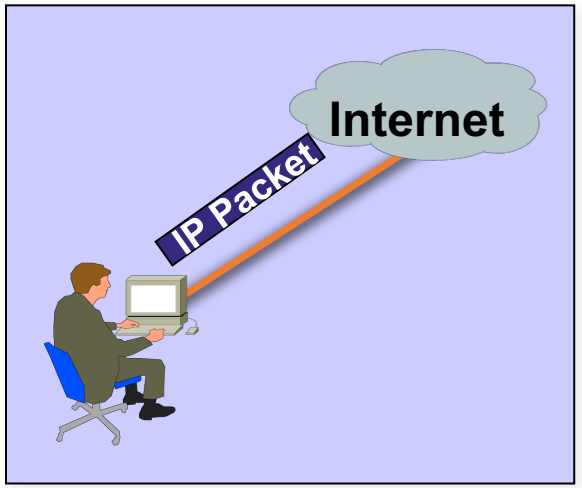
1. 您需要确切了解客戶和网络的状况。
2. 您需要能够基于这些知识来塑造，操纵和服务客户。
3. *您需要使网络保持不超过五个9*

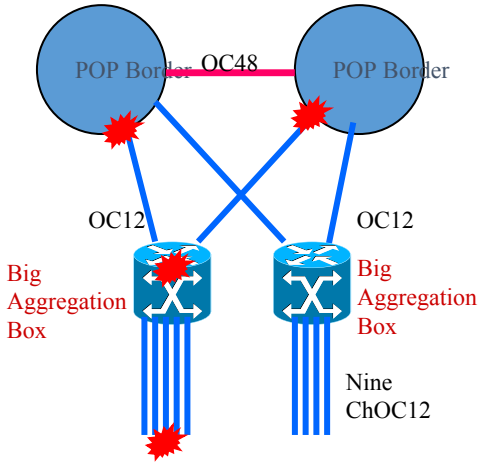
可用性是什么意思？

- 网络必须运行99.999%
- 我们使用Paul Baran可用性和弹性模型进行此操作。
- 问题：大多数知识产权工程师不知道PaulBaran可用性和弹性模型的原理。



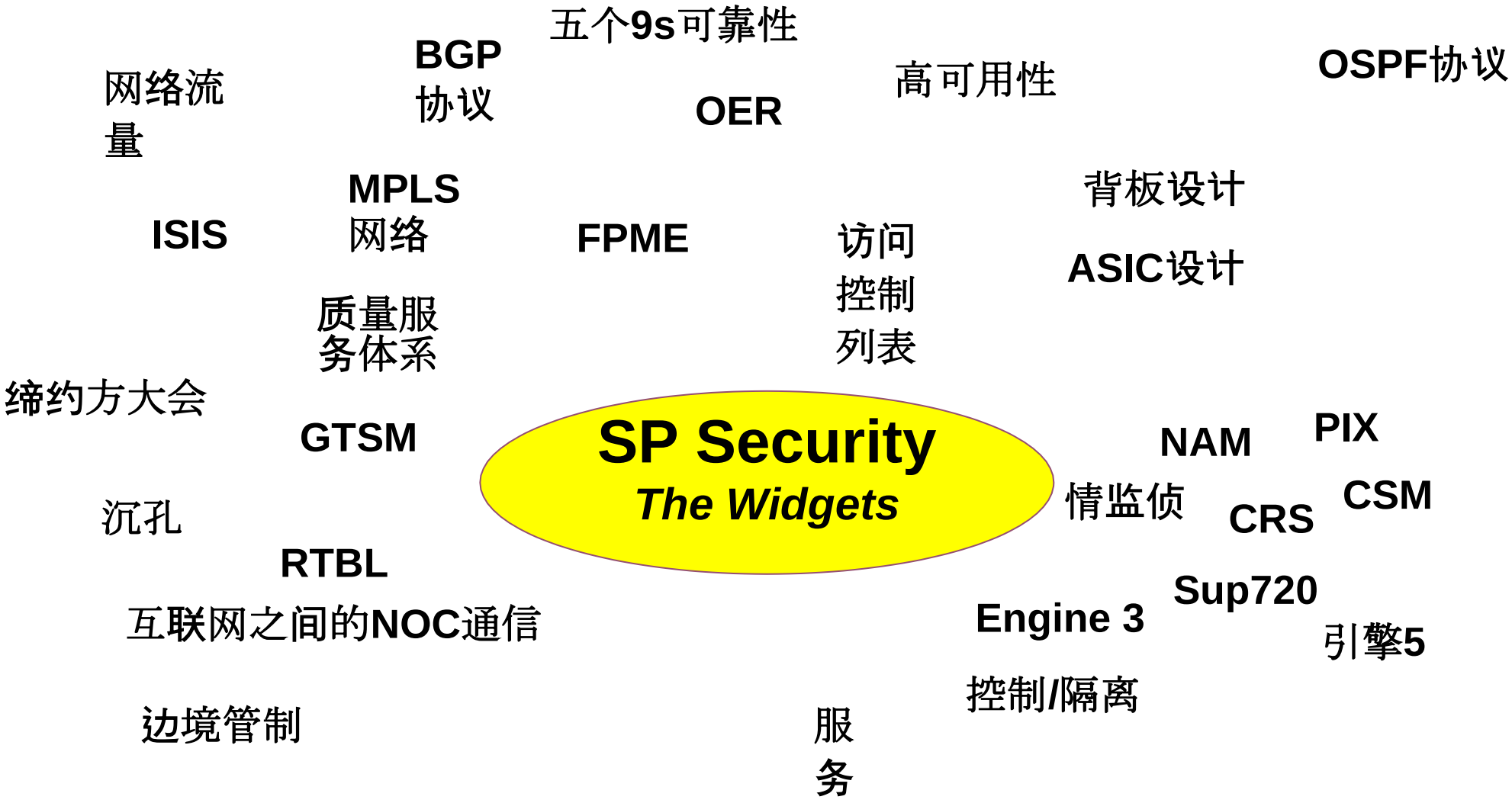
全部关于数据包.....



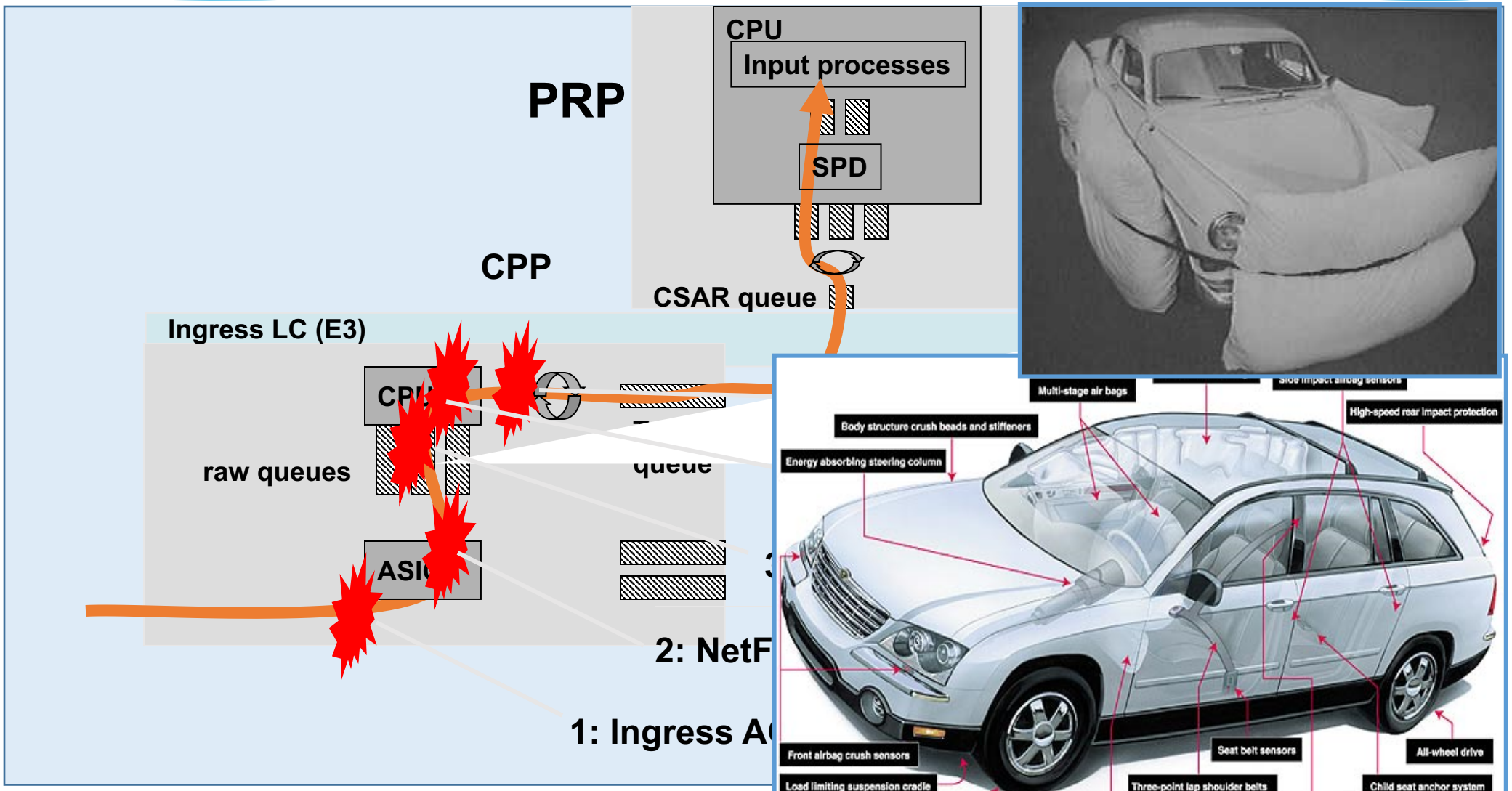


- 全部关于数据包.....
- 一旦数据包进入互联网，某个地方的某人必须执行以下两项操作之一：
  - *传递数据包*
  - *丢弃数据包*
- 在拒绝服务攻击的背景下，问题是“丢弃数据包”动作将在谁和哪里发生

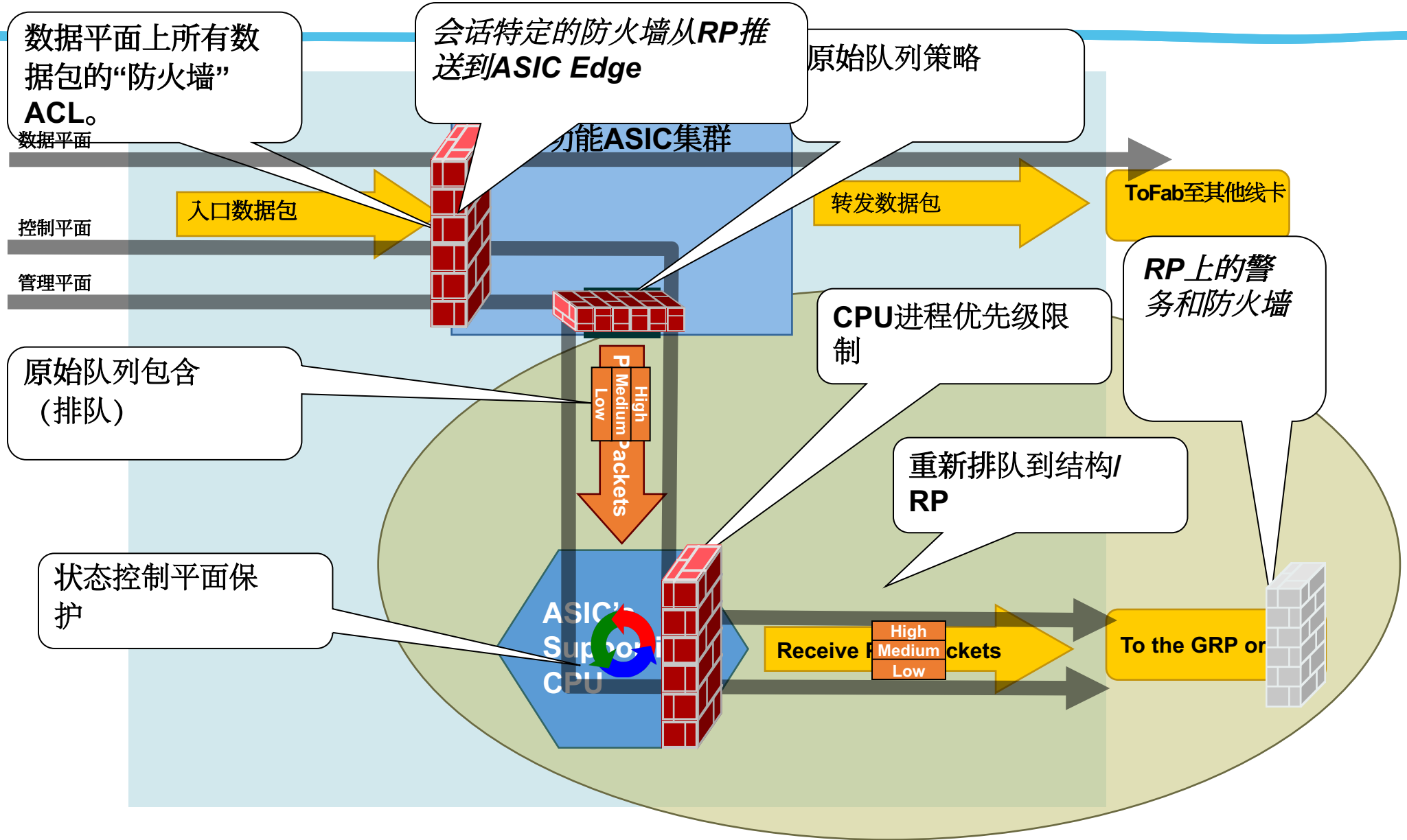
运营商安全工具包–全方位使用



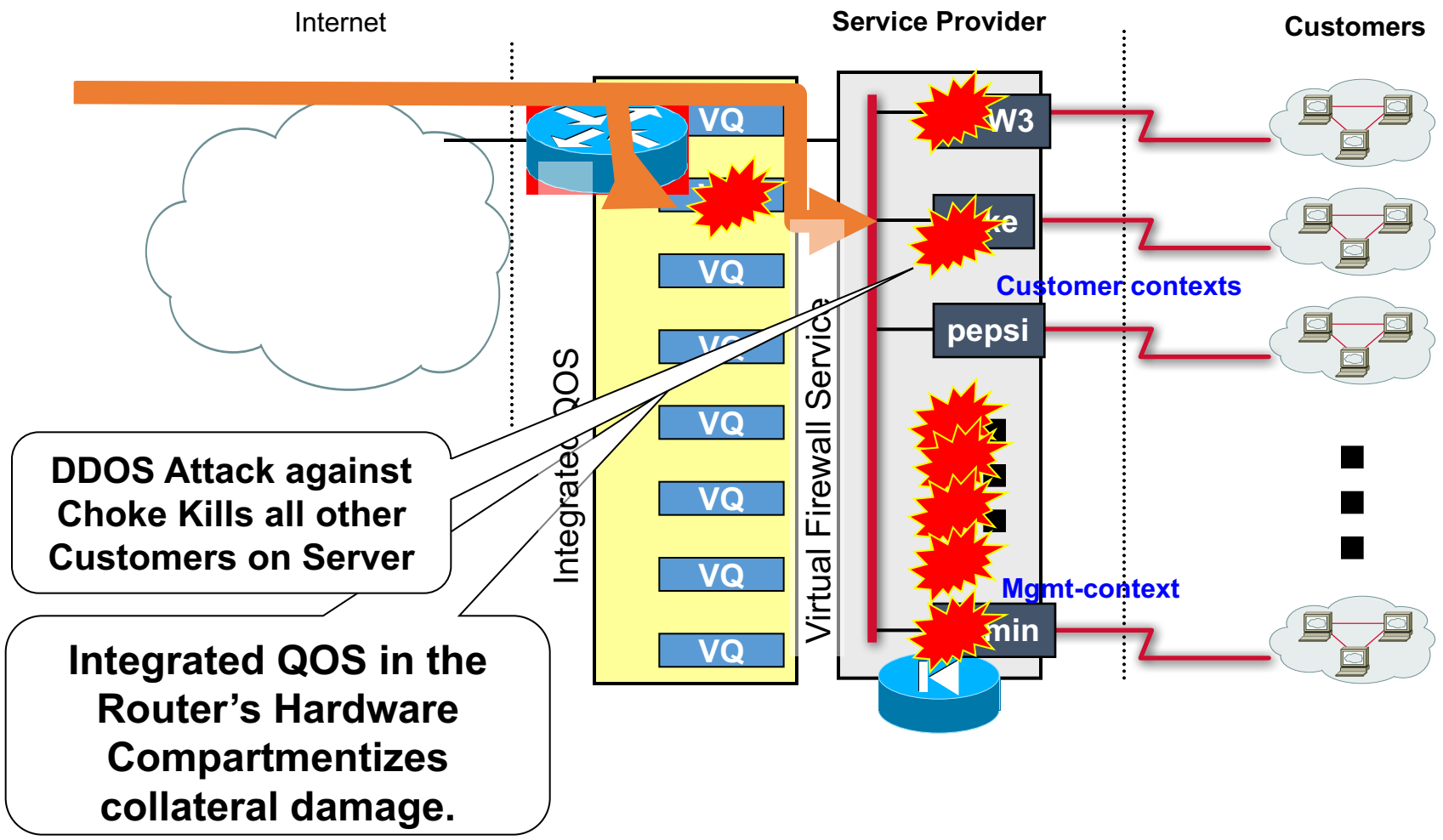
安全性不是事后的想法！


CPU
Input processes
PRP
SPD
CPP
CSAR queue
Ingress LC (E3)
raw queues
2: NetF
1: Ingress A
Multi-stage air bags
Body structure crush beads and stiffeners
Energy absorbing steering column
High-speed rear impact protection
Front airbag crush sensors
Load limiting suspension cradle
Tire pressure monitoring
Seat belt sensors
Three-point lap shoulder belts
Inflatable knee blocker
Seat belt pretensioners, constant force retractors
All-wheel drive
Child seat anchor system

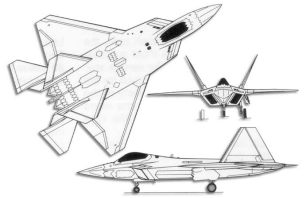
如何保护路由器内部?


数据平面上所有数据包的“防火墙”ACL。
会话特定的防火墙从RP推送到ASIC Edge
原始队列策略
数据平面
控制平面
管理平面
功能ASIC集群
入口数据包
转发数据包
ToFab至其他线卡
RP上的警务和防火墙
CPU进程优先级限制
原始队列包含（排队）
High
Medium
Low
重新排队到结构/RP
状态控制平面保护
ASIC's
CPU
Receive
ckets
To the GRP or

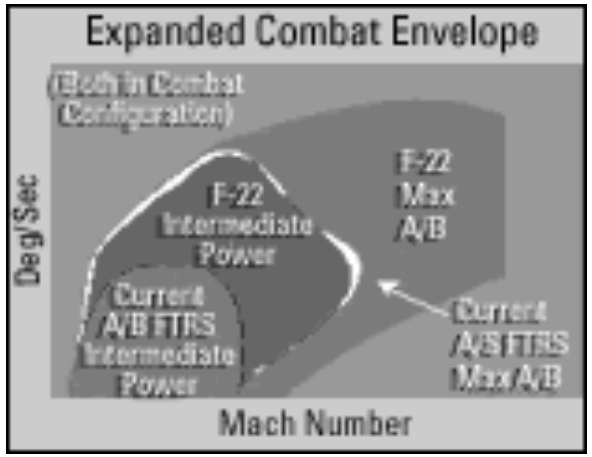
Throwing Hardware at the Problem?

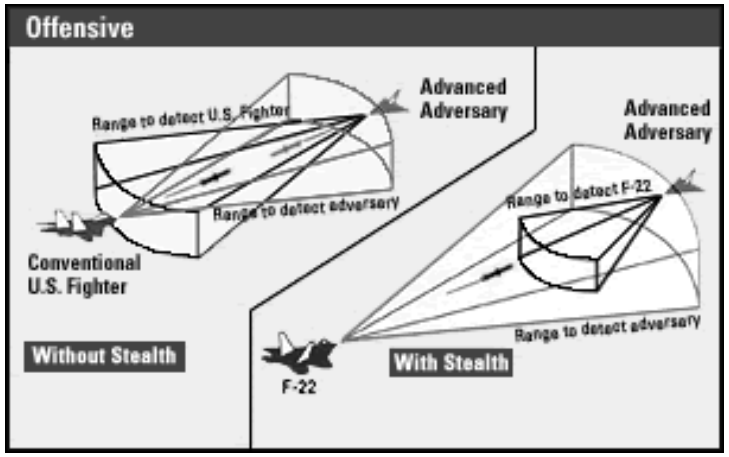


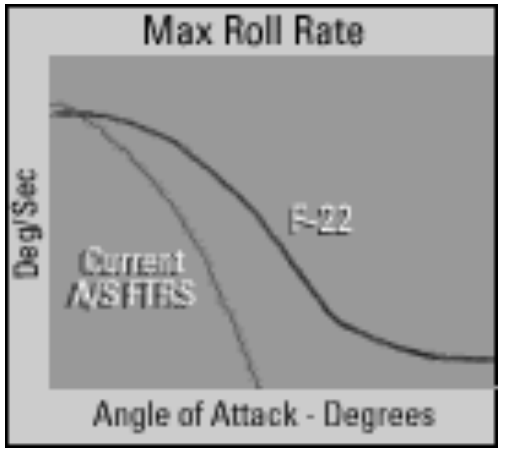
你在推信封吗？



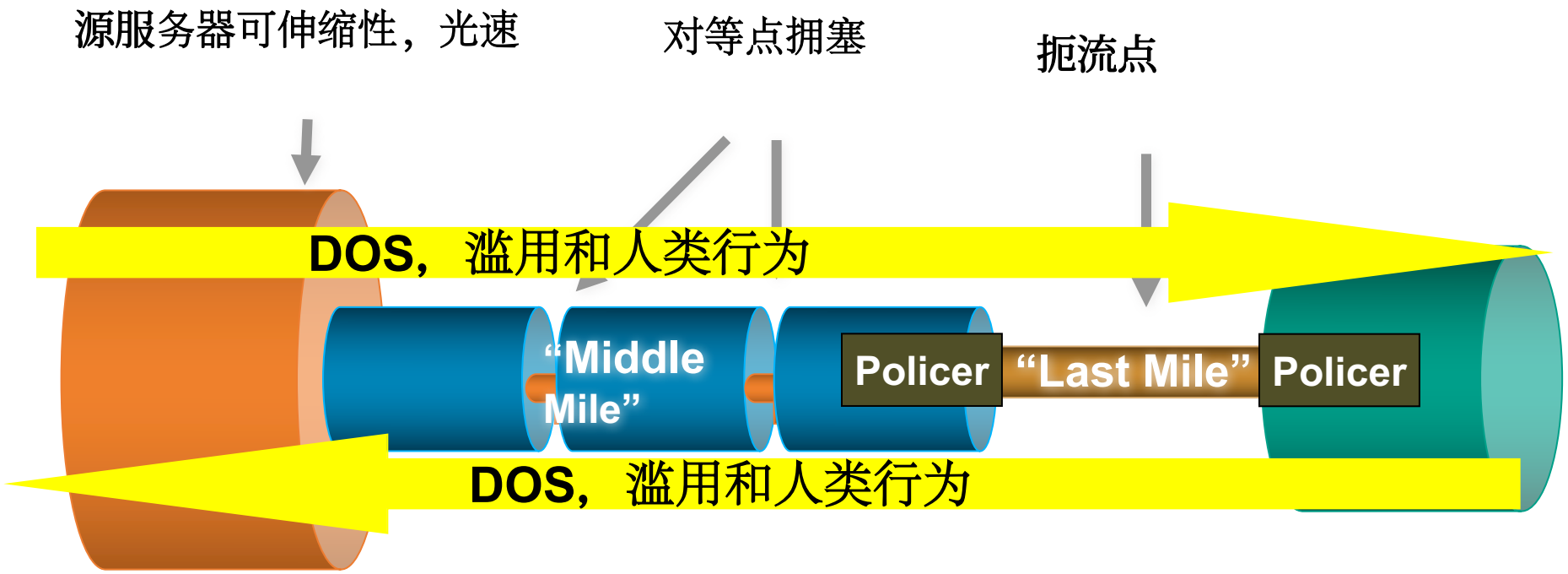
- 了解您的设备和基础设施：
  - 了解所有设备（路由器，交换机，工作站等）的性能包络。您需要知道设备的真正功能。如果不能自己动手，那就需要采购。
  - 了解网络功能。如果可能，进行测试。在安全事件期间，惊喜并不好。



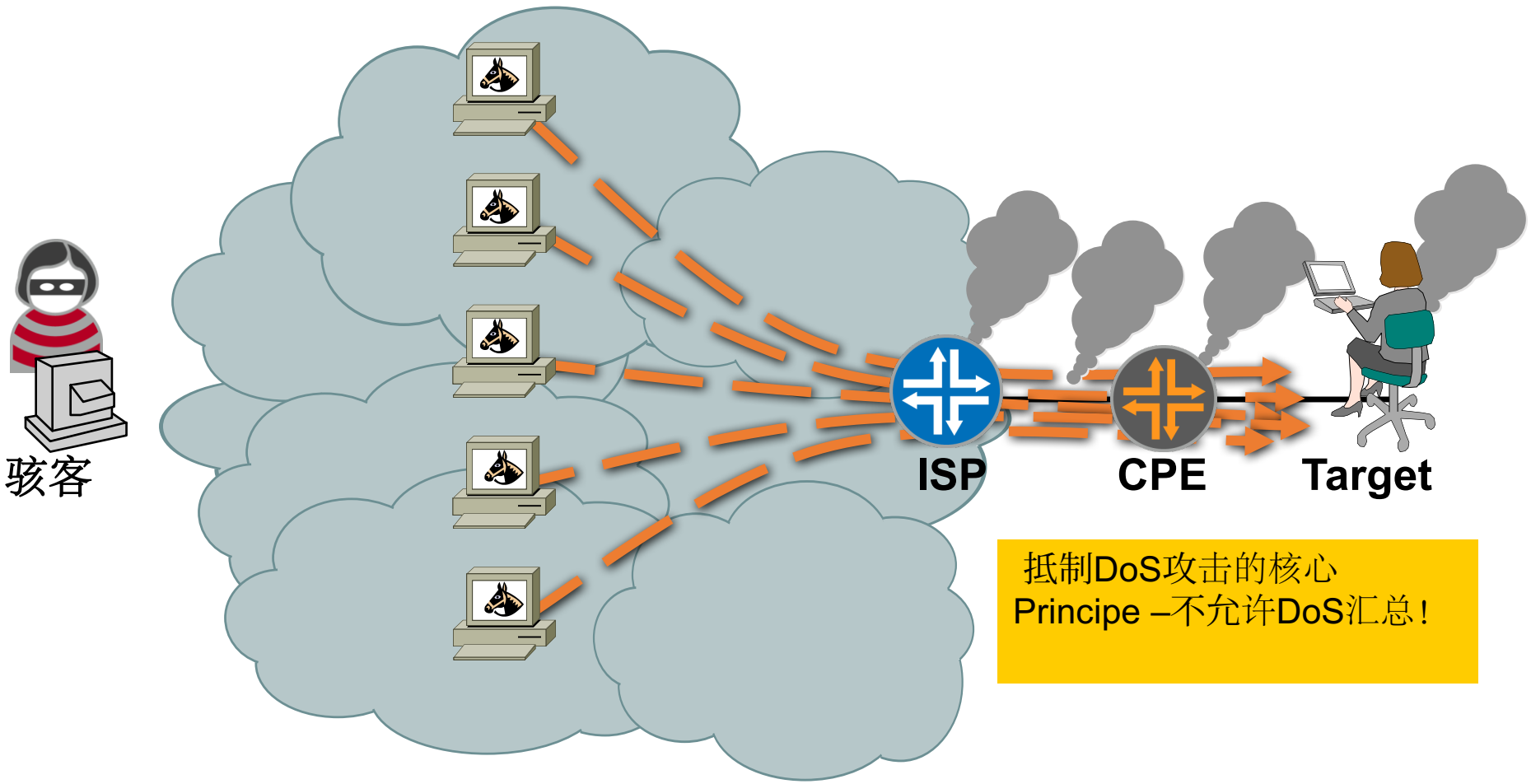




阻塞点=附带损害

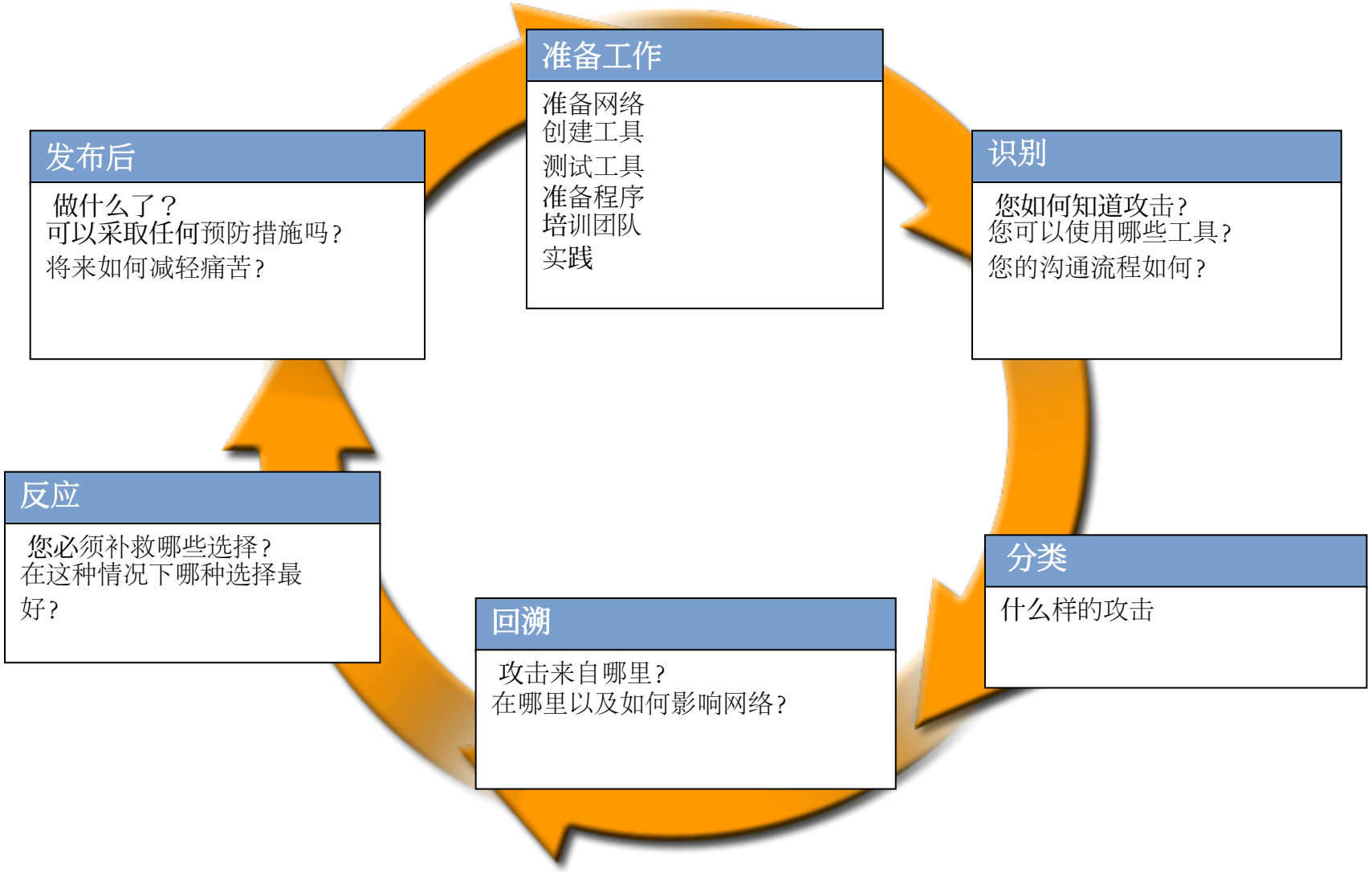

源服务器可伸缩性，光速
对等点拥塞
扼流点
DOS，滥用和人类行为
“Middle Mile”
Policer
“Last Mile”
Policer
DOS，滥用和人类行为
互联网骨干网跨互联网
连接
局部循环
处所网络

拒绝服务聚合点

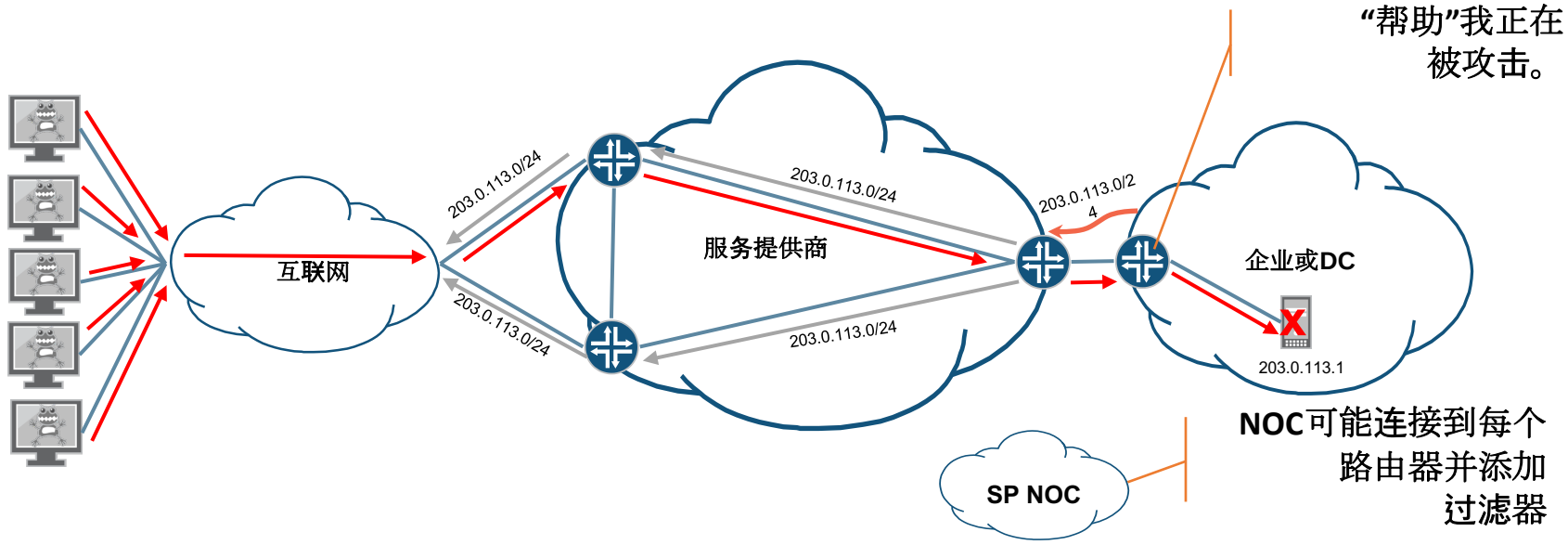


抵制DoS攻击的核心
Principe –不允许DoS汇总！

事故响应的六个阶段

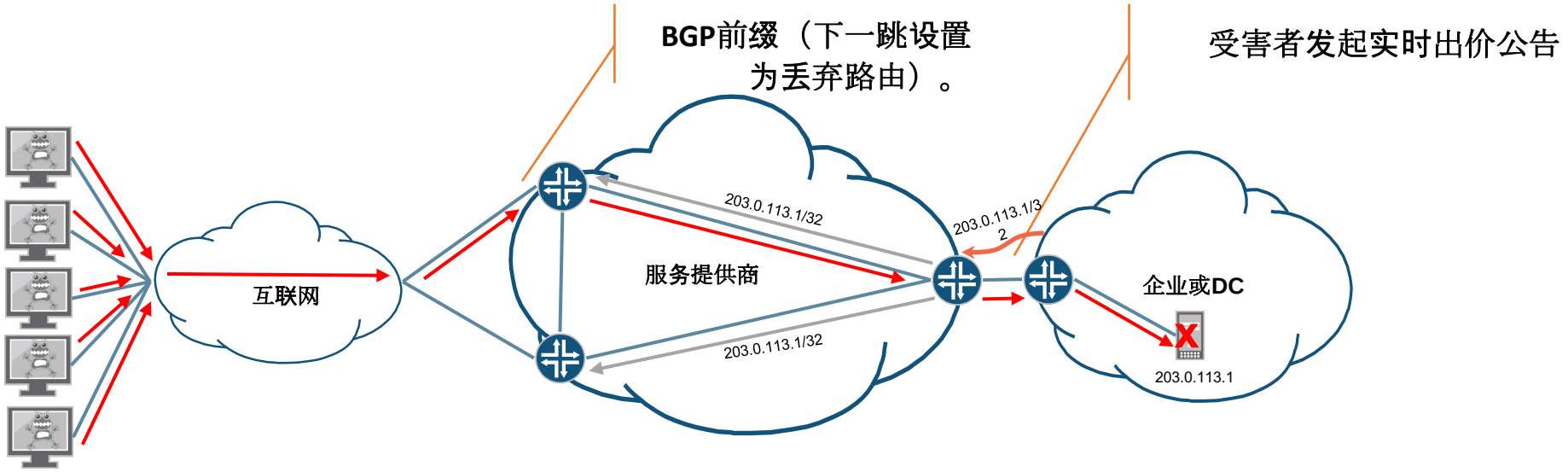

准备工作
准备网络
创建工具
测试工具
准备程序
培训团队
实践
识别
您如何知道攻击？
您可以使用哪些工具？
您的沟通流程如何？
分类
什么样的攻击
回溯
攻击来自哪里？
在哪里以及如何影响网络？
反应
您必须补救哪些选择？
在这种情况下哪种选择最好？
发布后
做什么了？
可以采取任何预防措施吗？
将来如何减轻痛苦？

在过去，阻止分布式拒绝服务



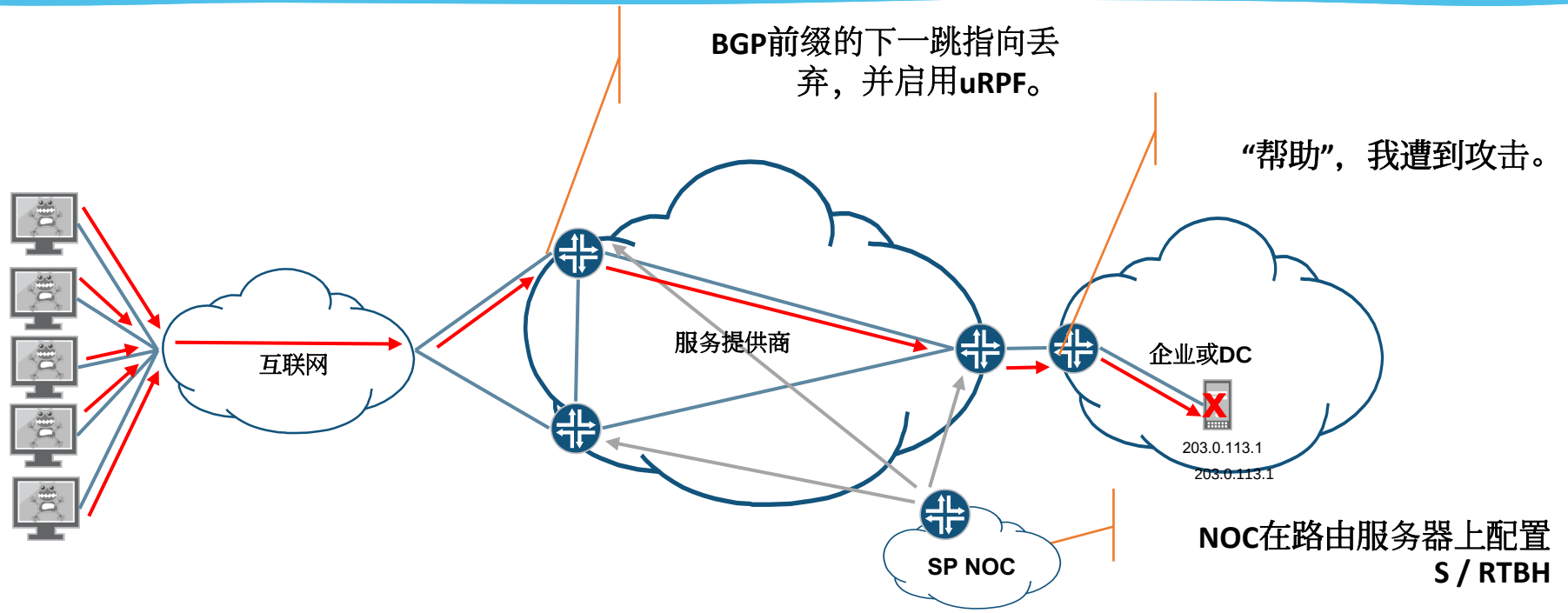
- 易于实施，并使用易于理解的结构
- 需要客户和提供商之间的高度协调
- 在大型网络外围扩展规模较大
- 错误配置的可能和代价

目标远程触发黑洞（D / RTBH）



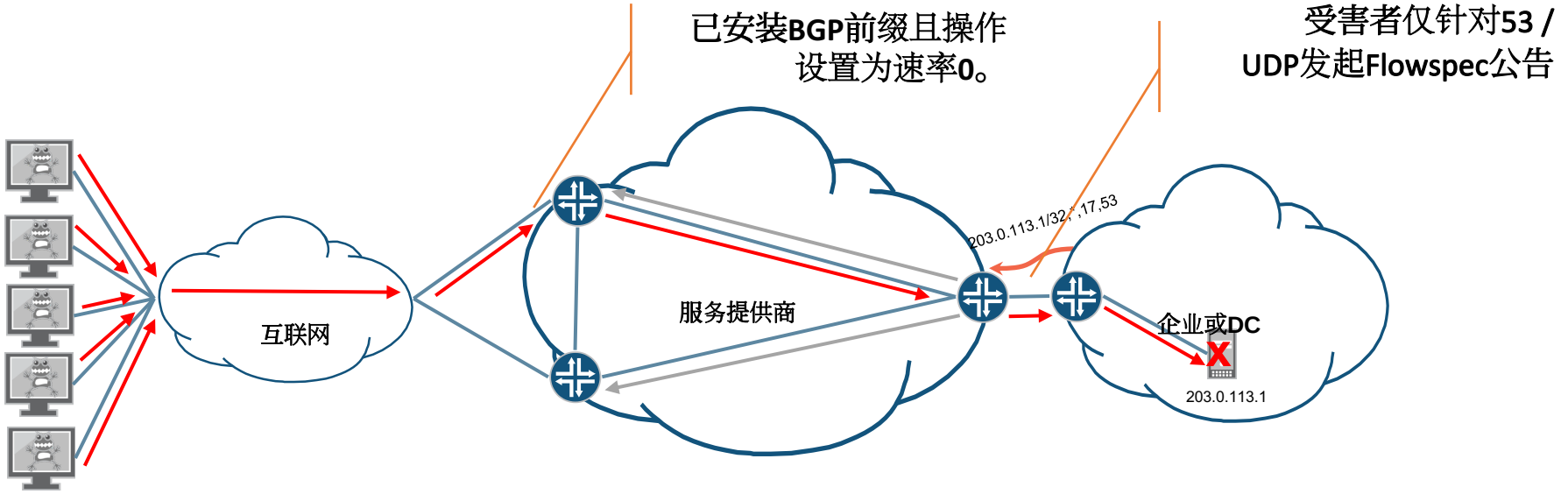
- 大约2000年的RFC 3882
- 需要在所有边缘路由器上预先配置丢弃路由
- 受害者的目的地地址完全无法到达，但攻击（和附带破坏）已经停止。

源远程触发黑洞（S / RTBH）



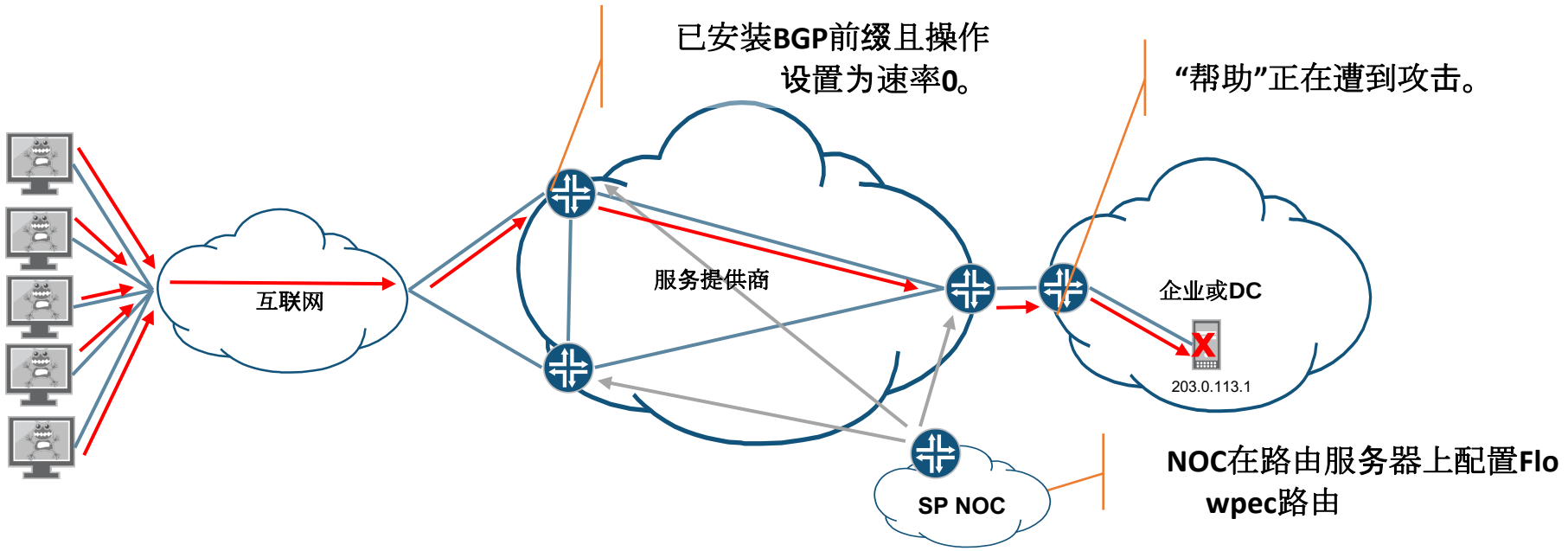
- 大约在2005年的RFC 5635
- 需要在所有边缘路由器上预先配置丢弃路由和uRPF
- 被攻击者的目的地地址仍然可用仅适用于单个（或少量）源。

使用Flowspec进行域间分布式拒绝服务防护



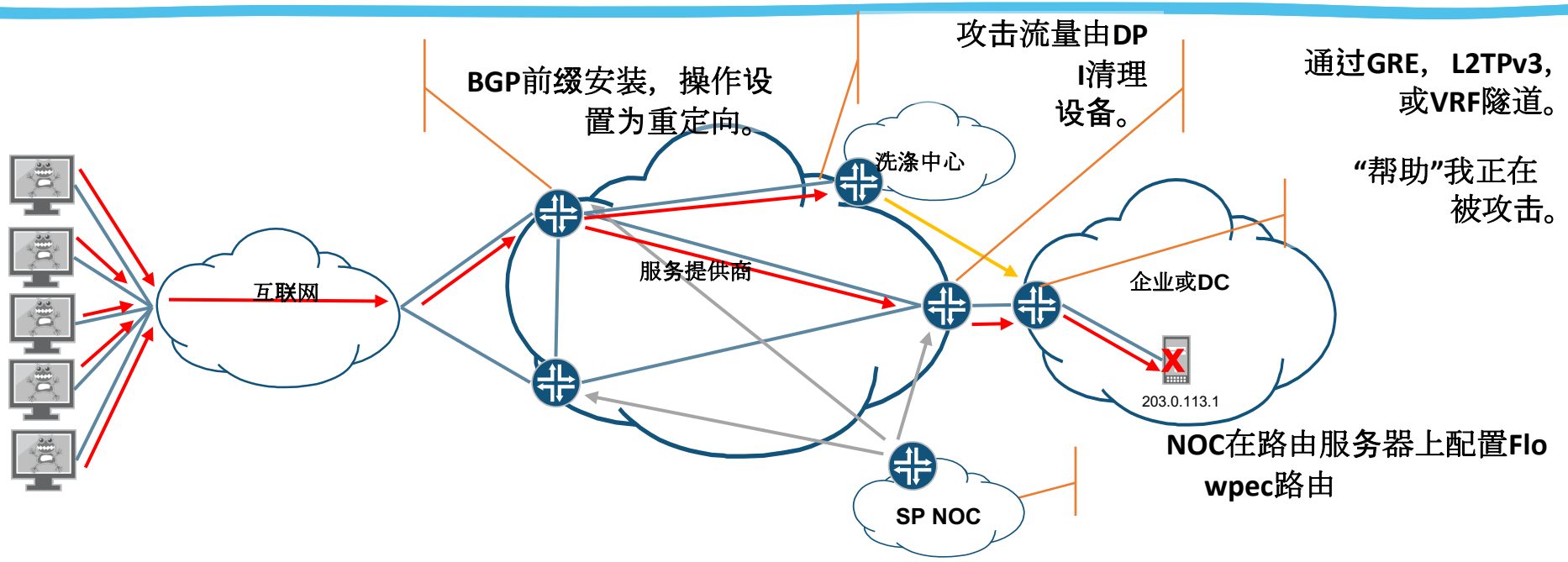
- 允许ISP客户启动过滤器。
- 需要在客户边缘进行理性的过滤。

使用Flowspec进行域内分布式拒绝服务防护



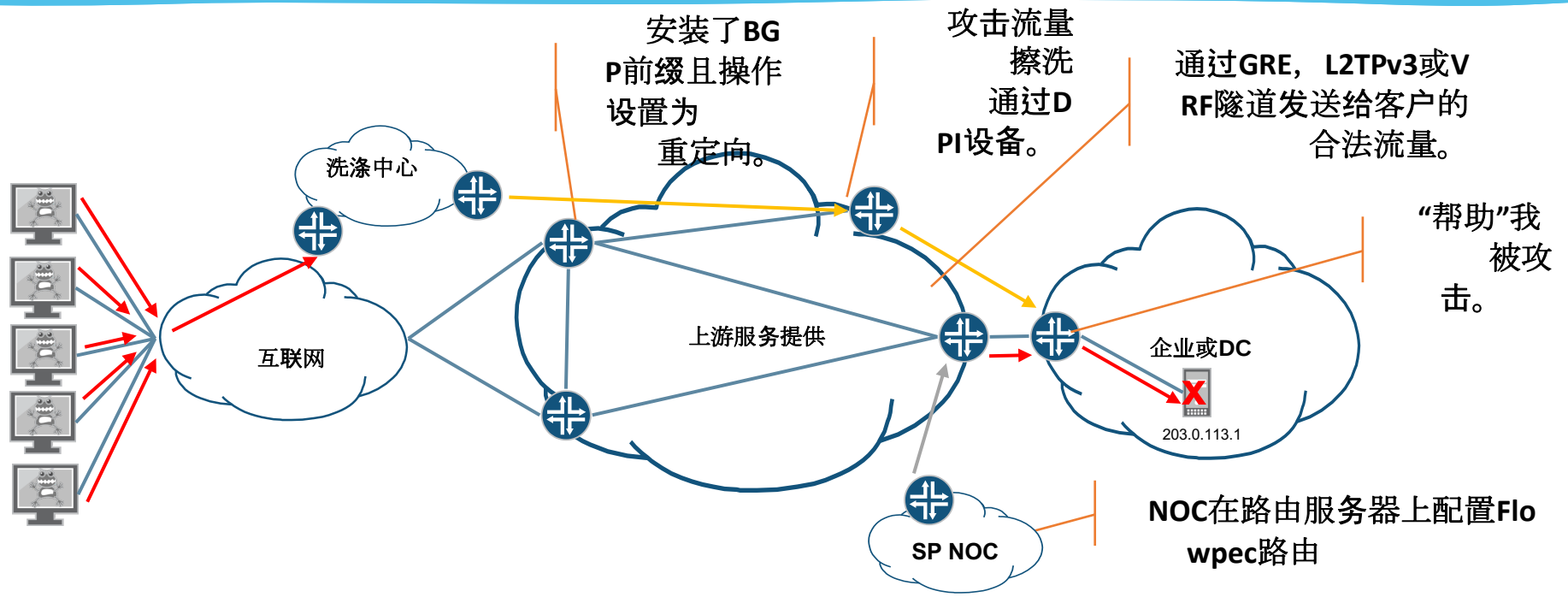
- 可以通过电话，SP网络中的检测或客户的网络门户启动。
- 需要客户和提供商之间的协调。

使用清理中心缓解分布式拒绝服务



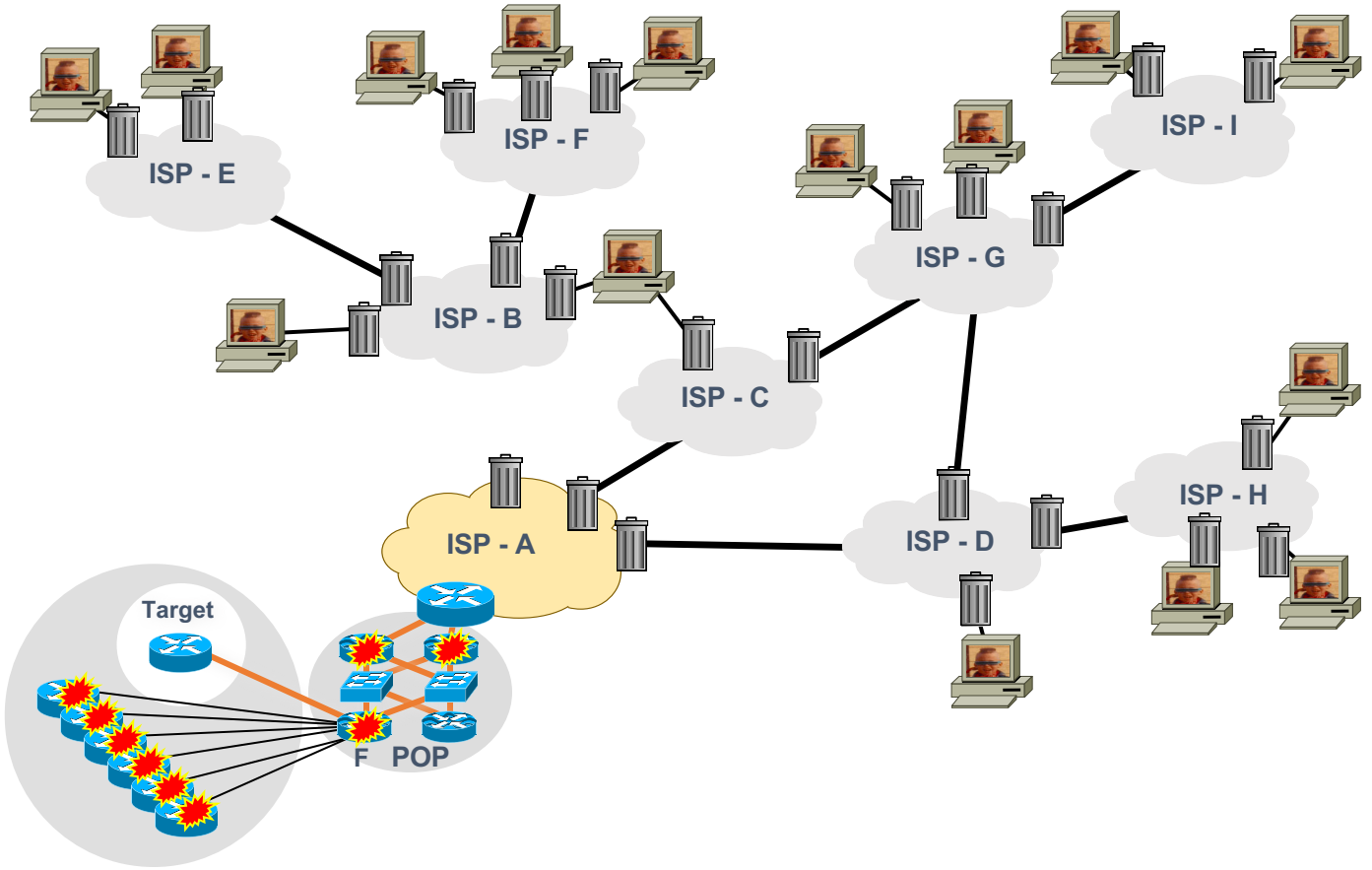
- 可以通过电话，SP网络中的检测或客户的网络门户启动。
- 允许缓解应用程序层攻击而无需完成攻击。

使用清理中心缓解分布式拒绝服务

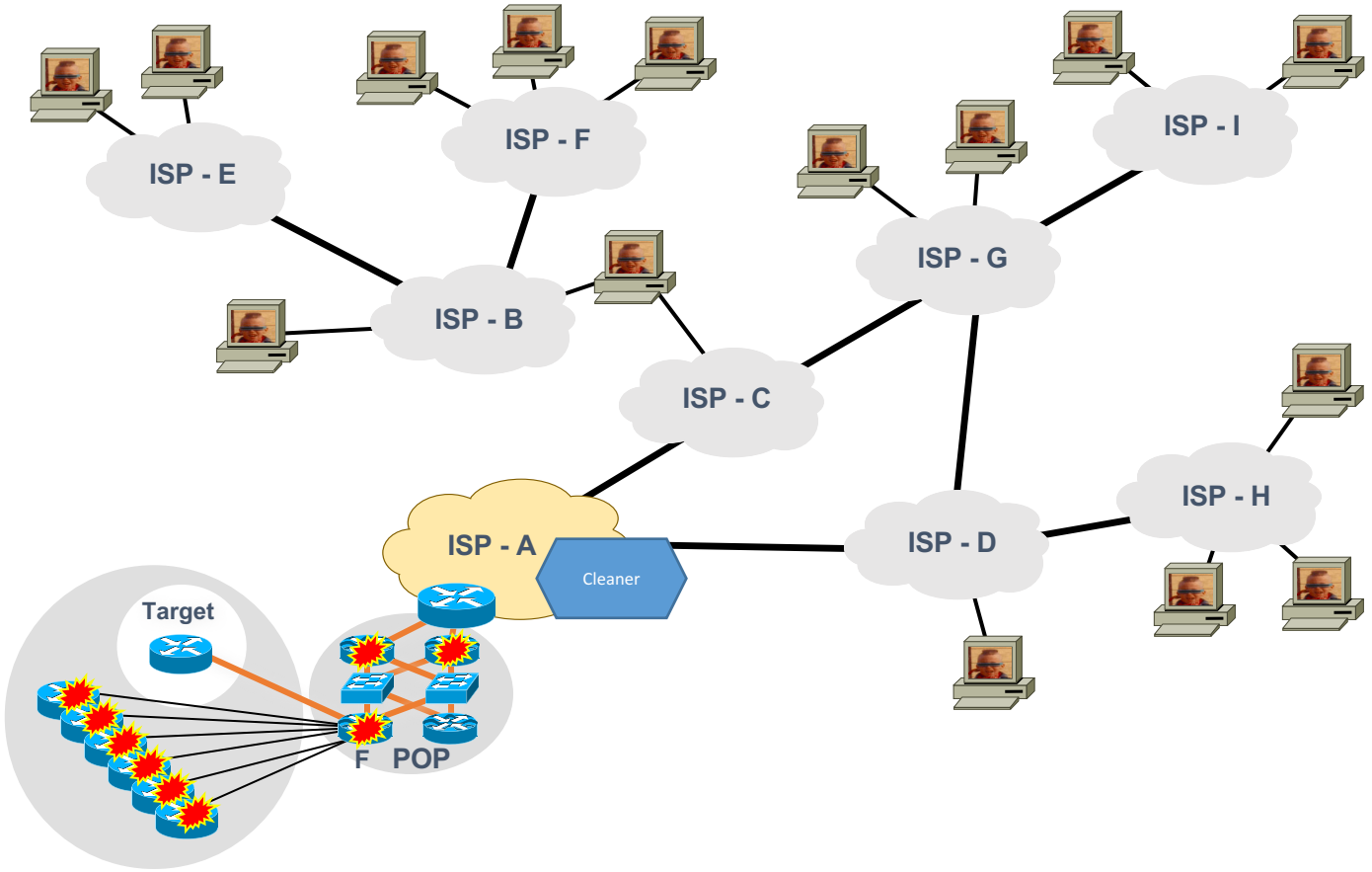


- 可以通过电话，SP网络中的检测或客户的网络门户启动。
- 允许缓解应用程序层攻击而无需完成攻击。

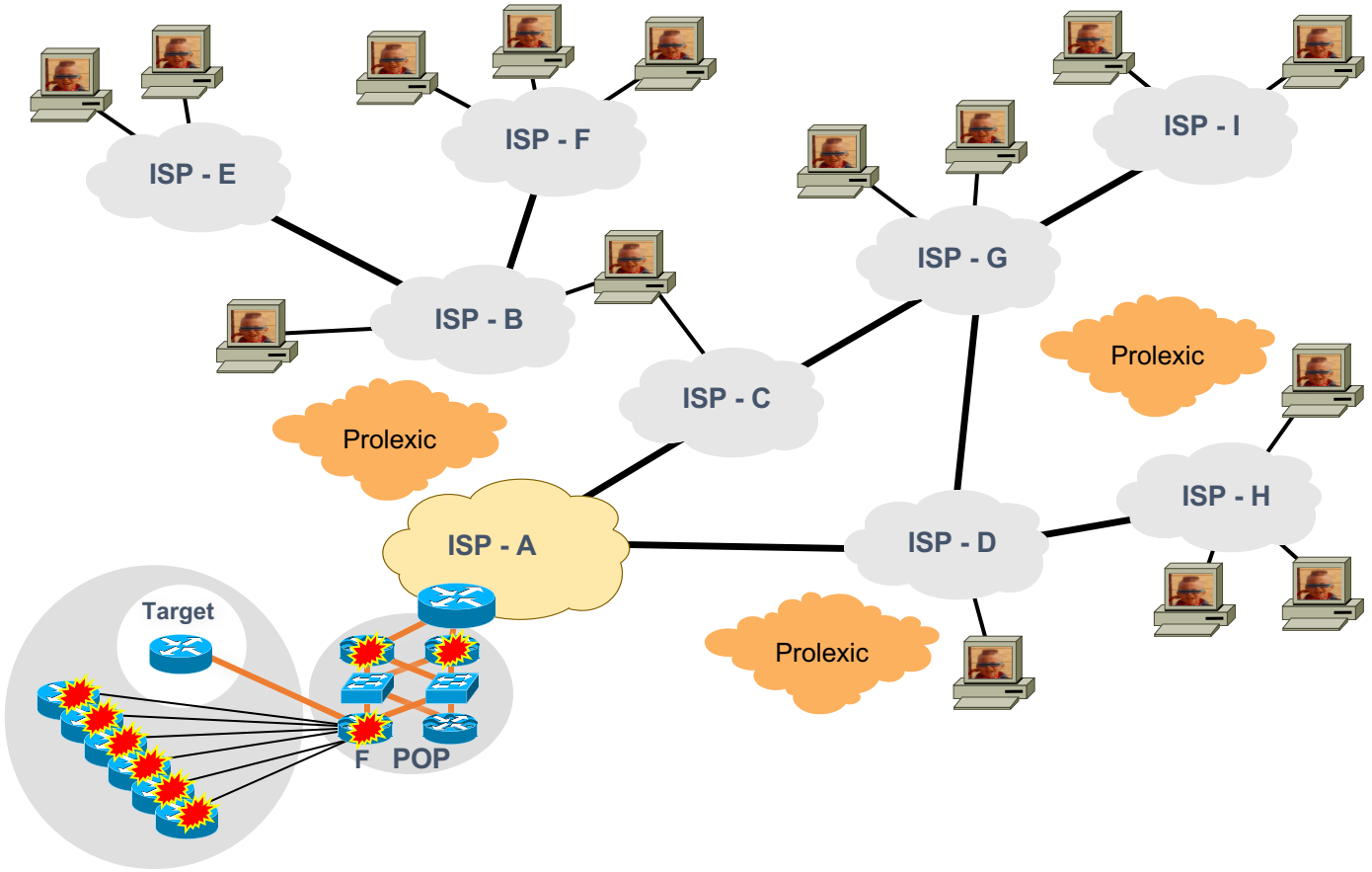
当今的DDOS –我们可以使用RTBH进行后退



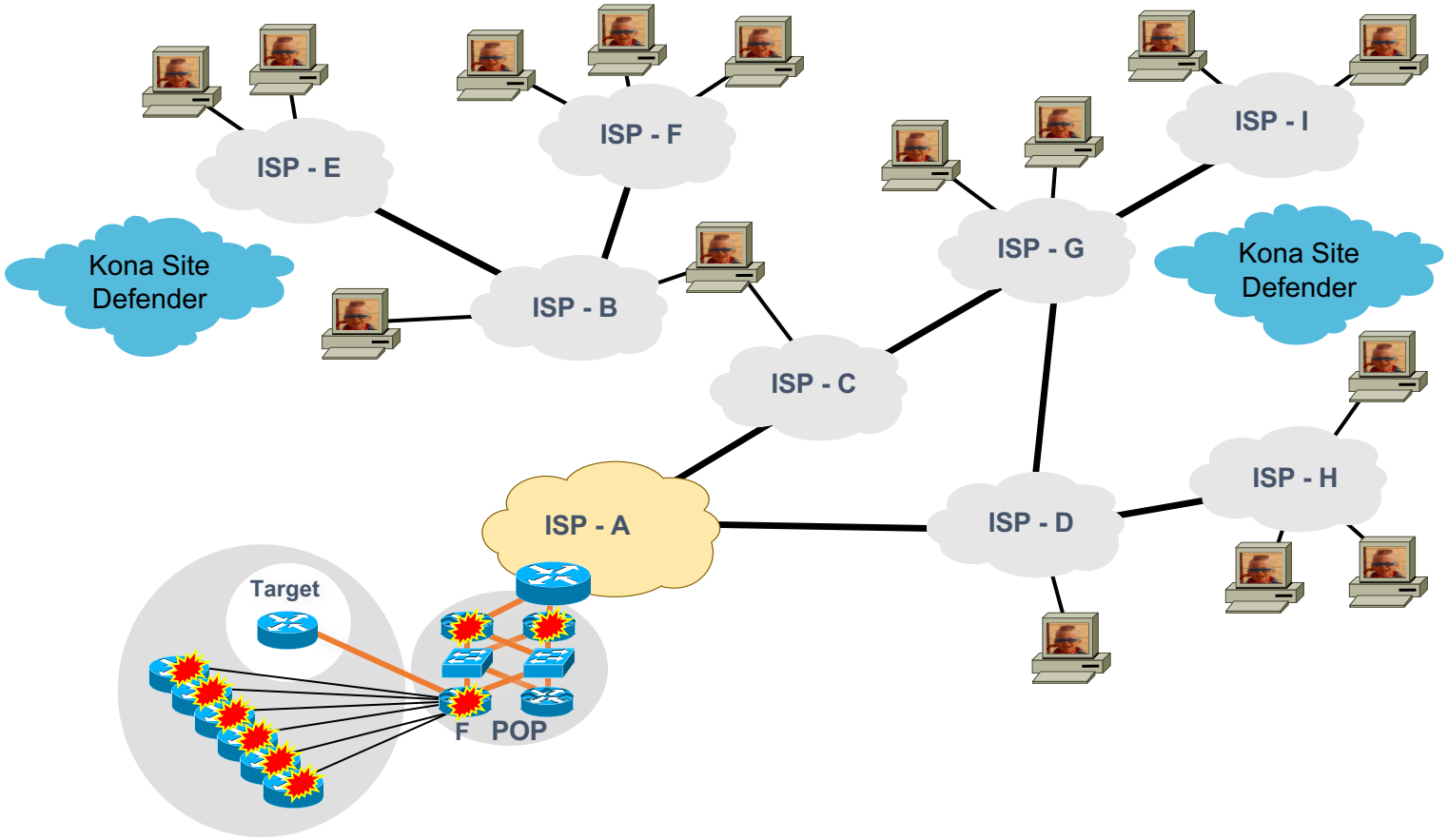
今日DDOS –抵御攻击–内部清理



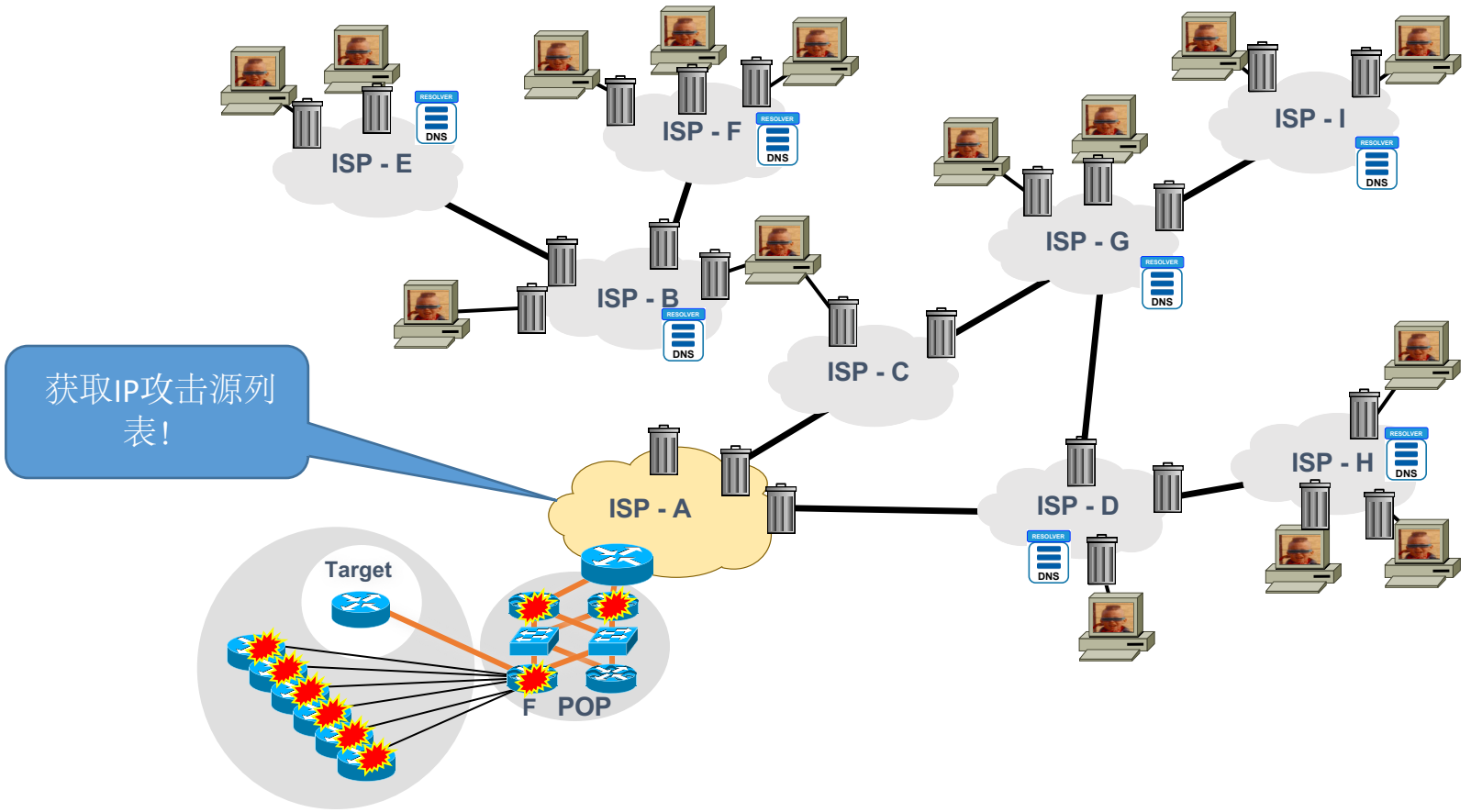
今日DDOS –克服攻击–脱离前提



当今的DDOS –构建更多的弹性服务

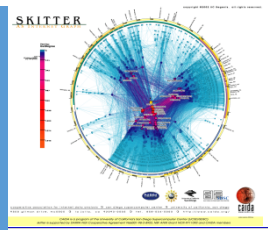


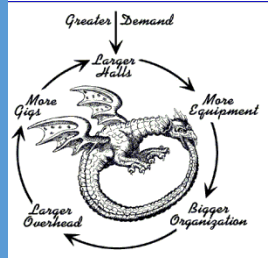
现在我们可以作为联邦的一部分进行补救

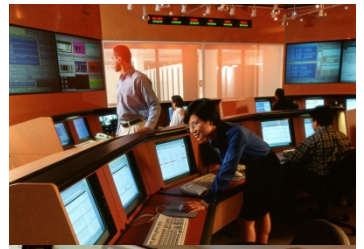


暂停提问

工具投入使用iDDOS攻击



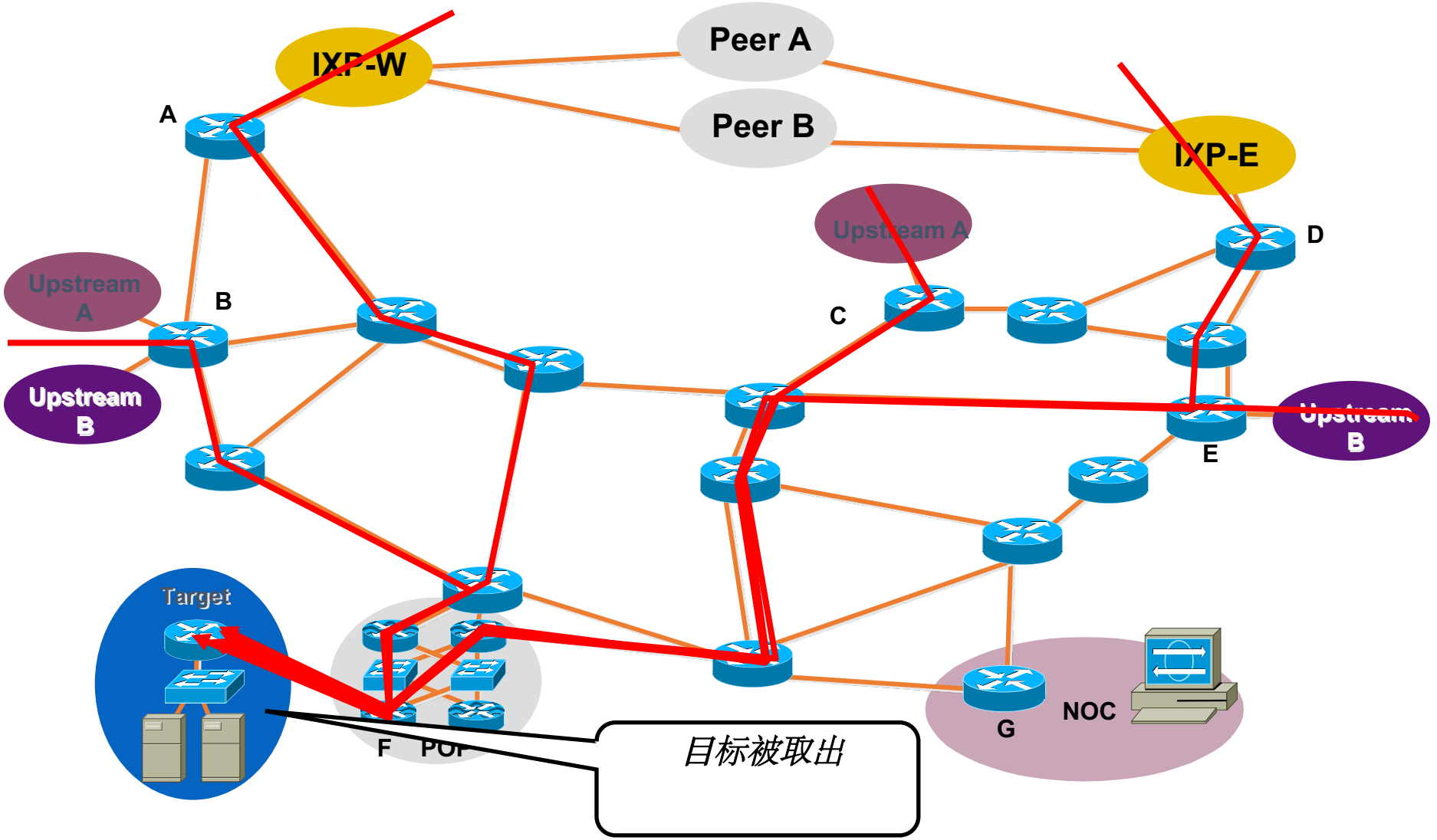




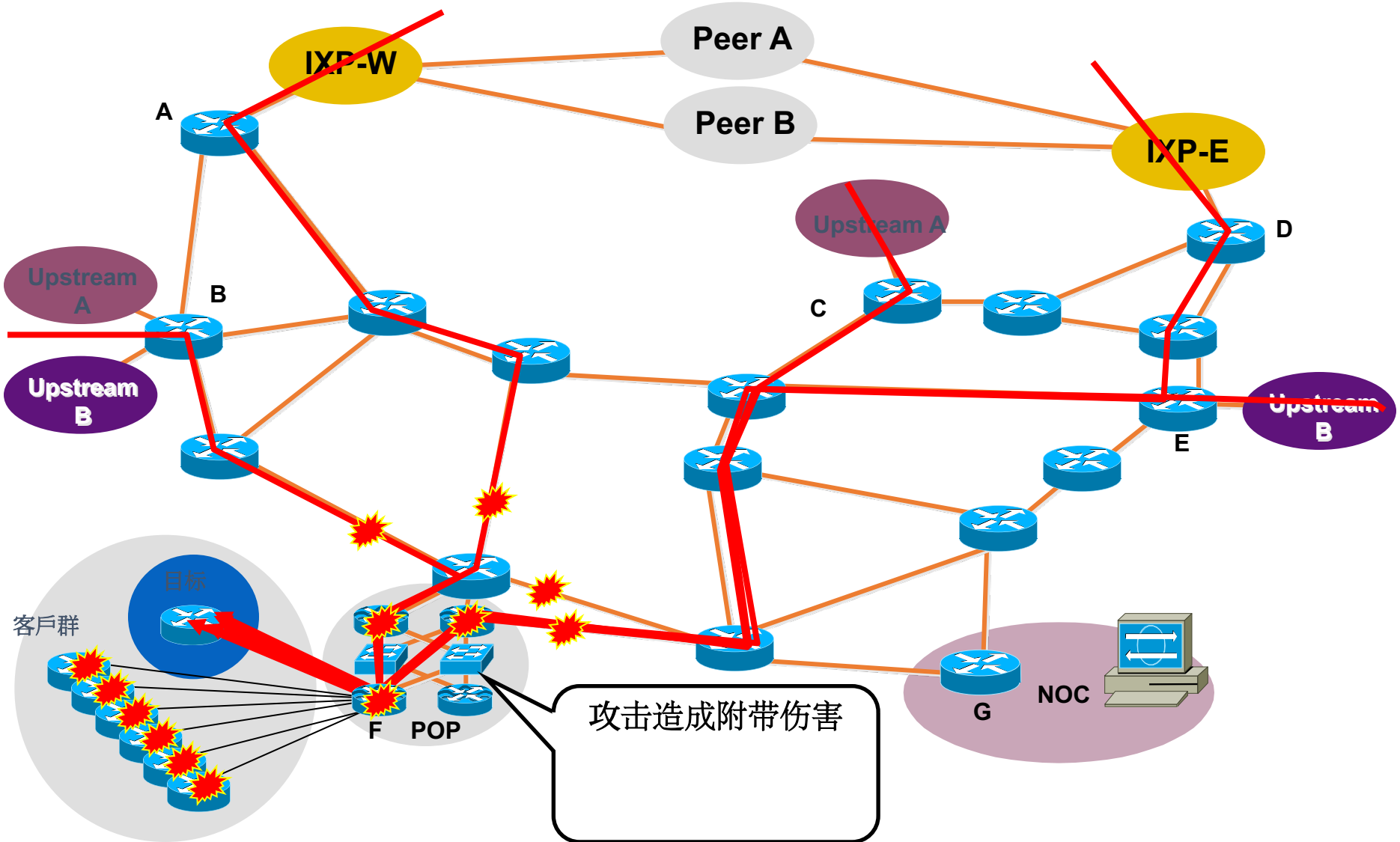
SITREP

- 网络中一切正常。
- 然后，警报响起-网络中发生了一些事情。

拒绝客户使用之前


IXP-W
Peer A
Peer B
IXP-E
A
B
C
D
E
F
G
Upstream A
Upstream B
Upstream A
Upstream B
Target
POP
NOC
目标被取出

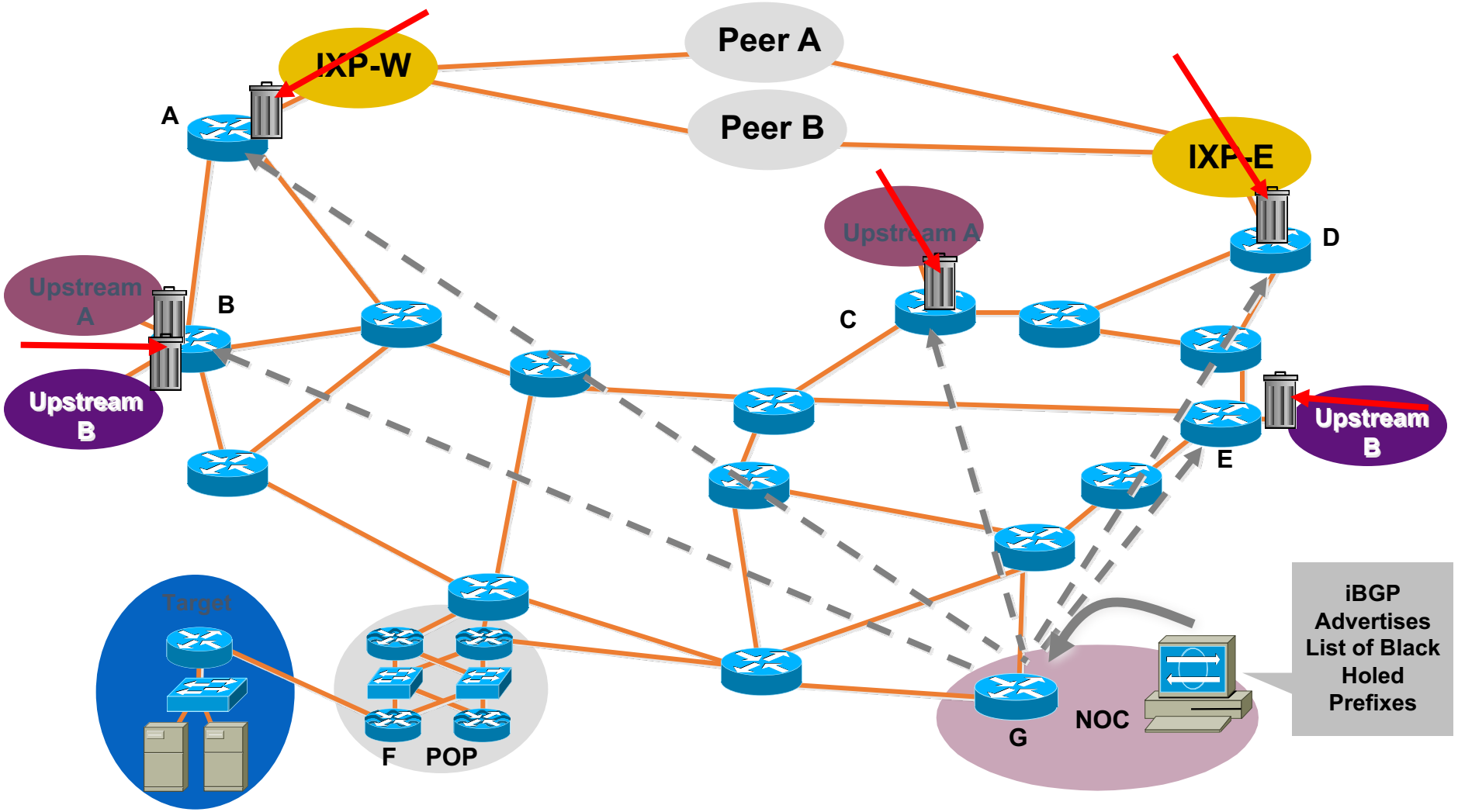
DOS（先于）客戶附带损害赔偿



SITREP –进行中的攻击

- 对客户的攻击正在影响许多客户。
- 侧面损坏事故！
- 立即采取的行动：解决附带损害问题。

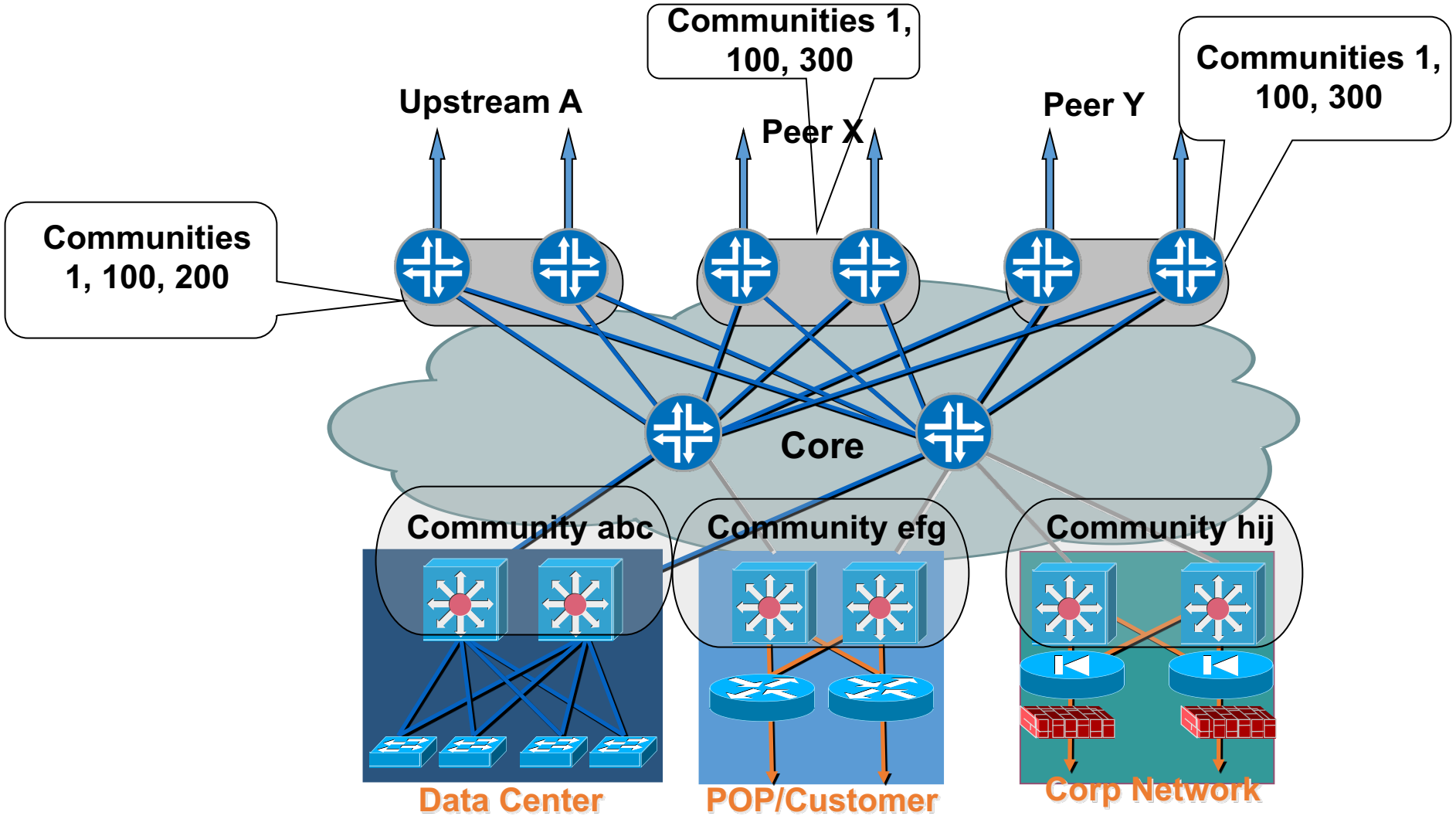
DOS丢弃客户后，数据包丢弃被推送到边缘



SITREP – 正在进行的攻击

- 附带损害减轻
- 被攻击的客户拥有部分服务。
- DOS攻击仍然有效
- 选项：
  - 汇槽分析的一部分流量。
  - 观察DOS攻击，等待攻击轮播或停止。
  - 激活“清洁管道”以进行全面服务恢复。

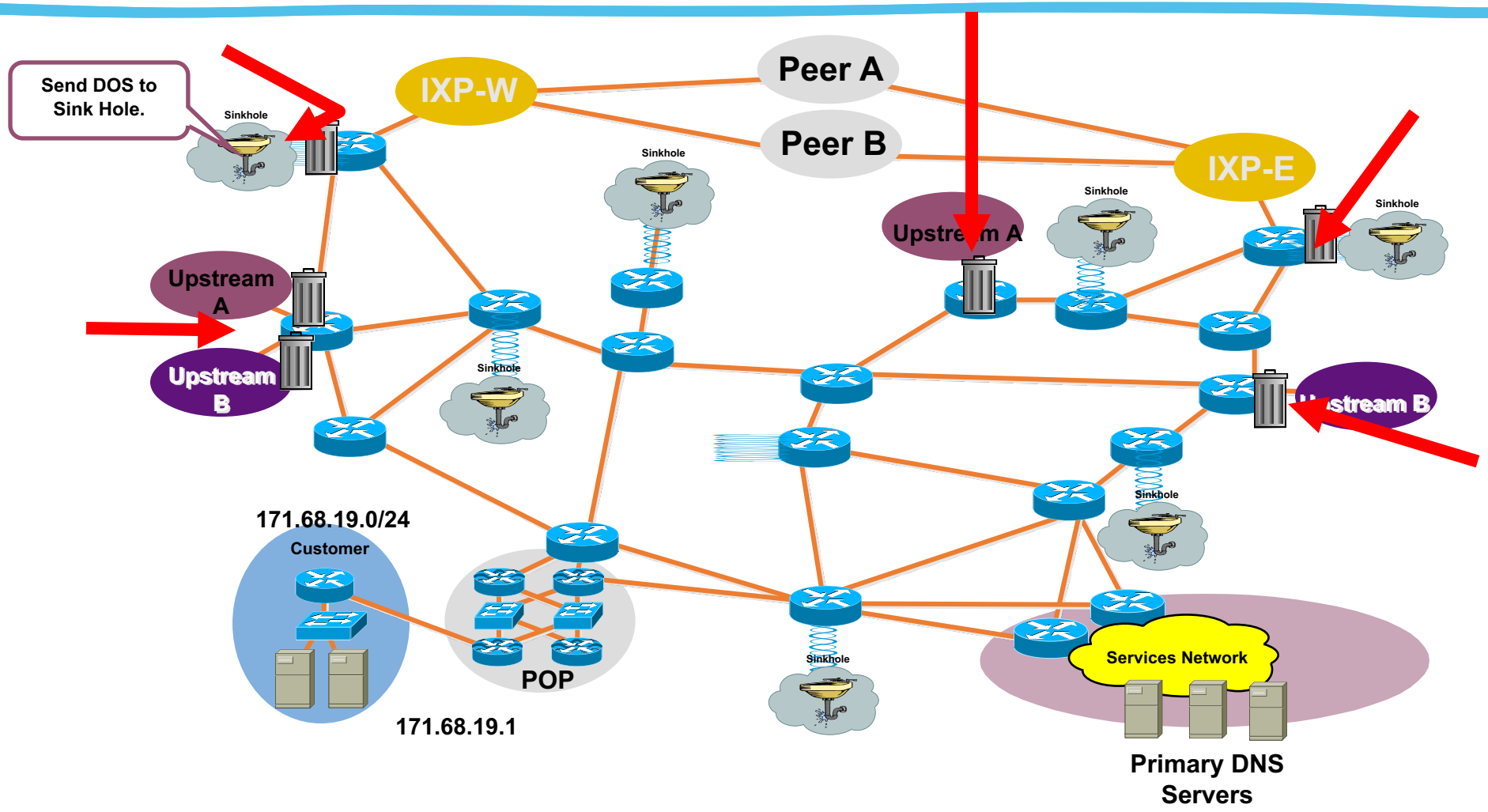
远程触发的丢弃和BGP社区



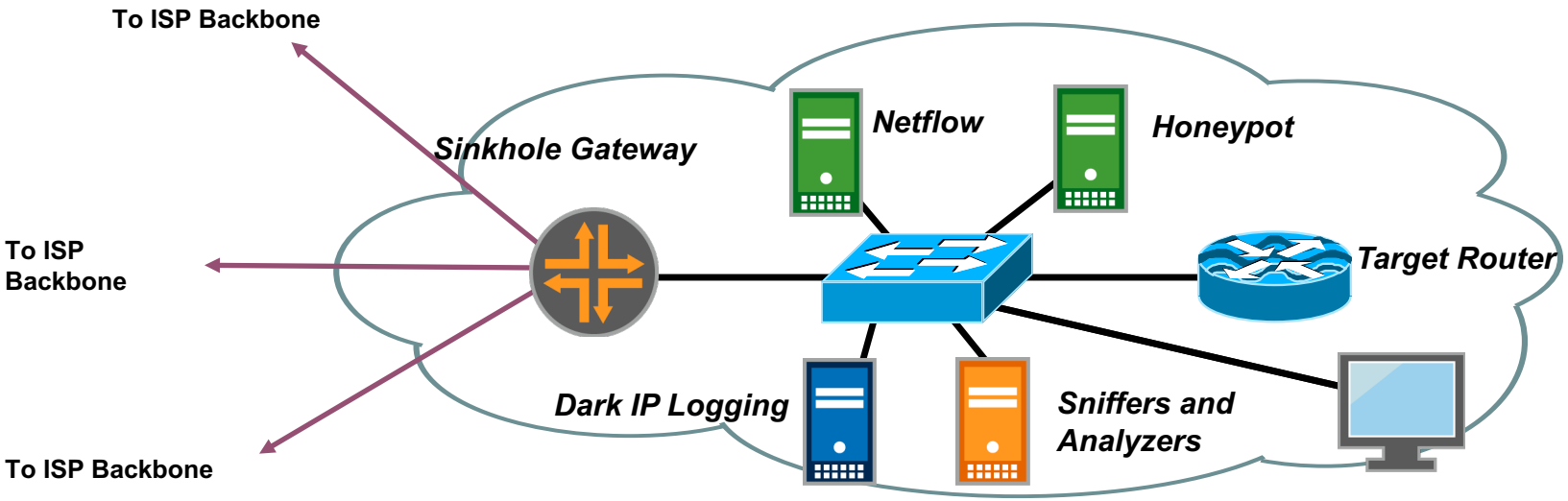
SITREP – 正在进行的攻击

- 附带损害减轻
- 被攻击的客户拥有部分服务。
- DOS攻击仍然有效
- 行动：监控攻击并获取有关攻击的更多详细信息
  –使用基于BGP社区的触发将一个区域流发送到一个汇槽

BGP社区触发污水池


Send DOS to Sink Hole.
Sinkhole
IXP-W
Peer A
Peer B
IXP-E
Upstream A
Upstream B
171.68.19.0/24
Customer
POP
171.68.19.1
Services Network
Primary DNS Servers

分析攻击



- 使用互联网和供应商提供的工具来分析攻击的详细信息。
- 这将提供有关下一步可以做什么或不能做什么的信息。

SITREP – 正在进行的攻击

- 附带损害减轻
- 被攻击的客户拥有部分服务。
- DOS攻击仍然有效
- 操作：向受害者（受害者）提供清洁管道全面服务回收（具体取决于供应商的详细信息）。

什么是全面服务恢复

- “清洁管道”是一个用于描述全面服务恢复的术语。全面服务恢复的期望是：
  - DDOS攻击已全面启动，所有客户服务均正常运行-达到合同规定的SLA。
  - 用于全面服务恢复的设备不容易受到DDOS攻击，基础设施也不易受到附带损害。
- 全方位服务恢复/清洁管道产品非常专业。与适当的供应商联系。

完整与部分服务恢复

- 部分服务恢复非常容易……将攻击推回ASN边缘。
- 全面服务恢复需要围绕关键服务进行有重点的计划。

暂停提问

接下来是什么？

- 下载白皮书，博客，研讨会资料，网址为：www.senki.org

- 连接！Barry通过Linkedin与同事，同事和有抱负的人才建立联系（也可以在Twitter上关注Barry（@BarryRGreene），或在Se nki上关注博客（www.senki.org）。www.linkedin.com/in/ba rryrgreene/).