双向安全管理框架（又称为分布式拒绝服务对等）

CenturyLink & AT&T

Nimrod Levy, Don Smith, John Schiel

nl7942@att.com, donald.smith@Centurylink.com , John.Schiel@Centurylink.com

LEXICON

ISP间流量规格

- 分布式拒绝服务对等方发起的Flowspec公告，用于丢弃针对受害者IP的攻击流量

不需要的流量

- 一个互联网服务提供商为另一互联网服务提供商

分布式拒绝服务对等互连过滤的流量

- 互联网服务提供商（ISP）正在为另一个对等节点丢弃

“不必要的流量”

- 免结算对等

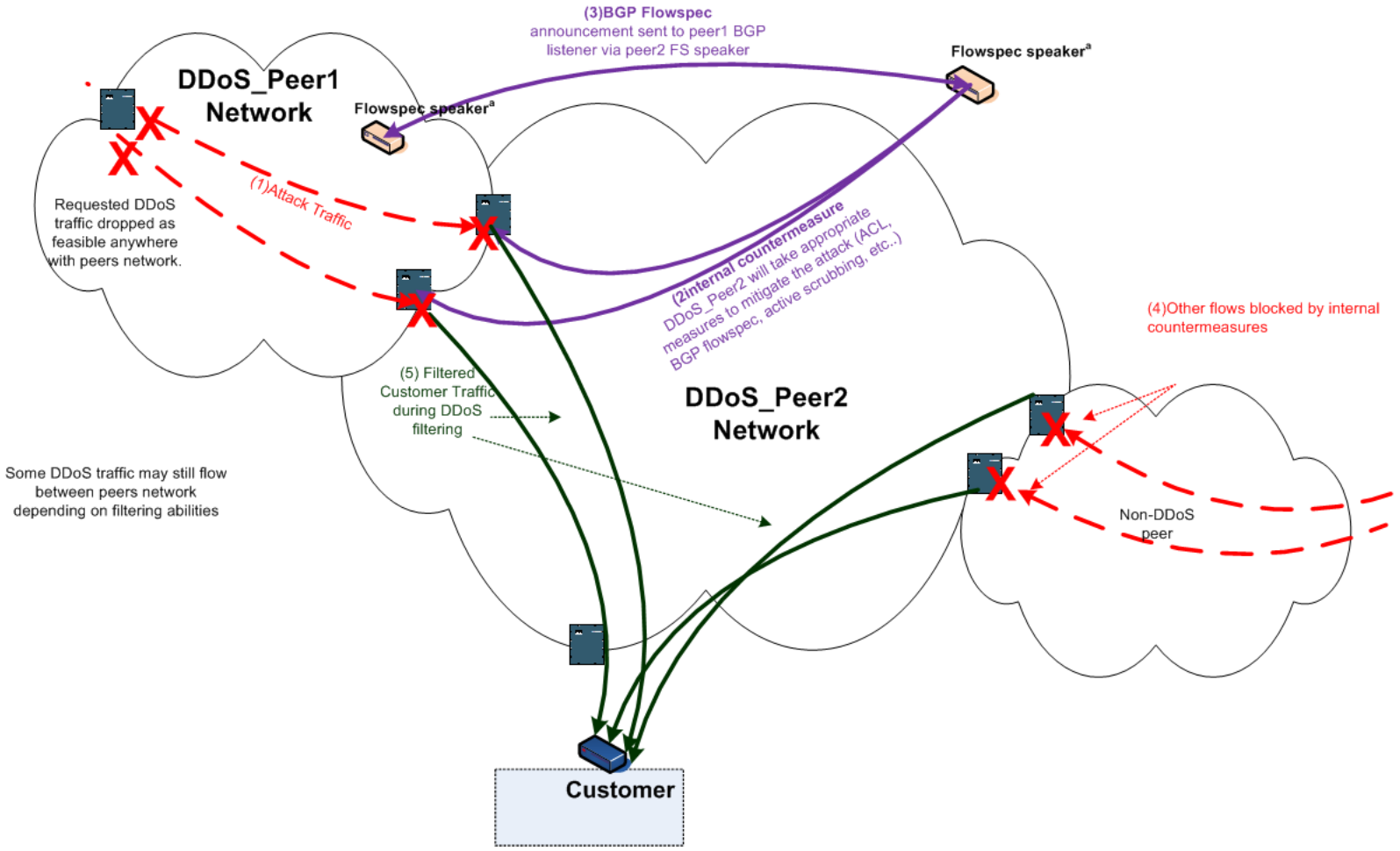
背景，假设和背景

- 提供对等网络交换过滤请求的过程
- 在对等网络之间
- 互惠互利的关系/环境
- 机构而非个人->始终如一的方法

发起超越同行的原因

- 对请求网络的客户/受害者或基础设施的重大影响
- 对通知网络的重大好处
- 传达网络卫生建议
- 漏洞管理
- 前提条件：请求网络已在其自身网络上实施了合理的缓解措施

分布式拒绝服务对等图


(3)BGP Flowspec
announcement sent to peer1 BGP
listener via peer2 FS speaker
Flowspec speaker[a]
Flowspec speaker[a]
DDoS_Peer1
Network
Requested DDoS
traffic dropped as
feasible anywhere
with peers network.
(1)Attack Traffic
(2)Internal countermeasure
DDoS_Peer2 will take appropriate
measures to mitigate the attack (ACL,
BGP flowspec, active scrubbing, etc..)
(4)Other flows blocked by internal
countermeasures
(5) Filtered
Customer Traffic
during DDoS
filtering
DDoS_Peer2
Network
Some DDoS traffic may still flow
between peers network
depending on filtering abilities
Non-DDoS
peer
Customer

要求：发起，认证，验证

- 必须具有AAA和CIA的基本概念。
- 不仅需要身份验证，授权和计费
  - 机密性
  - 正直诚信
  - 可用性
- 安全过滤请求的方法
  - BGP路由公告/ ISP间Flowspec
  - 使用预先建立的联系点致电
  - EMAIL到NOC / SOC通用别名
  - 票务系统

支持的类型/动作（对等）

- “标准5元组” + ICMP
- 可用的TYPES
  - 1: Dest Prefix　　2: Src Prefix　　3: IP Protocol
  - 4: Port Type　　5: Dest port　　6: Src port
  - 7: ICMP type　　8: ICMP code　　9: TCP flags
  - 10: Packet LEN　　11: DSCP　　12: Fragment
- 初始类型1、3、5、6、7、8
- 允许操作->删除
- 辩解？

路由广告规则

- 最大前缀N，对N的百分比发出警报，在N + 1时断开
- 与冗余公告保持一致
- 持续时间不确定-> max-prefix退出然后添加
- 初始操作丢弃数据包
- 将BGPv4用于IPv4和IPv6流路由
- NO_EXPORT，限制长度/ 25…/ 32
- 为此目的建立一致的社区

通知网络的响应

- 在同级之间的任何合理时间实施阻止。
- 考虑实施网络卫生实践
- 致谢
  - 我们收到了您的请求
  - 我们做了某事/某处
  - 反馈回路

其他注意事项

- 请求对等方撤回/取消的请求
- 仅限重大事件
- 对等方没有义务，可以随时自行决定终止操作
- 两个网络都必须评估附带影响
- 与同行进行双边实施

试点/概念证明的好处

- 扩展ISP抵御大型分布式拒绝服务攻击的能力
- 分布式拒绝服务响应更加有效：
  - 机构而非个人关系
  - 预先建立/认证的信任关系
  - 预协商和预定义流程
  - 书面请求，特定数据元素
- 不承载不必要的流量的其他好处

问题/担忧

- 法律/公共政策/法规
- 保密问题
- 报告

参考材料

- BCP 38 http://www.bcp38.info/index.php/Main_Page
- BCP 84 https://tools.ietf.org/html/bcp84
- UTRS http://www.team-cymru.org/UTRS/index.html
- DBHF community https://tools.ietf.org/html/rfc7999
- Flowspec
  - https://tools.ietf.org/html/rfc5575
  - https://www.nanog.org/sites/default/files/tuesday_general_ddos_ryburn_63.16.pdf