

IPsec

IPsec - ^_ = / D W

† #Y\$ x 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 |

† 6 † 13567 8

† " B->G7V

† DZ =

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