

分布式拒绝服务缓解

使用BGP Flowspec

贾斯汀·赖本
高级系统工程师

背景资料

- 这是谁？
 - <http://www.linkedin.com/in/justinryburn>
- 为什么选择这个主题？
 - 体验跟踪“分布式拒绝服务”。

分布式拒绝服务真的有问题吗？

“...拆除站点或阻止交易只是冰山一角。分布式拒绝服务攻击可能会导致声誉受损或对未交付服务的法律索赔。”

卡巴斯基实验室[1]

威瑞信[2]

“10 Gbps和
上类商品增长38%
从第二季度到第三季度。”

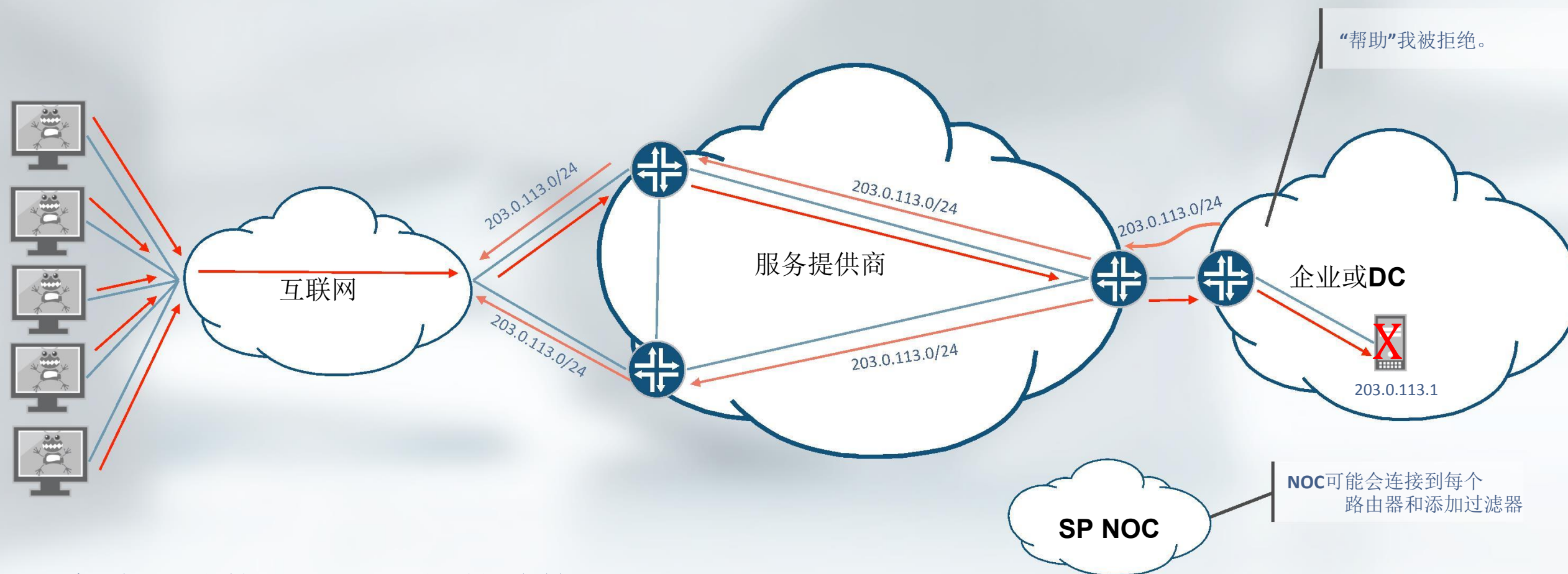
全国广播公司新闻[3]

“...超过40%
估计分布式拒绝服务损失甚至更高
每天超过一百万美元。”

科技时报[4]

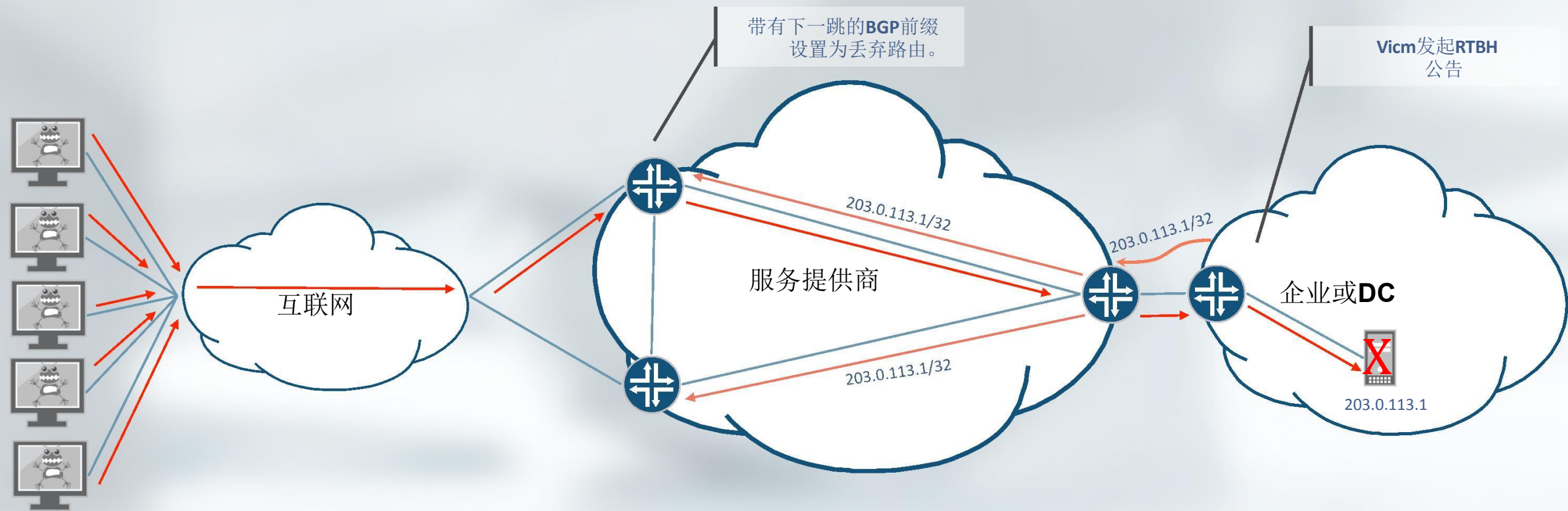
“分布式拒绝服务攻击严重削弱了索尼
PSN，而Microsoft处理
Xbox Live困境”

在过去，阻止分布式拒绝服务



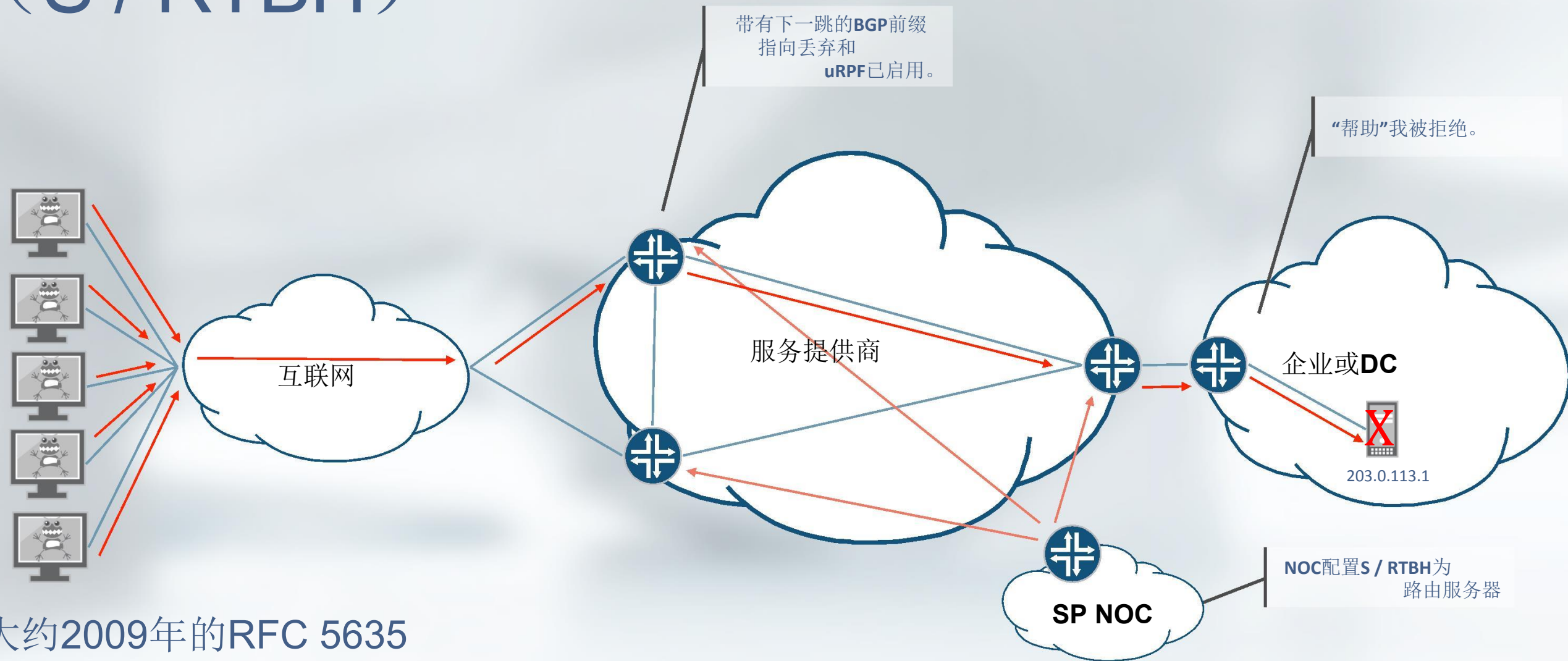
- 易于实施，并使用易于理解的结构
- 要求客户和提供商之间高度协调
- 规模大，可在大型网络外围扩展
- 配置错误可能是昂贵的

目的地远程触发黑洞 (D / RTBH)



- 大约在2004年的RFC 3882
- 要求在所有边缘路由器上预先配置丢弃路由
- 被攻击者的目的地地址完全无法到达，但攻击（和附带损坏）停止了。

源远程触发黑洞 (S / RTBH)



- 大约2009年的RFC 5635
- 要求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）信号源。

BGP流量规范

- 现在可以使用**BGP**分配有关流的特定信息
大约在**RFC 5575 [5]**中定义的**NLRI**（2009年）
 - AFI / SAFI = 1/133**: 单播流量过滤应用
 - AFI / SAFI = 1/134**: VPN流量过滤应用程序
- 流路由自动针对单播路由进行验证
信息或通过路由策略框架。
 - 必须属于最长匹配单播前缀。
- 验证后，将根据匹配和操作创建防火墙过滤器
标准。

BGP流量规范

- BGP Flowspec可以包含以下信息：

- 类型1-目的地前缀
- 类型2-源前缀
- 类型3-IP协议
- 类型4 –源或目标端口
- 类型5 –目标端口
- 类型6-源端口
- 类型7 – ICMP类型
- 类型8 – ICMP代码
- 类型9-TCP标志
- 类型10-数据包长度
- 类型11 – DSCP
- 类型12-片段编码

BGP流量规范

- 使用BGP扩展社区定义操作：
 - 0x8006 –流量速率（设置为0以丢弃所有流量）
 - 0x8007 –流量动作（采样）
 - 0x8008 –重定向到VRF（路由目标）
 - 0x8009 –流量标记（DSCP值）

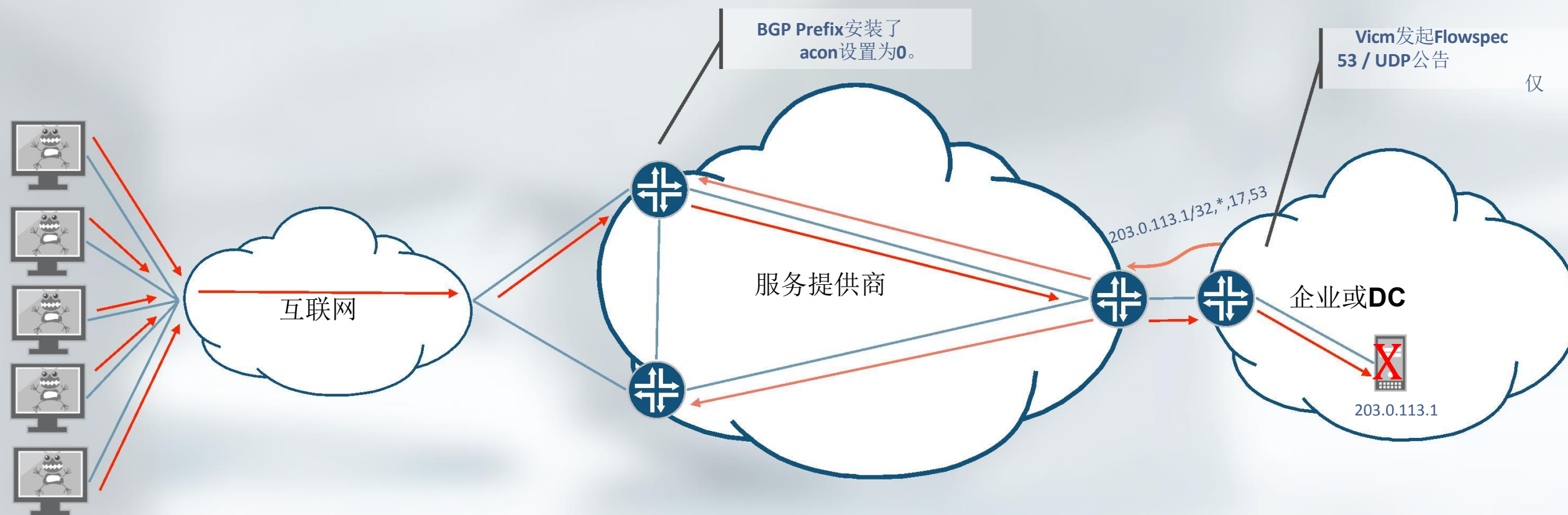
供应商支持

- 分布式拒绝服务检测供应商：
 - Arbor Peakflow SP 3.5
 - 瞻博网络分布式拒绝服务安全5.14.2-0
- 路由器供应商：
 - 阿尔卡特朗讯SR OS 9.0R1
 - 瞻博网络JUNOS 7.3
 - 思科5.2.0用于ASR和CRS [6]

是什么使BGP Flowspec更好？

- 与访问控制列表相同的粒度
 - 基于n元组匹配
- 与RTBH自动化
 - 将过滤器传播到大型网络中的所有边缘路由器更容易
- 利用BGP最佳实践和策略控制
 - 可以将与RTBH相同的过滤和最佳实践应用于BGP Flowspec

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。
- 需要在客户端边缘进行理性过滤。

边缘路由器配置

Alcatel-Lucent

```
router
  autonomous-system 64496
  bgp
    group "CUST-FLOWSPEC"
      neighbor 192.0.2.1
        family ipv4 flow-ipv4
        peer-as 64511
        no flowspec-validate
      exit
    exit
  no shutdown
exit
Exit
```

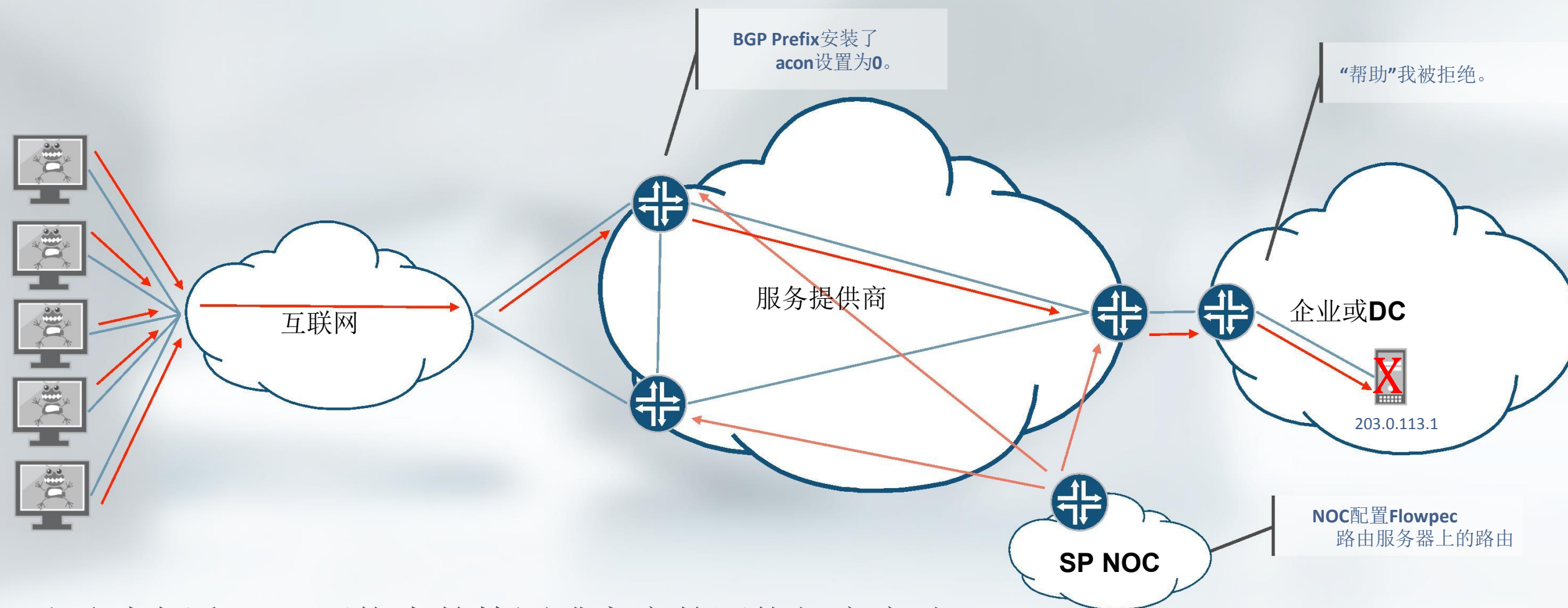
Cisco [7]

```
router bgp 64496
  ! Initializes the global address family
  address-family ipv4 flowspec
  !
  neighbor 192.0.2.1
    remote-as 64511
    ! Ties it to a neighbor configuration
  address-family ipv4 flowspec
```

Juniper

```
protocols {
  bgp {
    group CUST-FLOWSPEC {
      peer-as 64511;
      neighbor 192.0.2.1 {
        family inet {
          flow;
        }
      }
    }
  }
  routing-options {
    flow {
      term-order standard;
    }
  }
}
```


使用Flowspec进行域内分布式拒绝服务缓解



- 可以通过电话，SP网络中的检测或客户的网络门户启动。
- 要求客户和提供商之间进行协调。

边缘路由器配置

Alcatel-Lucent

```
router
  autonomous-system 64496
  bgp
    group "RR-CLIENT-FLOWSPEC"
      neighbor 198.51.100.1
        family ipv4 flow-ipv4
        peer-as 64496
      exit
    exit
  no shutdown
exit
exit
```

Cisco [7]

```
router bgp 64496
  ! Initializes the global address family
  address-family ipv4 flowspec
  !
  neighbor 198.51.100.1
    remote-as 64496
    ! Ties it to a neighbor configuration
  address-family ipv4 flowspec
```

Juniper

```
protocols {
  bgp {
    group RR-CLIENT-FLOWSPEC {
      type internal;
      neighbor 198.51.100.1 {
        family inet {
          flow;
        }
      }
    }
  }
  routing-options {
    flow {
      term-order standard;
    }
  }
}
```

路由服务器配置

Alcatel-Lucent	Cisco [7]	Juniper
<pre>router autonomous-system 64496 bgp group "RR-CLIENT-FLOWSPEC" neighbor 198.51.100.2 family ipv4 flow-ipv4 peer-as 64496 exit exit no shutdown exit exit</pre>	<pre>router bgp 64496 ! Initializes the global address family address-family ipv4 flowspec ! neighbor 198.51.100.2 remote-as 64496 ! Ties it to a neighbor configuration address-family ipv4 flowspec</pre>	<pre>protocols { bgp { group RR-CLIENT-FLOWSPEC { type internal; neighbor 198.51.100.2 { family inet { flow; } export FLOWROUTES_OUT; } } } }</pre>

路由服务器配置

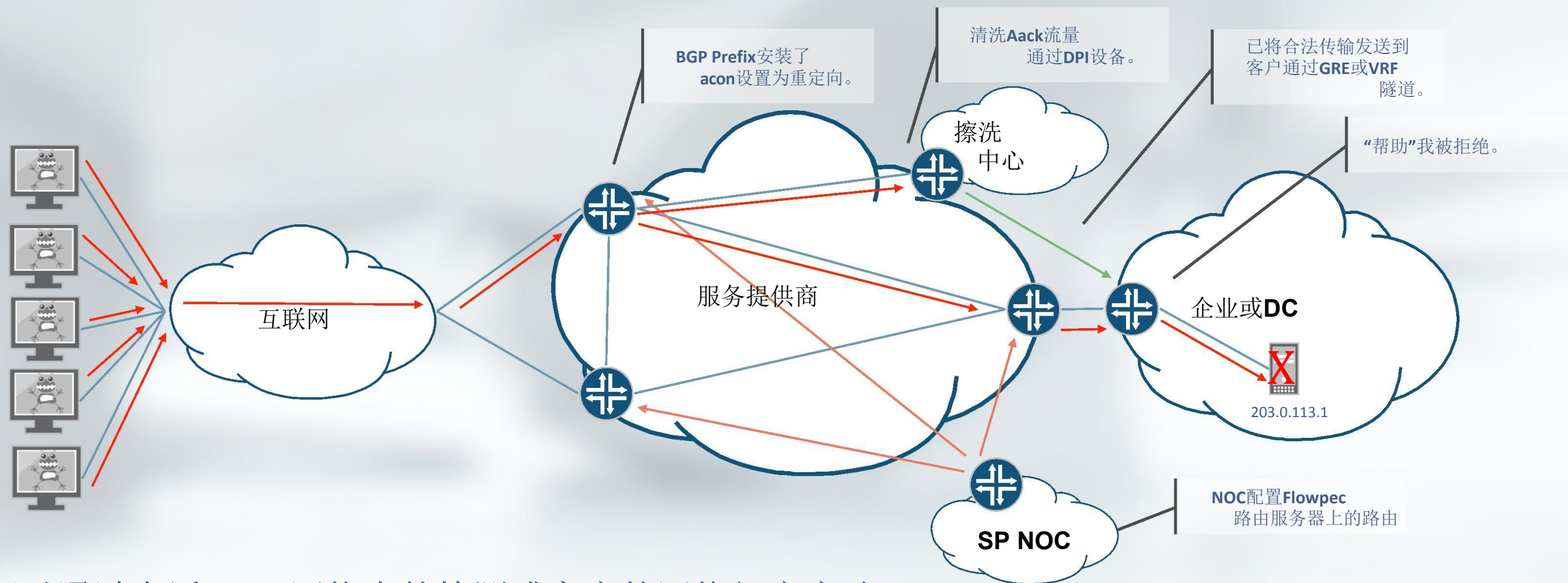
Cisco [7]

```
class-map type traffic match-all attack_fs
  match destination-address ipv4 203.0.113.1/32
  match protocol 17
  match destination-port 53
end-class-map
!
policy-map type pbr attack_pbr
  class type traffic attack_fs
    drop
  class class-default
end-policy-map
!
flowspec
  address-family ipv4
    service-policy type pbr attack_pbr
exit
```

Juniper

```
routing-options {
  flow {
    term-order standard;
    route attack_fs {
      match {
        destination 203.0.113.1/32
        protocol udp;
        destination-port 53;
      }
      then discard;
    }
  }
}
policy-options {
  policy-statement FLOWROUTES_OUT {
    from {
      rib inetflow.0;
    }
    then accept;
  }
}
```

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。

边缘路由器配置

Alcatel-Lucent

```
router
  autonomous-system 64496
  bgp
    group "RR-CLIENT-FLOWSPEC"
      neighbor 198.51.100.1
        family ipv4 flow-ipv4
        peer-as 64496
      exit
    exit
  no shutdown
exit
exit
```

Cisco [7]

```
router bgp 64496
  ! Initializes the global address family
  address-family ipv4 flowspec
  !
  neighbor 198.51.100.1
    remote-as 64496
    ! Ties it to a neighbor configuration
  address-family ipv4 flowspec
```

Juniper

```
protocols {
  bgp {
    group RR-CLIENT-FLOWSPEC {
      type internal;
      neighbor 198.51.100.1 {
        family inet {
          flow;
        }
      }
    }
  }
}
routing-options {
  flow {
    term-order standard;
  }
}
```

路由服务器配置

Alcatel-Lucent	Cisco [7]	Juniper
<pre>router autonomous-system 64496 bgp group "RR-CLIENT-FLOWSPEC" neighbor 198.51.100.2 family ipv4 flow-ipv4 peer-as 64496 exit exit no shutdown exit exit</pre>	<pre>router bgp 64496 ! Initializes the global address family address-family ipv4 flowspec ! neighbor 198.51.100.2 remote-as 64496 ! Ties it to a neighbor configuration address-family ipv4 flowspec</pre>	<pre>protocols { bgp { group RR-CLIENT-FLOWSPEC { type internal; neighbor 198.51.100.2 { family inet { flow; } export FLOWROUTES_OUT; } } } }</pre>

路由服务器配置

Cisco [7]

```
class-map type traffic match-all attack_fs
  match destination-address ipv4 203.0.113.1/32
  match protocol 17
  match destination-port 53
end-class-map
!
policy-map type pbr attack_pbr
  class type traffic attack_fs
    redirect nexthop 192.0.2.7
  class class-default
end-policy-map
!
flowspec
  address-family ipv4
    service-policy type pbr attack_pbr
exit
```

Juniper

```
routing-options {
  flow {
    term-order standard;
    route attack_fs {
      match {
        destination 203.0.113.1/32
        protocol udp;
        destination-port 53;
      }
      then discard;
    }
  }
}
policy-options {
  policy-statement FLOWROUTES_OUT {
    from {
      rib inetflow.0;
    }
    then {
      next-hop 192.0.2.7;
      accept;
    }
  }
}
```

我怎么知道它正在工作？

Alcatel-Lucent	Cisco [7]	Juniper
•显示路由器bgp路由flow-ipv4 •显示路由器bgp路由flow-ipv6 •显示过滤器ip fSpec-0 •显示过滤器ip fSpec-0关联 •显示过滤器ip fSpec-0计数器 •显示过滤器ip fSpec-0条目<条目号>	•显示流程flowspec_mgr的所有位置 •显示flowspec摘要 •显示flowspec vrf全部 •显示bgp ipv4 flowspec	•显示bgp邻居<neighbor> 匹配Inet流 •显示路由表inetflow.0扩展 •显示防火墙过滤器 __flowspec_default_inet__

我们要去哪里？

- IPv6支持

- <http://tools.ietf.org/html/draft-ietf-idr-flow-spec-v6-03>

- 放松验证

- <http://tools.ietf.org/html/draft-ietf-idr-bgp-flowspec-oid-00>

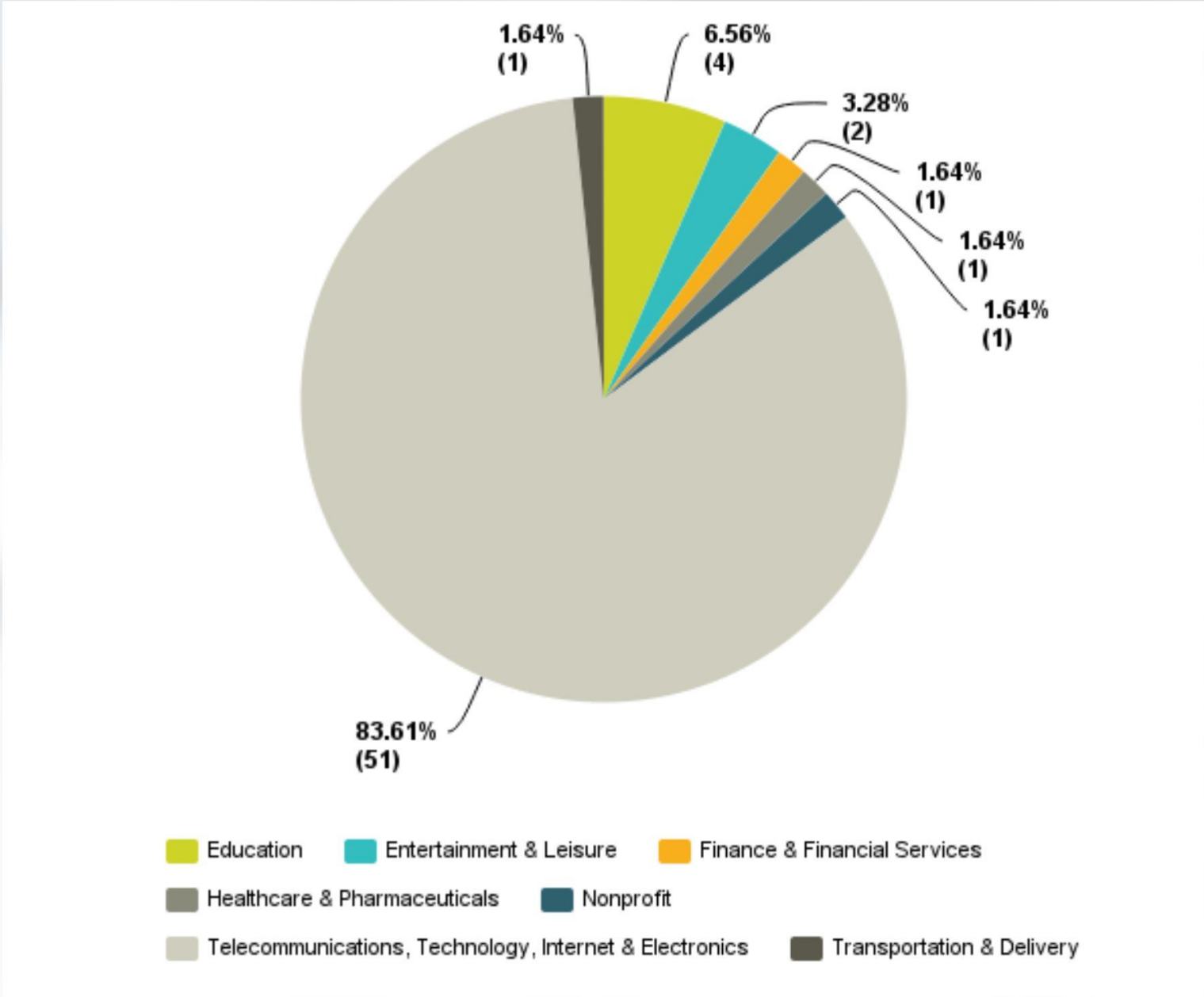
- 重定向到IP下一跳操作

- <http://tools.ietf.org/html/draft-simpson-idr-flowspec-redirect-02>

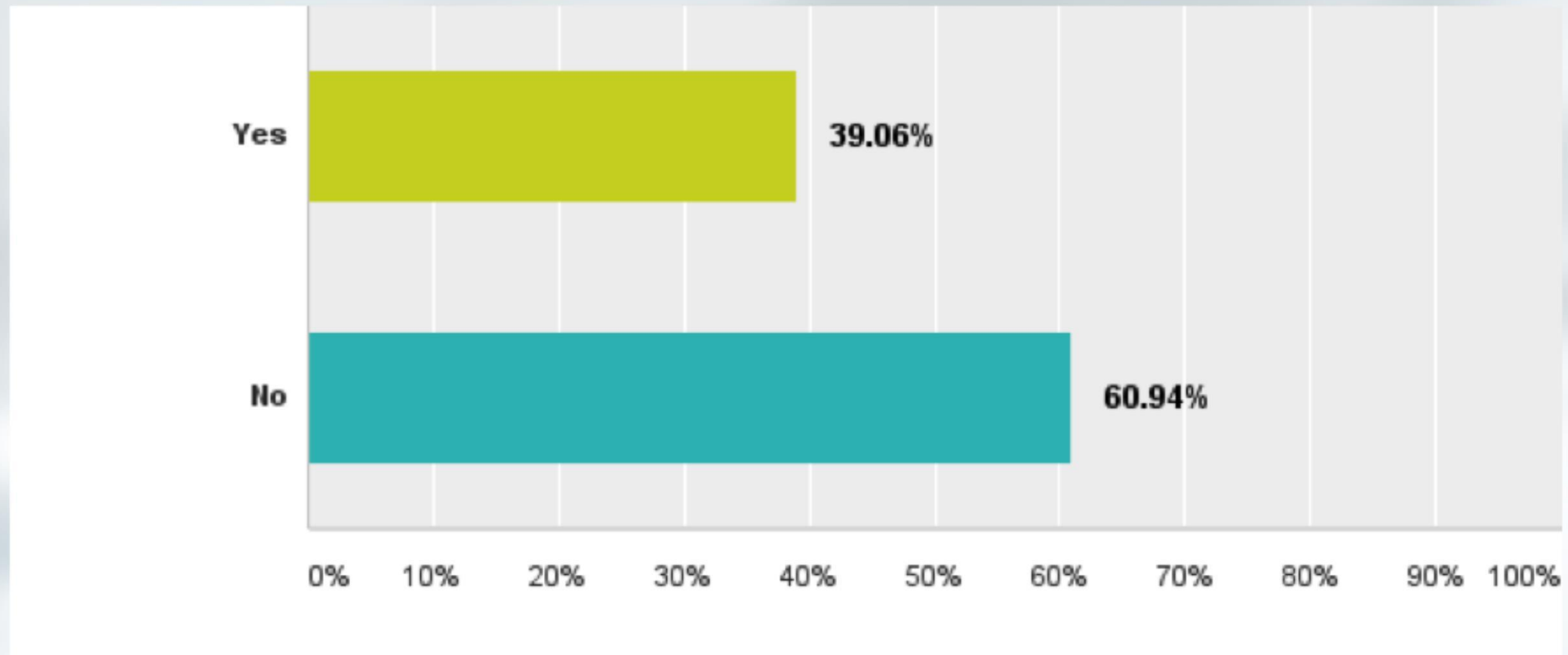


国情咨文

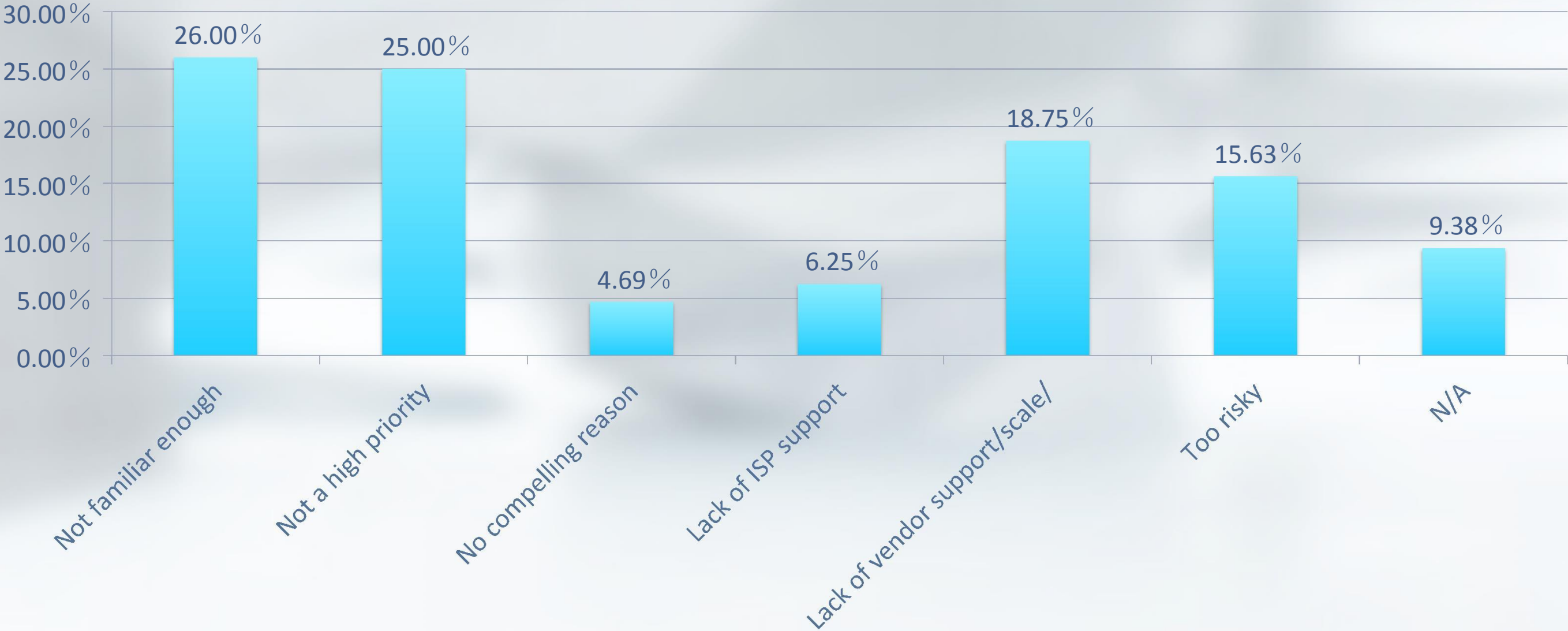
响应行业



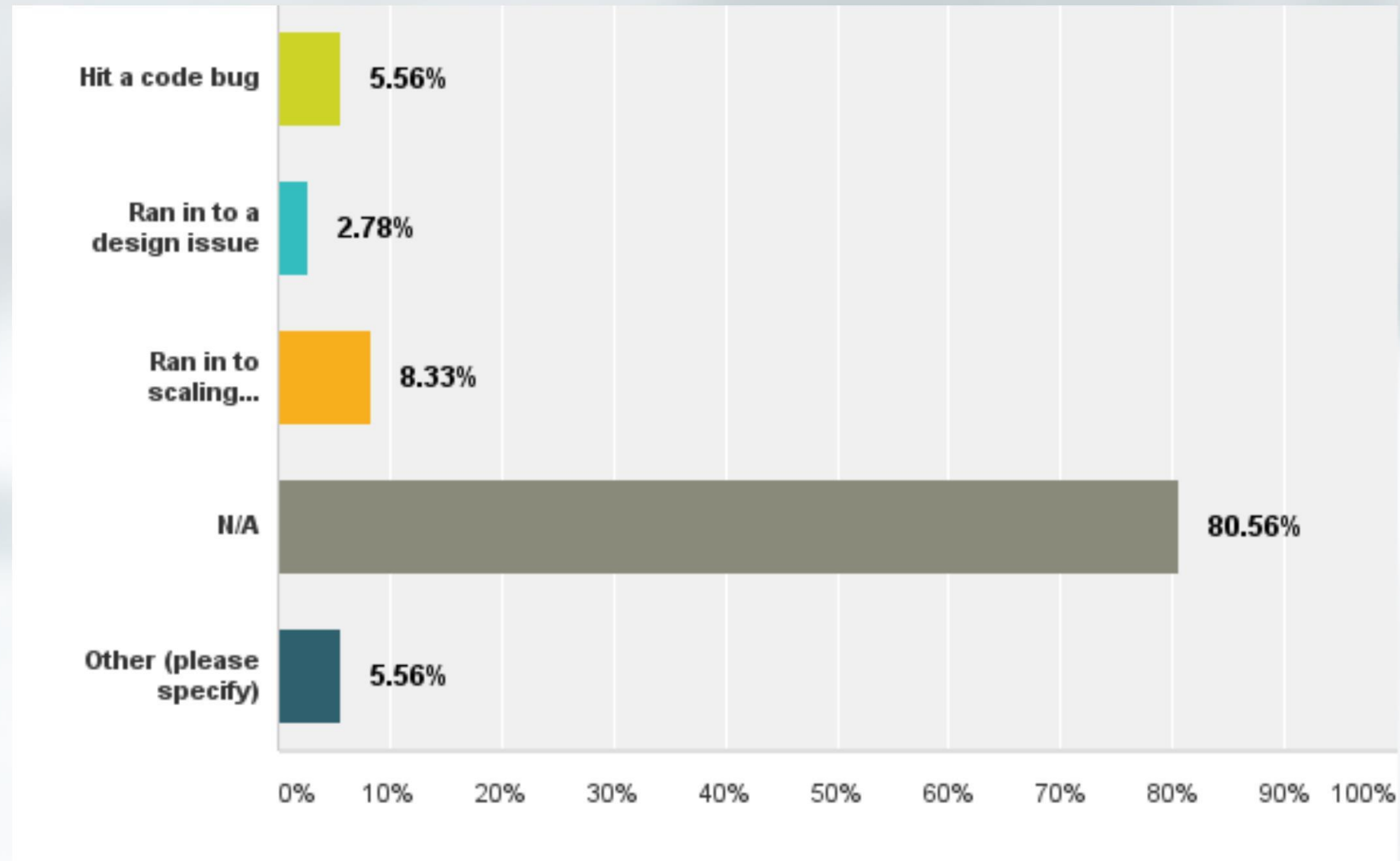
您是否有过BGP 在网络的任何部分启用Flowspec?



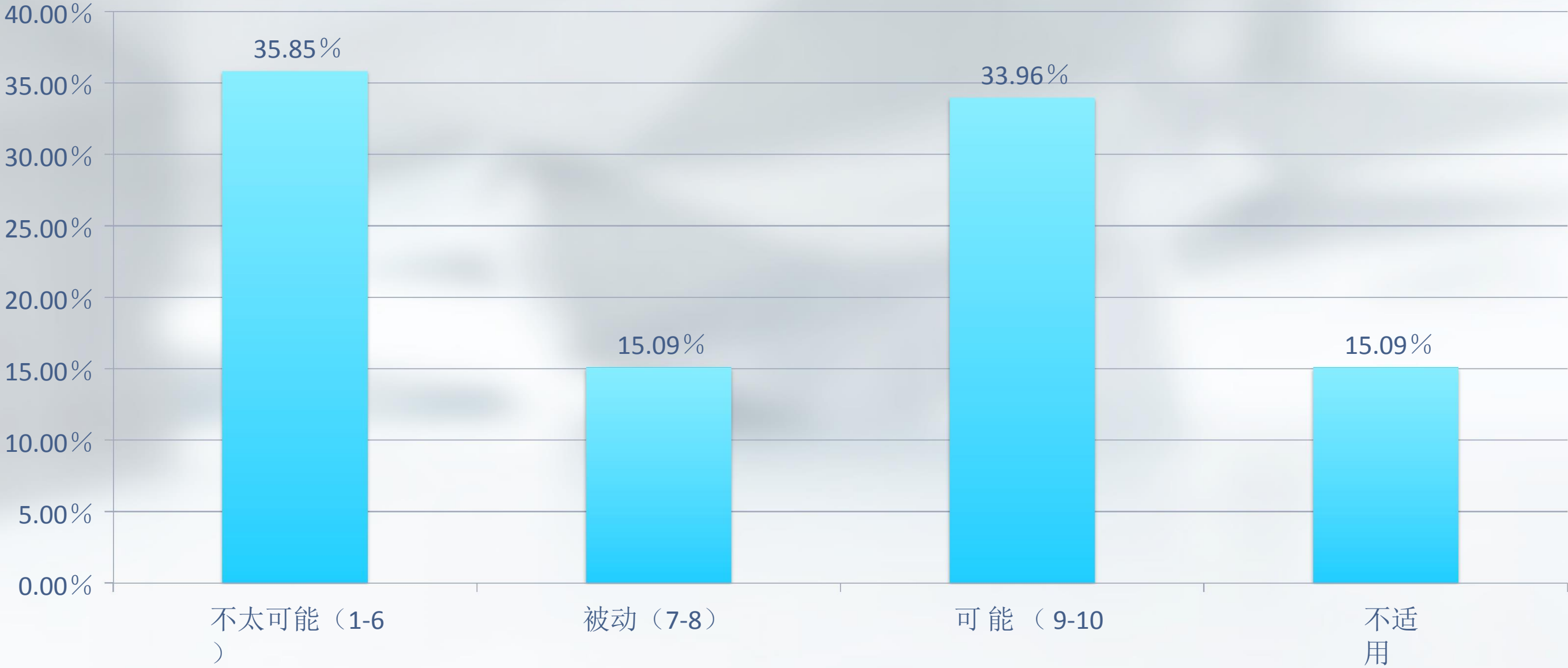
如果尚未启用，为什么不启用？



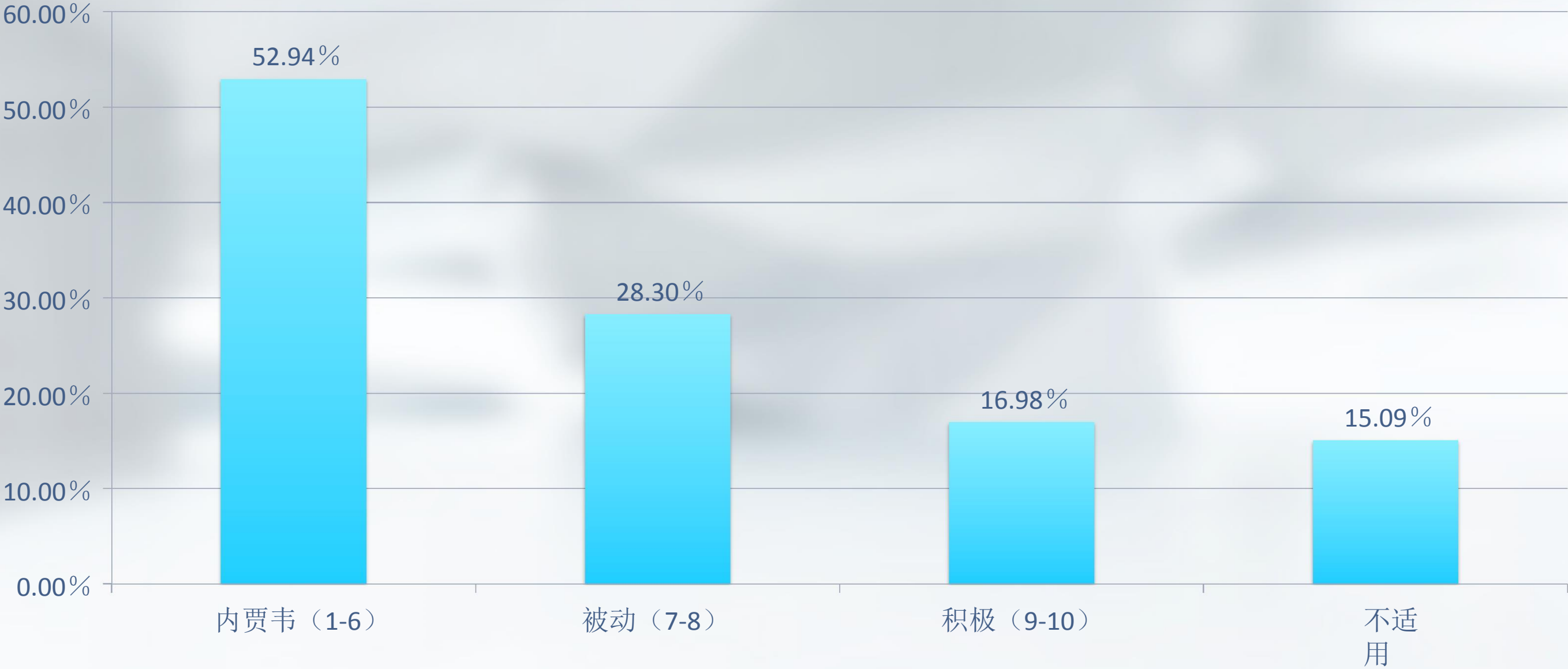
如果启用了此功能，但之后又禁用了它，为什么？



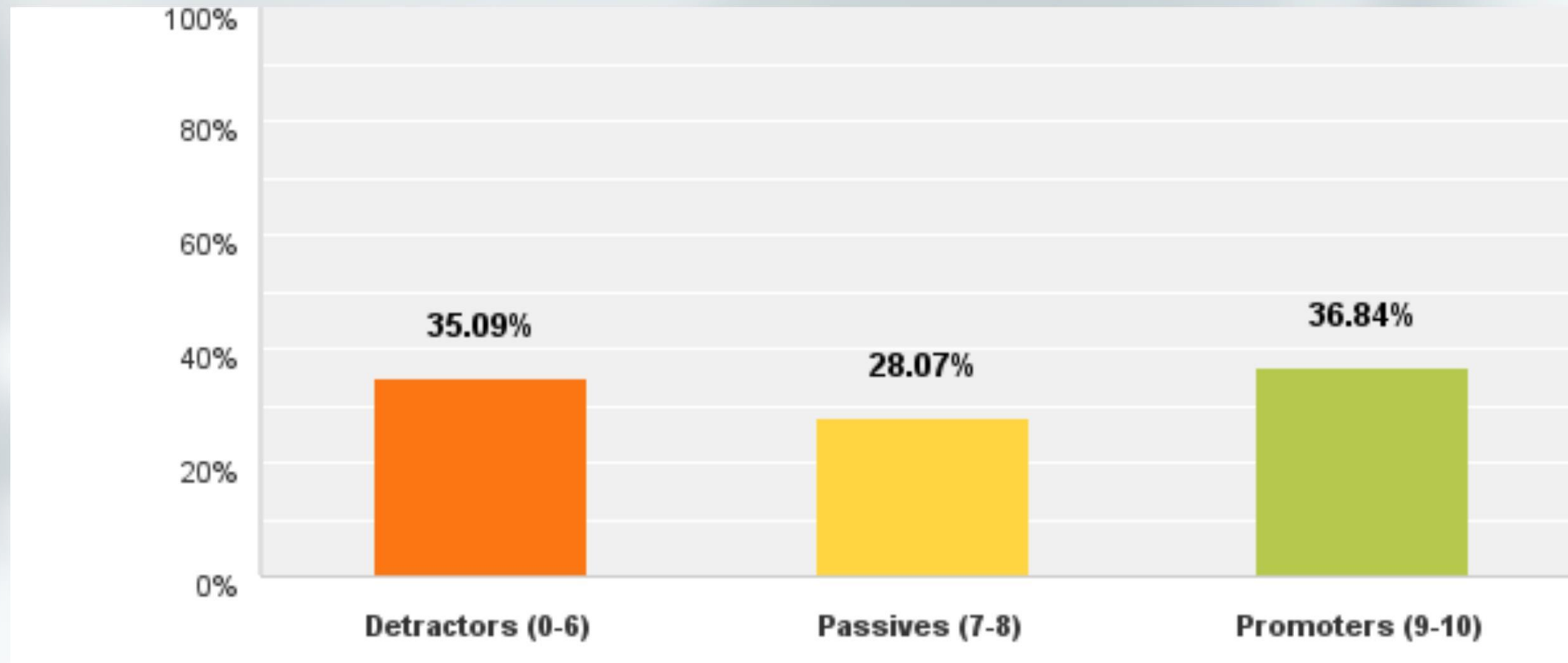
如果您当前未启用该功能，那么将来要启用BGP Flowspec吗？



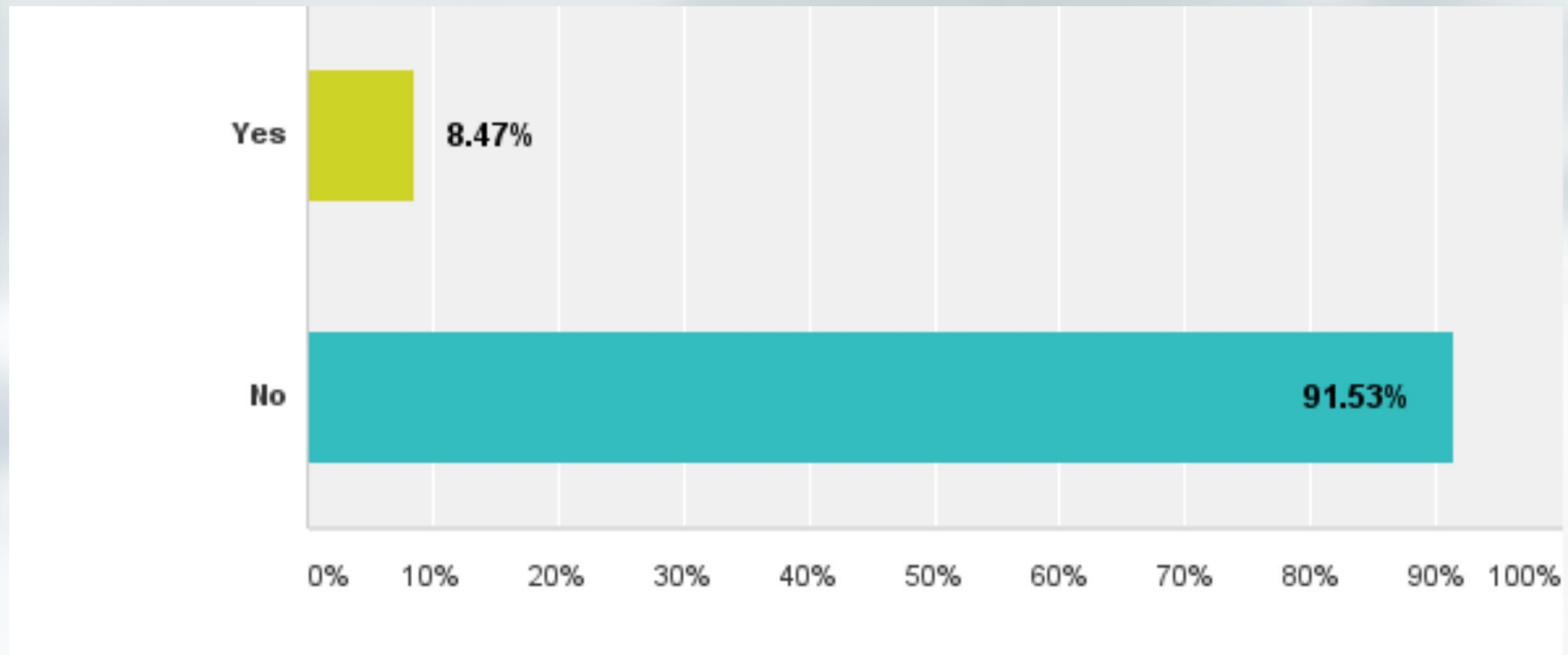
总体而言，您如何评价自己的体验 BGP Flowsec?



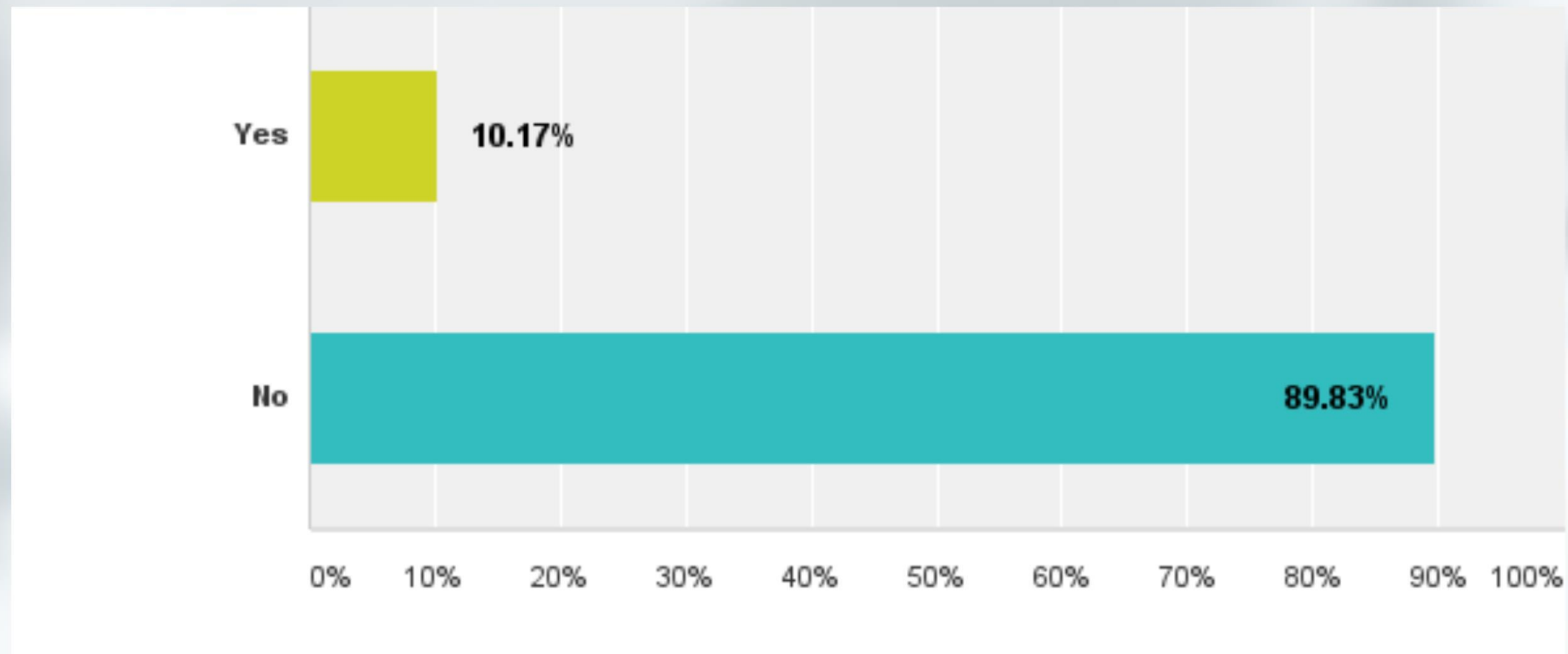
您推荐BGP的可能性有多大 Flowspec给朋友还是同事？



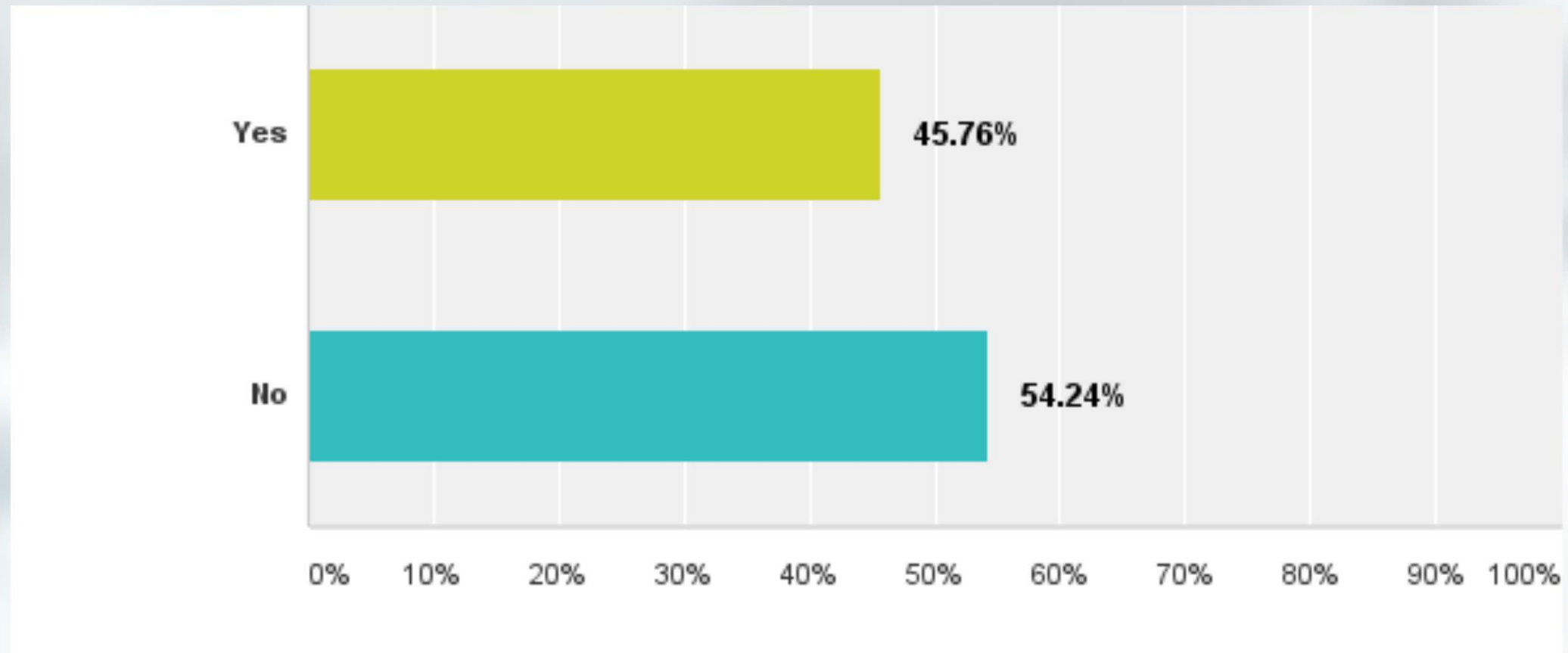
您是否允许客户向您发送BGP Flowspec通过BGP路由？



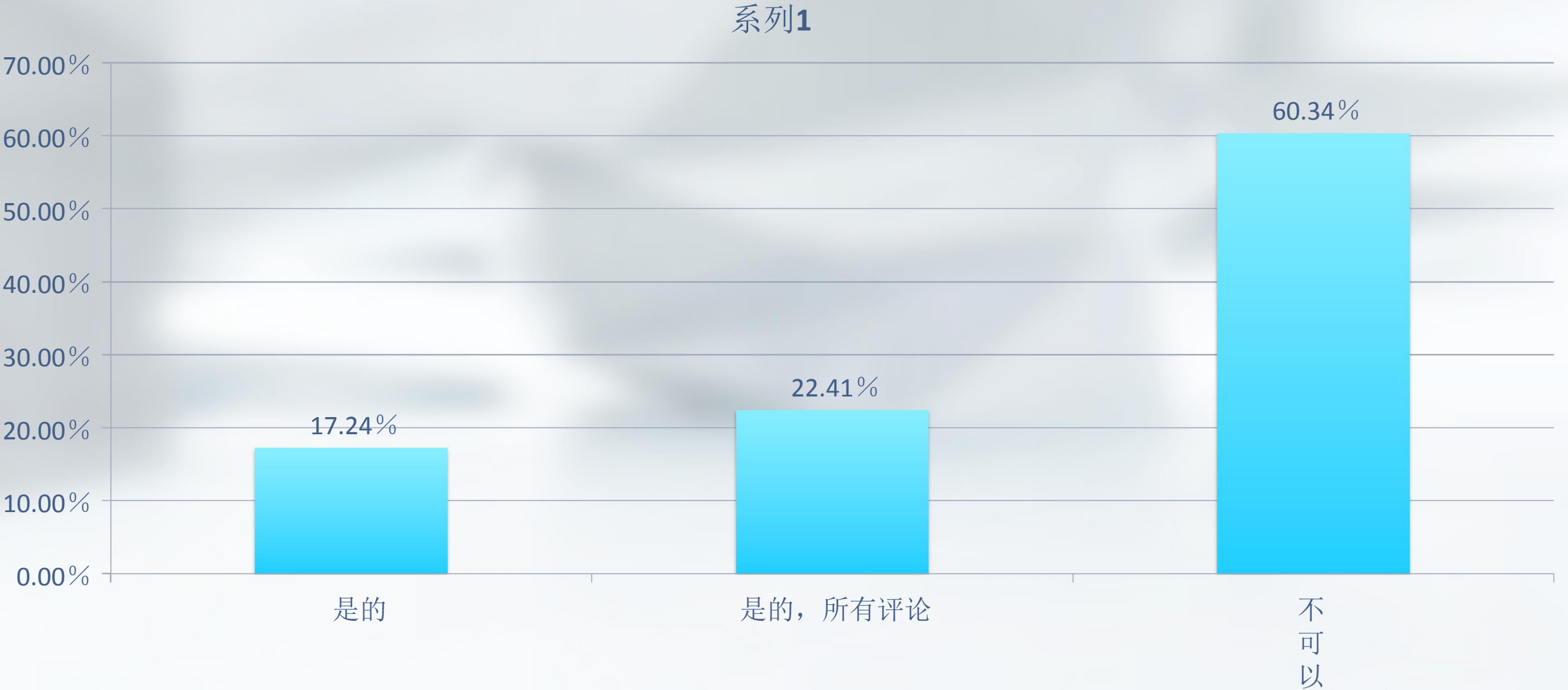
您是否有客户可以使用的网络门户 注入BGP Flowspec路由到您的IBGP？



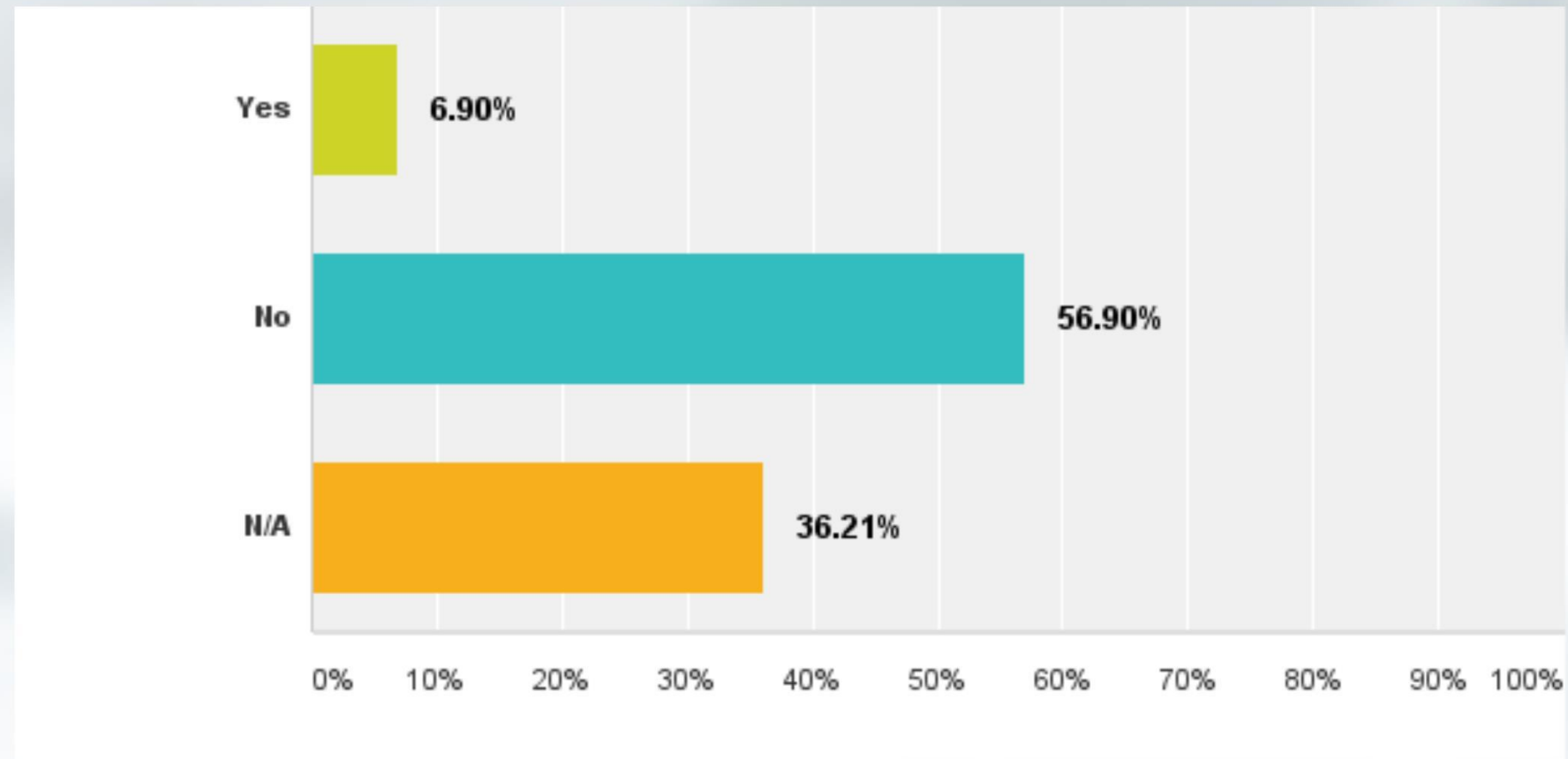
您有中央路由器吗？ 注入您的BGP Flowspec路由？



您是否允许分布式拒绝服务检测工具（如Arbor）发送BGP Flowspec路由到您的IBGP？



您是否对使用BGP的分布式拒绝服务缓解收费 Flowspec?



评论摘要

- 好主意，很乐意看到它起飞，但是...
- 企业和内容提供商正在等待互联网服务提供商接受其服务 **Flowspec** 路由。
 - 甚至有人愿意切换到执行此操作的ISP。
- 互联网服务提供商正在等待供应商支持它。
 - 更多供应商支持它
 - 他们的环境需要的特定功能
 - 更好的规模或稳定性

参考文献

- [1]卡巴斯基实验室–面向公众的公司每三分之一遇到分布式拒绝服务攻击<http://tinyurl.com/neu4zzr>
- [2] Verisign – 2014分布式拒绝服务攻击趋势<http://tinyurl.com/oujgx94>
- [3] NBC新闻–互联网速度急剧上升，但黑客攻击也在上升
<http://tinyurl.com/q4u2b7m>
- [4]科技时报–微软与DDoS攻击削弱了索尼PSN Xbox Live困境<http://tinyurl.com/kkdczjx>
- [5] RFC 5575-流程规范规则的传播
<http://www.ietf.org/rfc/rfc5575.txt>
- [6]思科-实施BGP Flowspec <http://tinyurl.com/mm5w7mo>
- [7]思科–了解BGP Flowspec <http://tinyurl.com/l4kwb3b>

谢谢你！
