分布式拒绝服务缓解

使用BGP Flowspec

Justin Ryburn
高级系统工程师

背景资料

- 这家伙是谁？
  - 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”。

Copyright © 2014 Juniper Networks, Inc.

分布式拒绝服务真的是一个问题吗？

“…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因未提供的服务而导致声誉损失或法律索赔。”

Kaspersky Lab [1]

Verisign [2]

“ 10 Gbps及以上类别的攻击自第二季度到第三季度增长了38%”

NBC News [3]

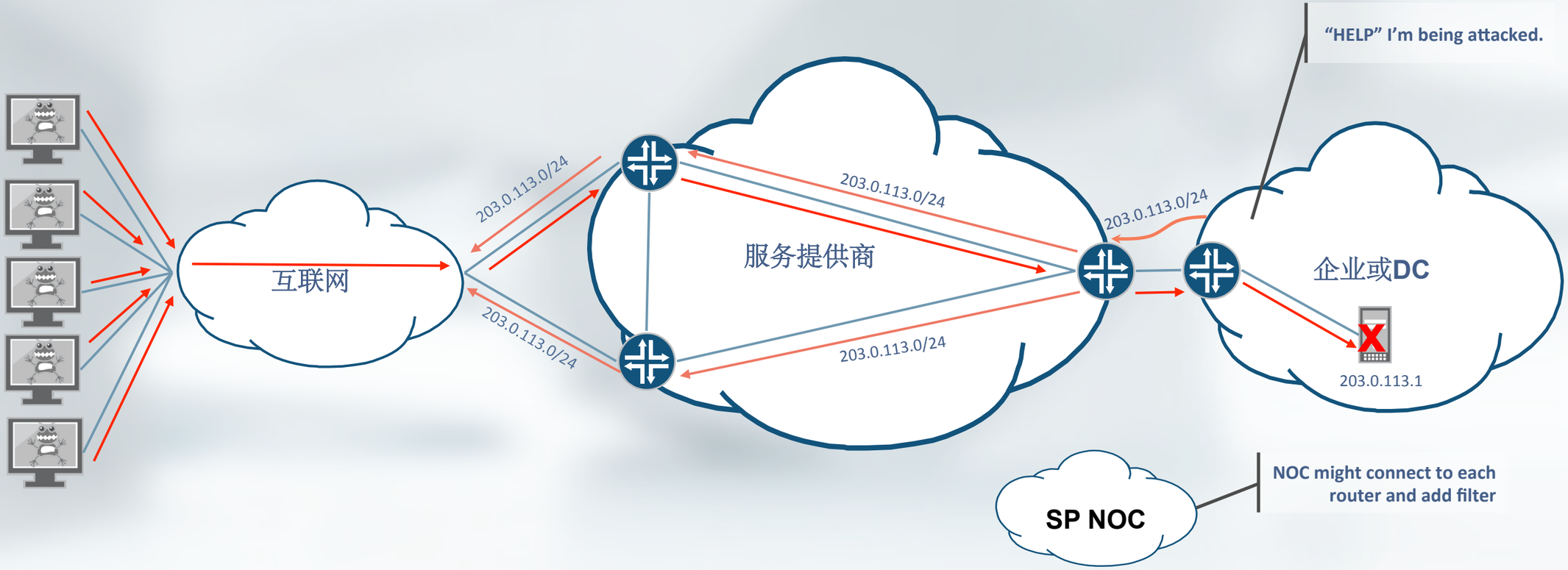
“……估计分布式拒绝服务每天损失超过100万美元，超过40％。”

Tech Times [4]

“当微软处理Xbox Live灾难时，分布式拒绝服务攻击使索尼PSN瘫痪”

Copyright © 2014 Juniper Networks, Inc.

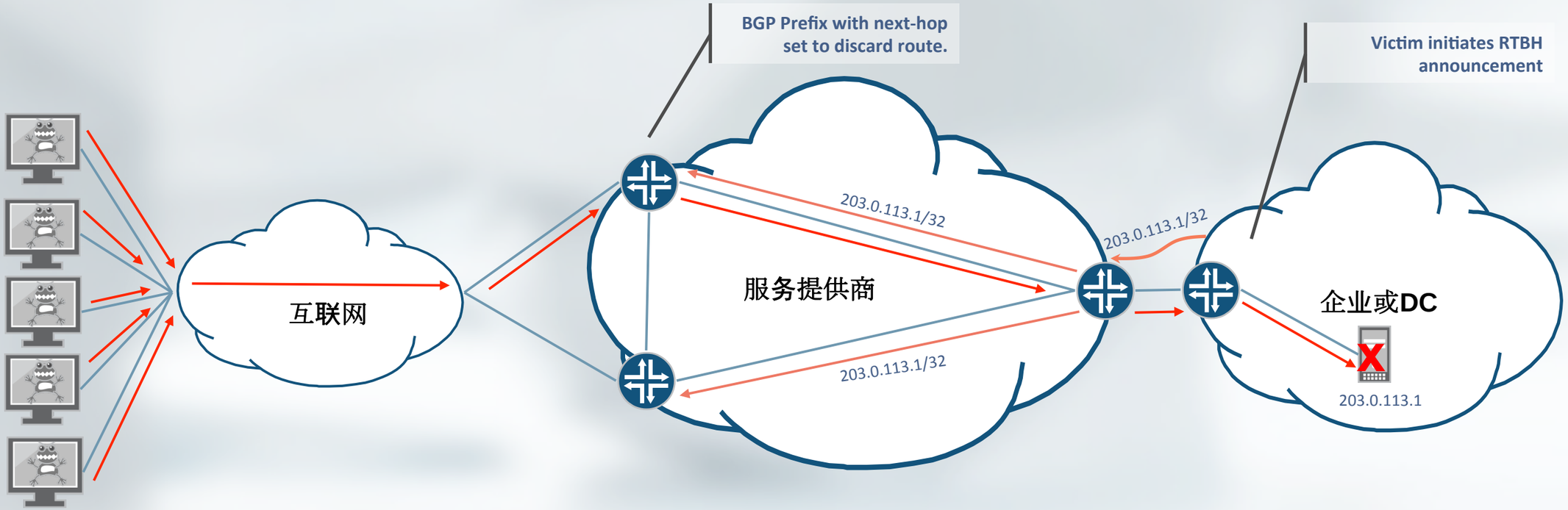
在过去，阻止分布式拒绝服务



- 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

Copyright © 2014 Juniper Networks, Inc.

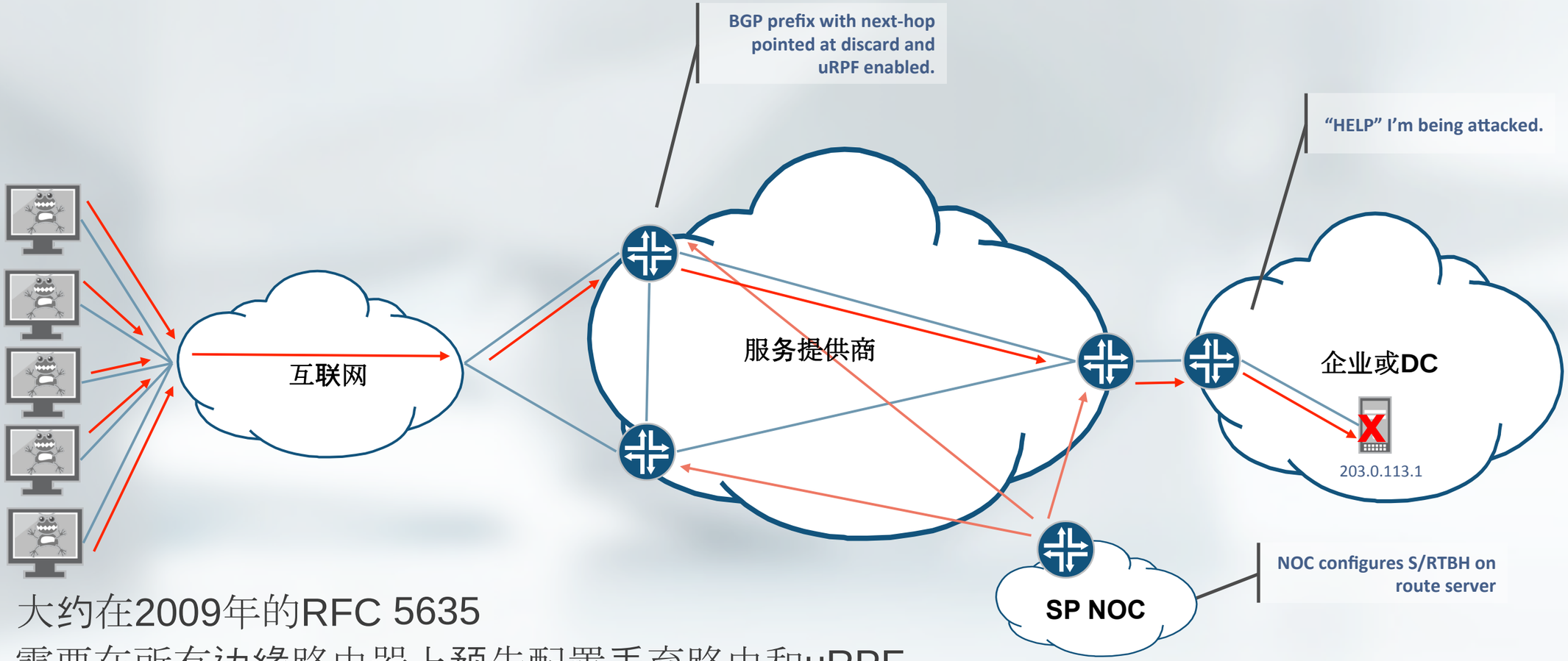
目标远程触发黑洞（D / RTBH）



- 大约在2004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。

Copyright © 2014 Juniper Networks, Inc.

信号源远程触发黑洞（S / RTBH）



- 大约在2009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。

Copyright © 2014 Juniper Networks, Inc.

BGP流量规范

- 现在可以使用RFC 5575 [5]大约于2009年定义的BGP NLRI分配有关流的特定信息
  - 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
- 根据单播路由信息或通过路由策略框架自动验证流路由。
  - 必须属于最长匹配单播前缀。
- 验证后，将根据匹配和操作标准创建防火墙过滤器。

Copyright © 2014 Juniper Networks, Inc.

BGP流量规范

- BGP Flowspec可以包含以下信息：
  - 类型1-目的前缀
  - 类型2-源前缀
  - 类型3-IP协议
  - 类型4 –源或目标端口
  - 类型5 –目的端口
  - 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

Copyright © 2014 Juniper Networks, Inc.

BGP流量规范

- 使用BGP扩展社区定义动作：
  - 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）

Copyright © 2014 Juniper Networks, Inc.

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JUNOS 7.3
  - 思科5.2.0 for ASR和CRS [6]

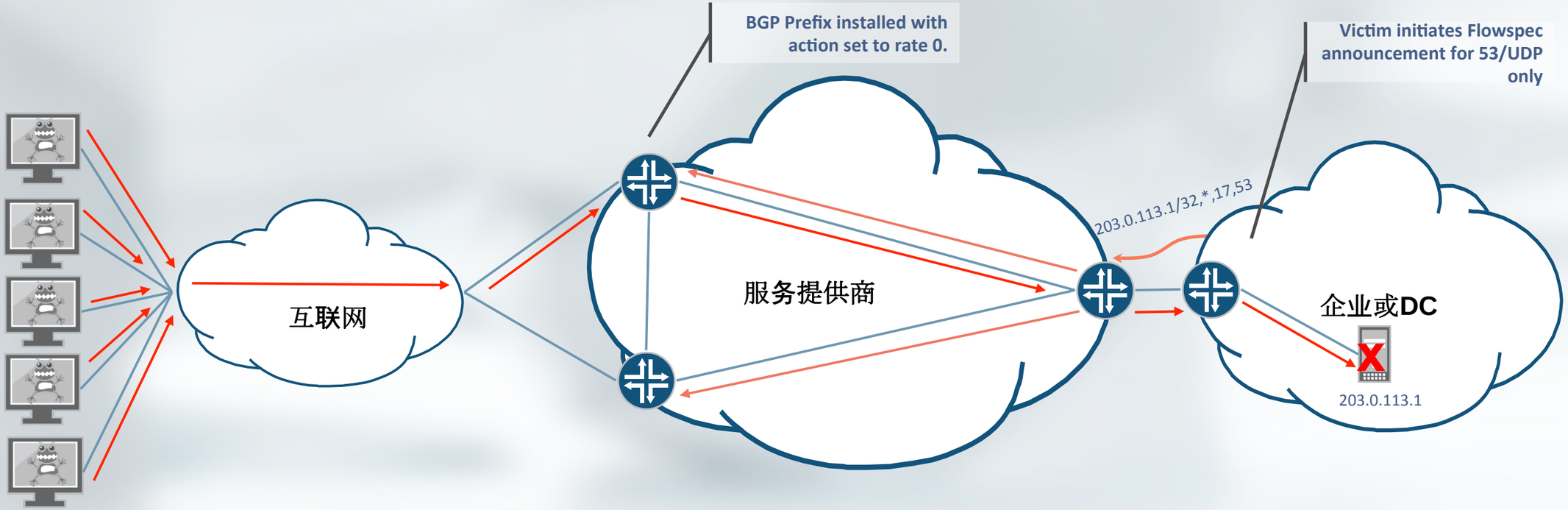
Copyright © 2014 Juniper Networks, Inc.

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自动化相同
  - 将过滤器传播到大型网络中的所有边缘路由器要容易得多
- 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

Copyright © 2014 Juniper Networks, Inc.

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。

Copyright © 2014 Juniper Networks, Inc.

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]

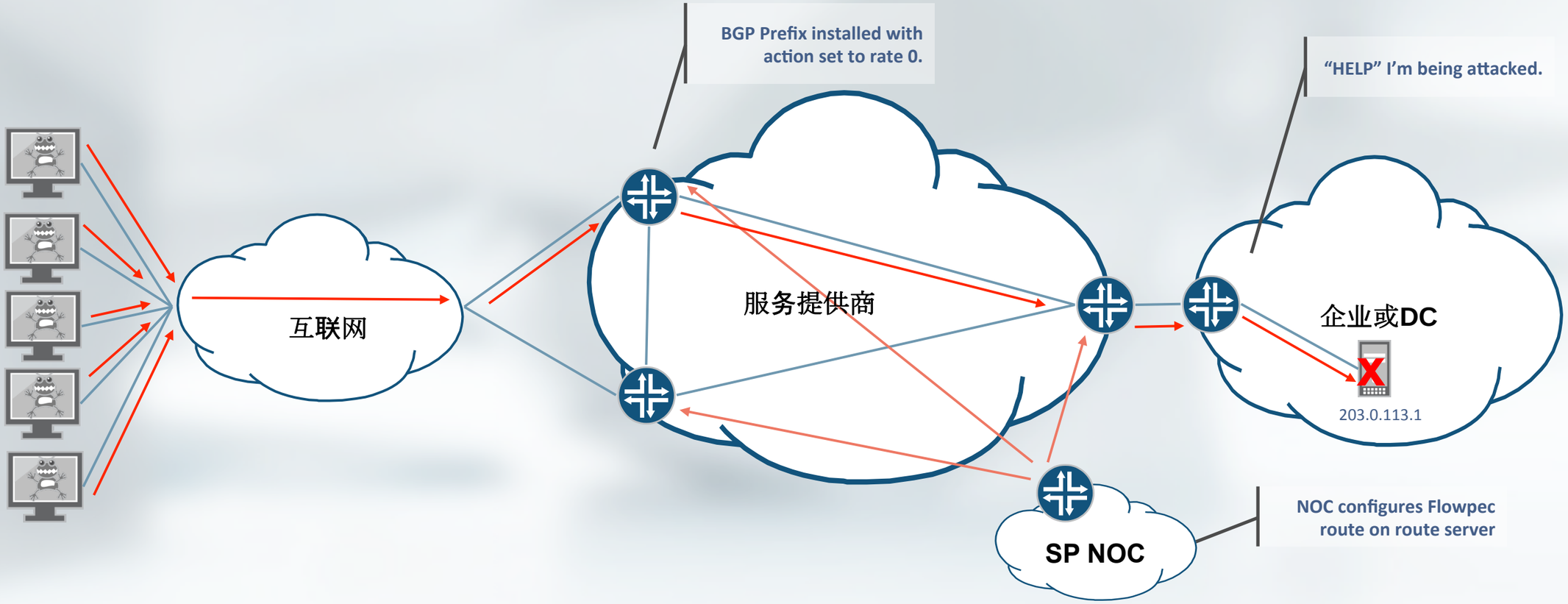
```
router bgp 64496
  ! Initializes the global address family
  address-family ipv4 flowspec
!
  neighbor 192.0.2.1
    remote-as 64511
    ! Ties it to a neighbor configuration
    address-family ipv4 flowspec
```

Juniper

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


Copyright © 2014 Juniper Networks, Inc.

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。
- 需要客户和提供商之间的协调。

Copyright © 2014 Juniper Networks, Inc.

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;
    }
}
```


Copyright © 2014 Juniper Networks, Inc.

路由服务器配置

Alcatel-Lucent

```
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
```

Cisco [7]

```
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
```

Juniper

```
protocols {
    bgp {
        group RR-CLIENT-FLOWSPEC {
            type internal;
            neighbor 198.51.100.2 {
                family inet {
                    flow;
                }
                export FLOWROUTES_OUT;
            }
        }
    }
}
```


Copyright © 2014 Juniper Networks, Inc.

路由服务器配置

Cisco [7]

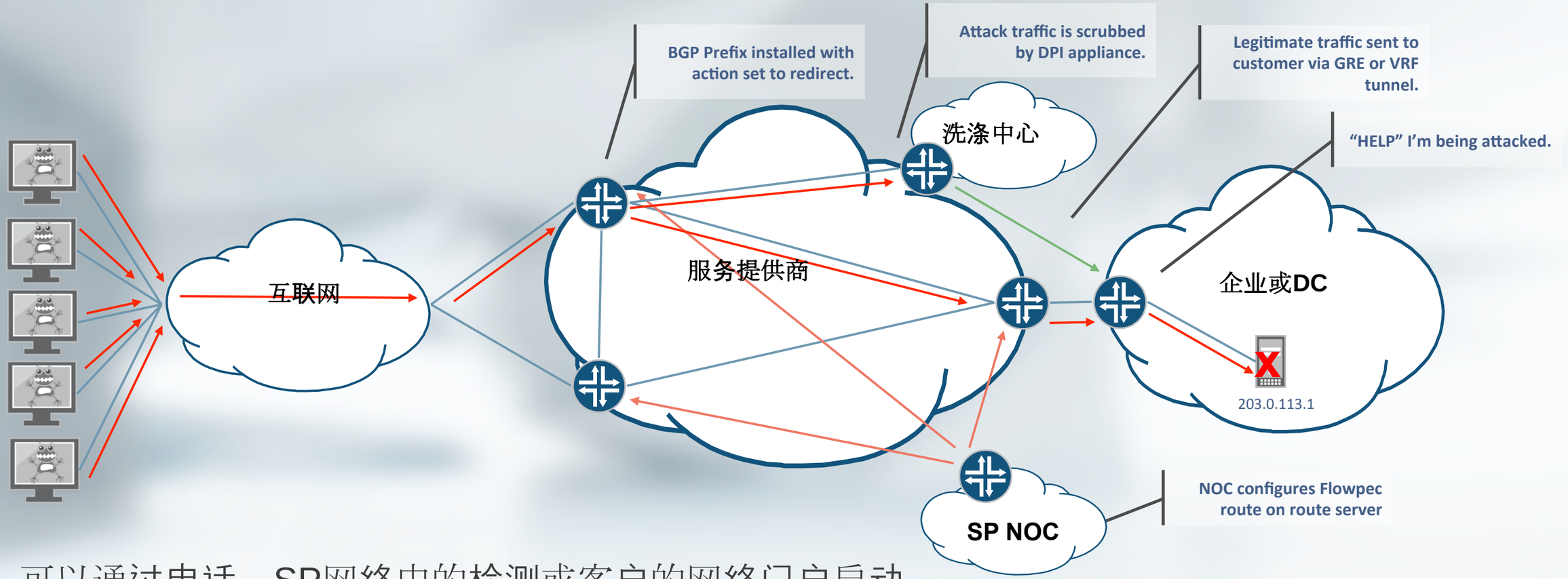
```
class-map type traffic match-all attack_fs
 match destination-address ipv4 203.0.113.1/32
 match protocol 17
 match destination-port 53
end-class-map
!
policy-map type pbr attack_pbr
 class type traffic attack_fs
  drop
 class class-default
end-policy-map
!
flowspec
 address-family ipv4
  service-policy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


Copyright © 2014 Juniper Networks, Inc.

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。

Copyright © 2014 Juniper Networks, Inc.

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;
    }
}
```


Copyright © 2014 Juniper Networks, Inc.

路由服务器配置

Alcatel-Lucent

```
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
```

Cisco [7]

```
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
```

Juniper

```
protocols {
    bgp {
        group RR-CLIENT-FLOWSPEC {
            type internal;
            neighbor 198.51.100.2 {
                family inet {
                    flow;
                }
                export FLOWROUTES_OUT;
            }
        }
    }
}
```


Copyright © 2014 Juniper Networks, Inc.

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;
        }
    }
}
```


Copyright © 2014 Juniper Networks, Inc.

我怎么知道它正在工作？

Alcatel-Lucent

- show router bgp routes flow-ipv4
- show router bgp routes flow-ipv6
- show filter ip fSpec-0
- show filter ip fSpec-0 associations
- show filter ip fSpec-0 counters
- show filter ip fSpec-0 entry <entry-id>

Cisco [7]

- show processes flowspec_mgr location all
- show flowspec summary
- show flowspec vrf all
- show bgp ipv4 flowspec

Juniper

- show bgp neighbor <neighbor> | match inet-flow
- show route table inetflow.0 extensive
- show firewall filter __flowspec_default_inet__

Copyright © 2014 Juniper Networks, Inc.

我们要去哪里？

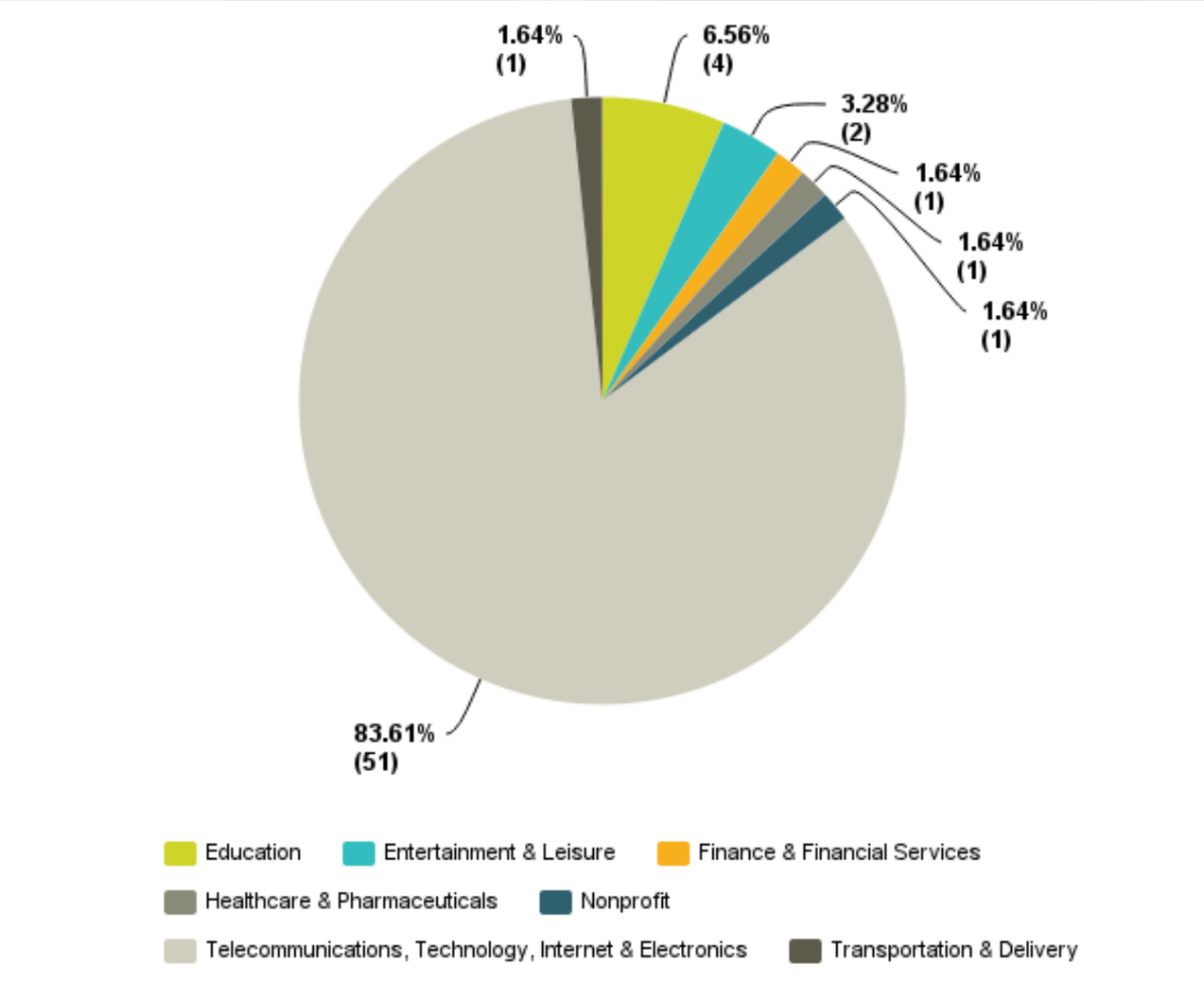
- IPv6支持
  - http://tools.ietf.org/html/draft-ietf-idr-flow-spec-v6-03
- 放松验证
  - http://tools.ietf.org/html/draft-ietf-idr-bgp-flowspec-oid-00
- 重定向到IP下一跳操作
  - http://tools.ietf.org/html/draft-simpson-idr-flowspec-redirect-02

Copyright © 2014 Juniper Networks, Inc.

国情咨文

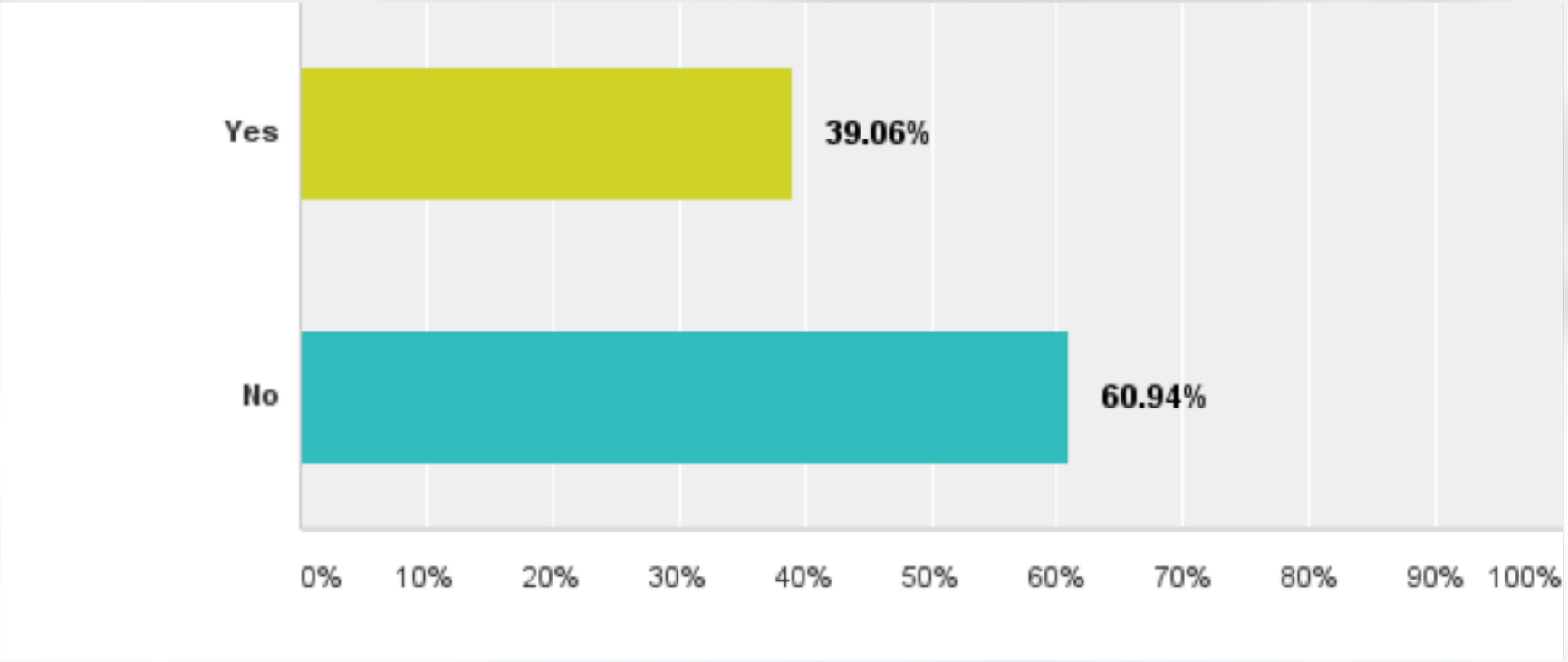
Copyright © 2014 Juniper Networks, Inc.

响应行业



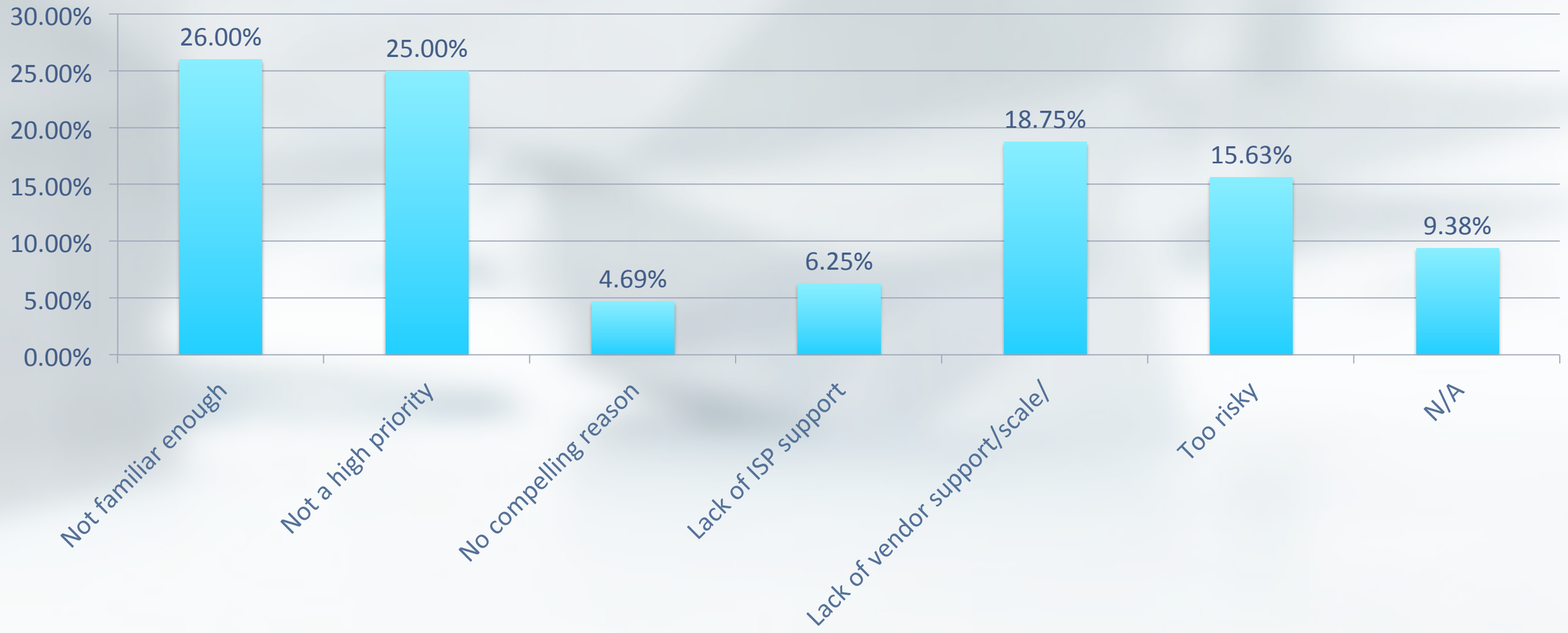
Copyright © 2014 Juniper Networks, Inc.

您是否已经在网络的任何部分启用了BGP Flowspec？



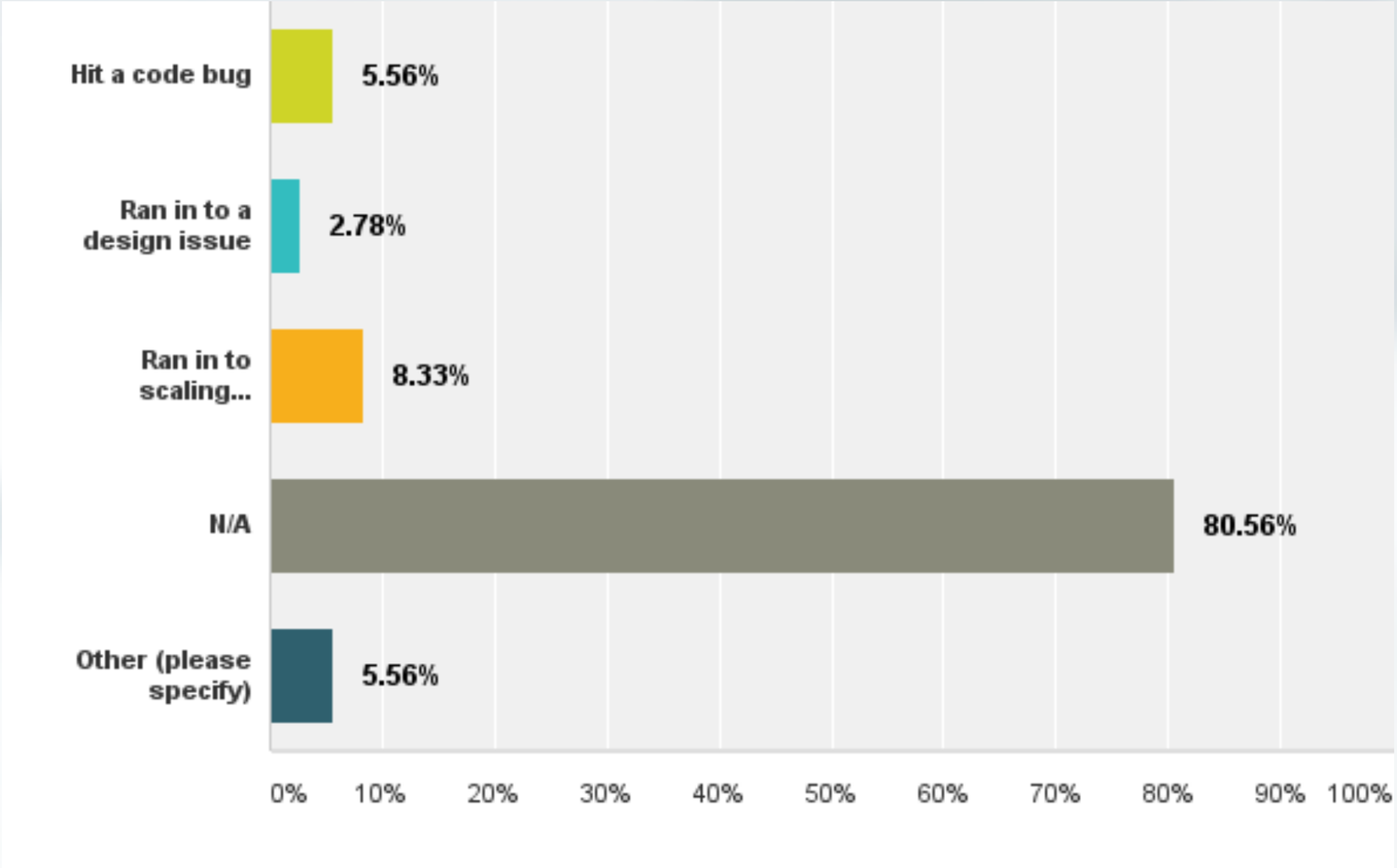
Copyright © 2014 Juniper Networks, Inc.

如果尚未启用，为什么不启用？



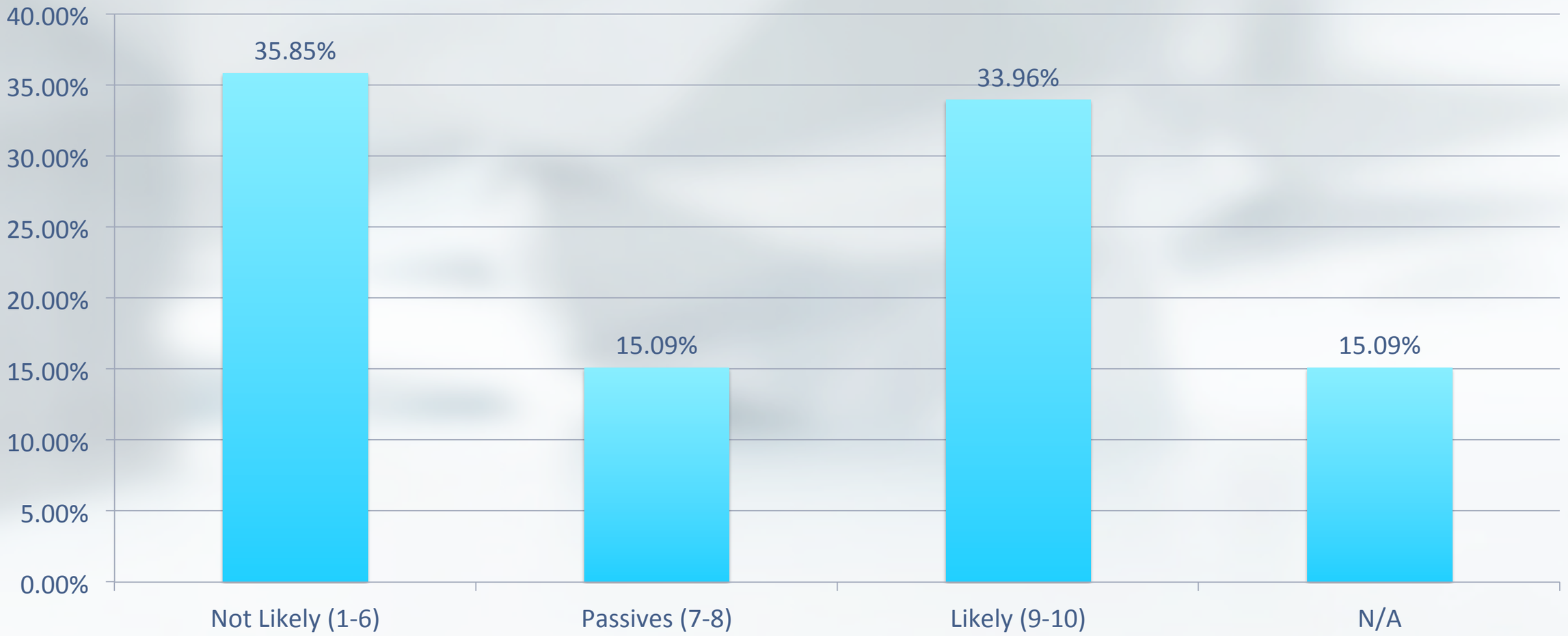
Copyright © 2014 Juniper Networks, Inc.

如果启用了此功能，但之后又禁用了它，为什么？



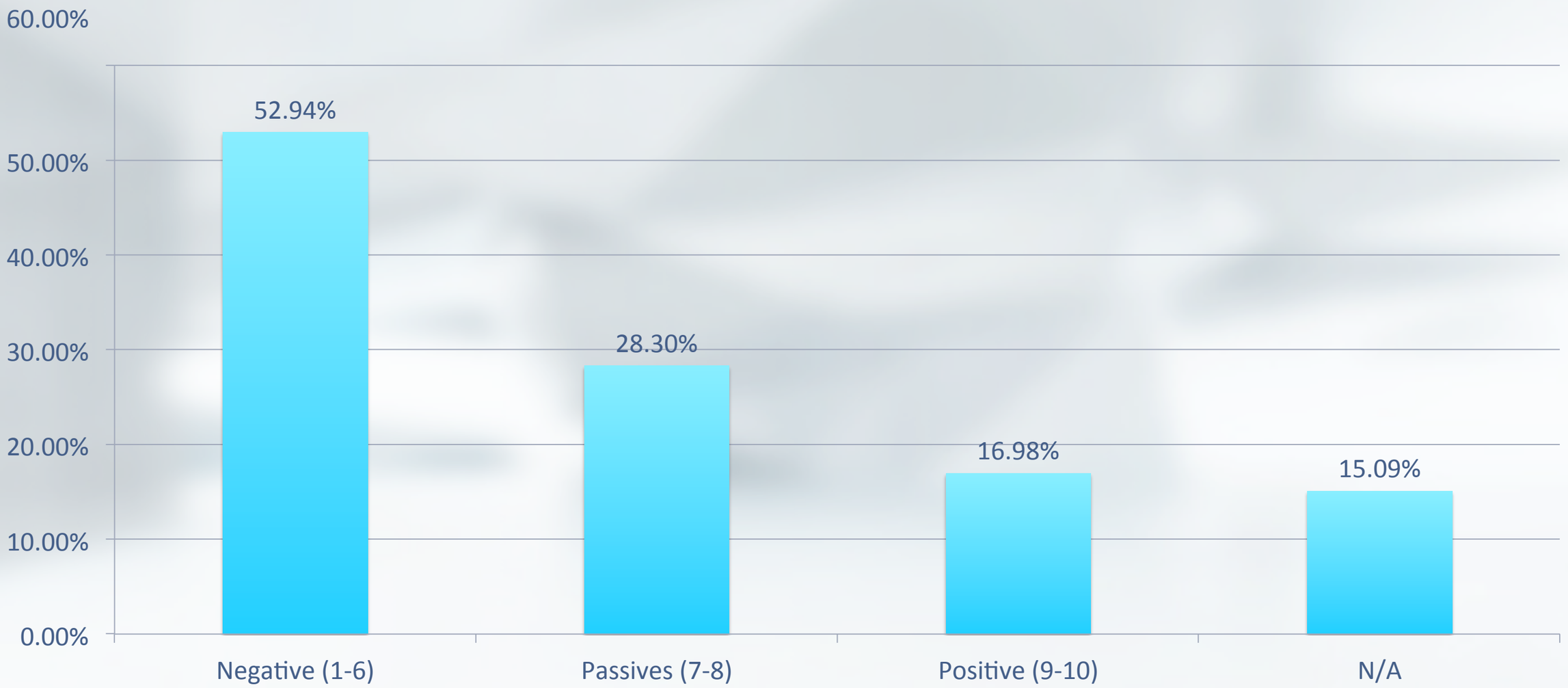
Copyright © 2014 Juniper Networks, Inc.

如果您当前未启用它，那么将来启用BGP Flowspec的可能性有多大？



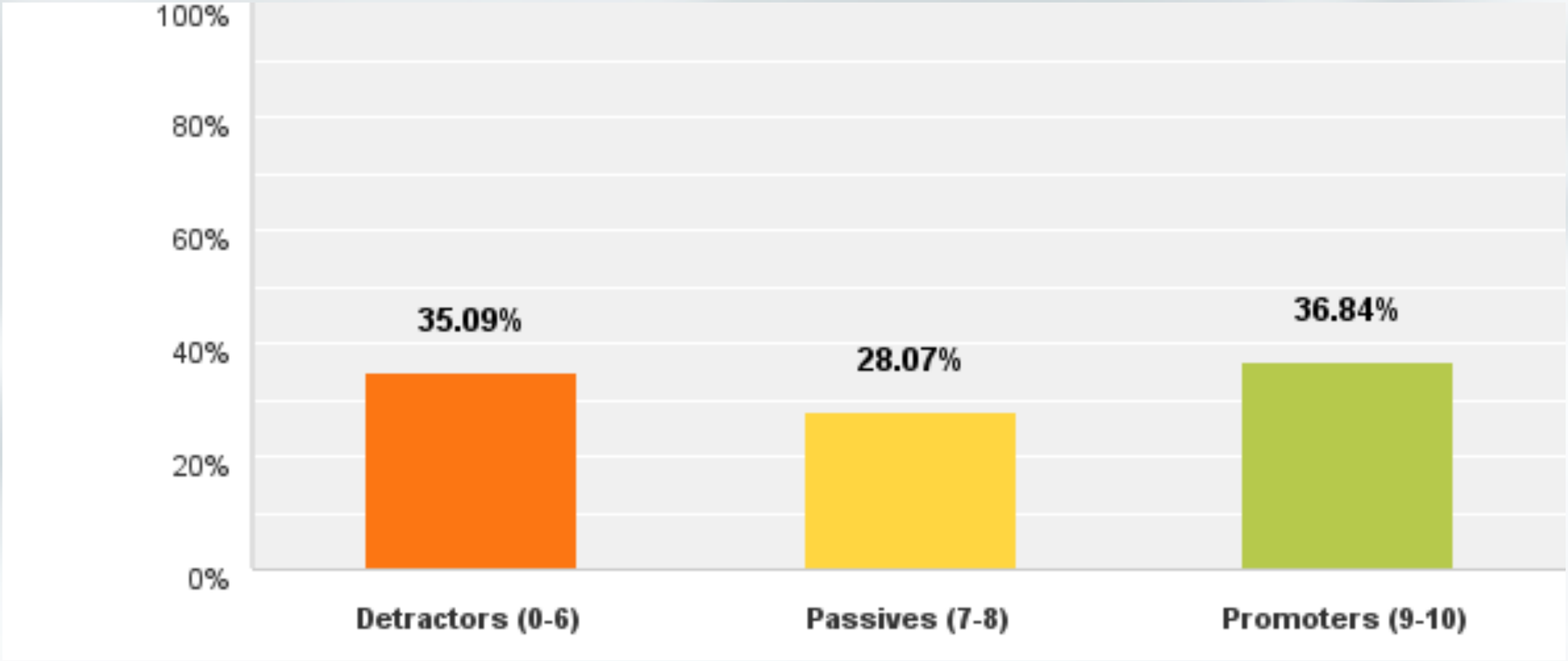
Copyright © 2014 Juniper Networks, Inc.

总体而言，您如何评价BGP Flowpsec体验？



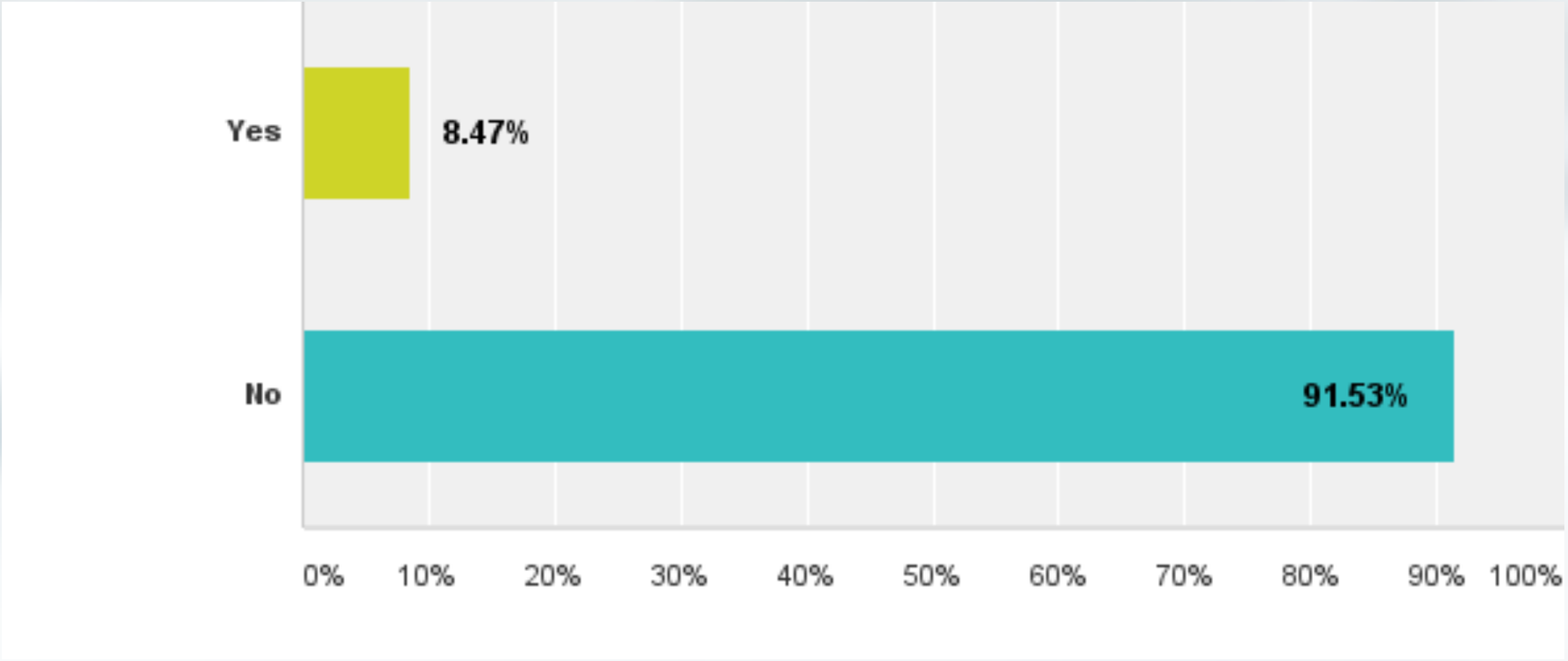
Copyright © 2014 Juniper Networks, Inc.

您向朋友或同事推荐BGP Flowspec的可能性有多大？



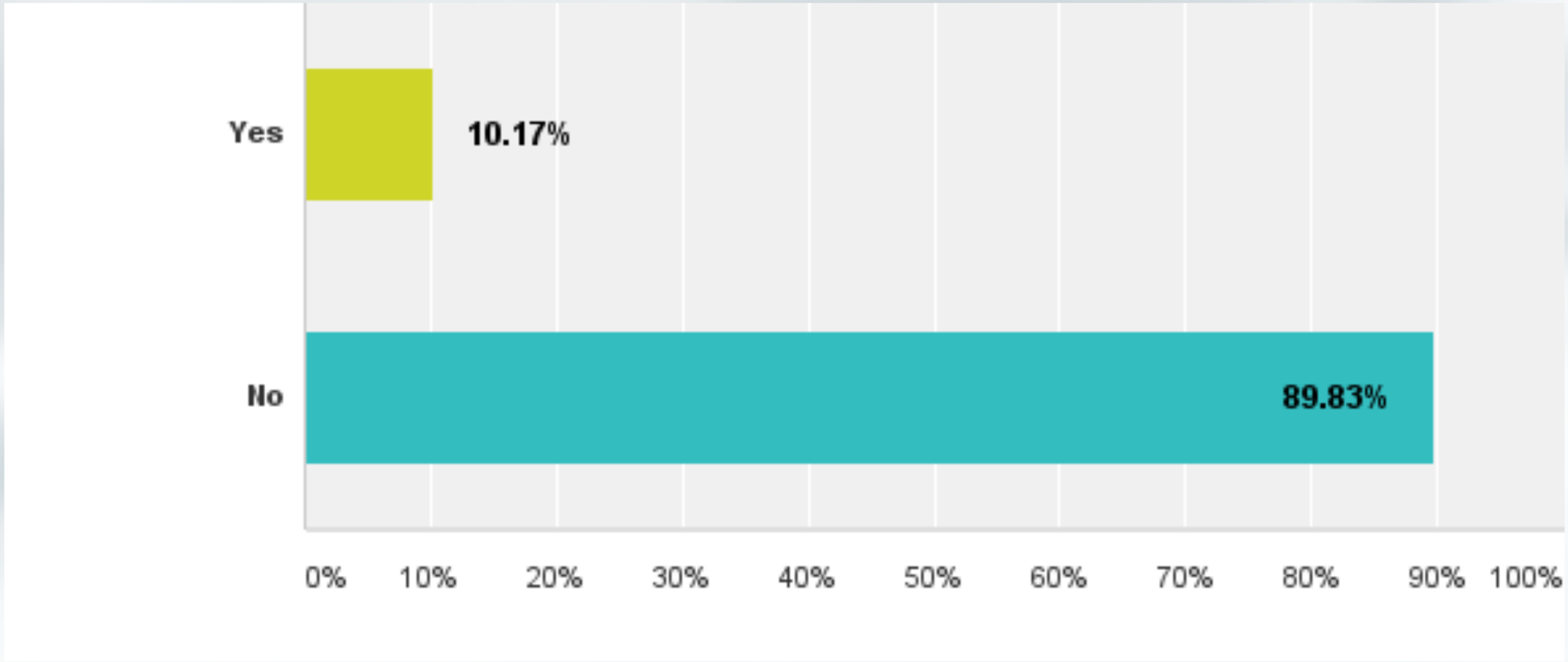
Copyright © 2014 Juniper Networks, Inc.

您是否允许客户通过BGP向您发送BGP Flowspec路由？



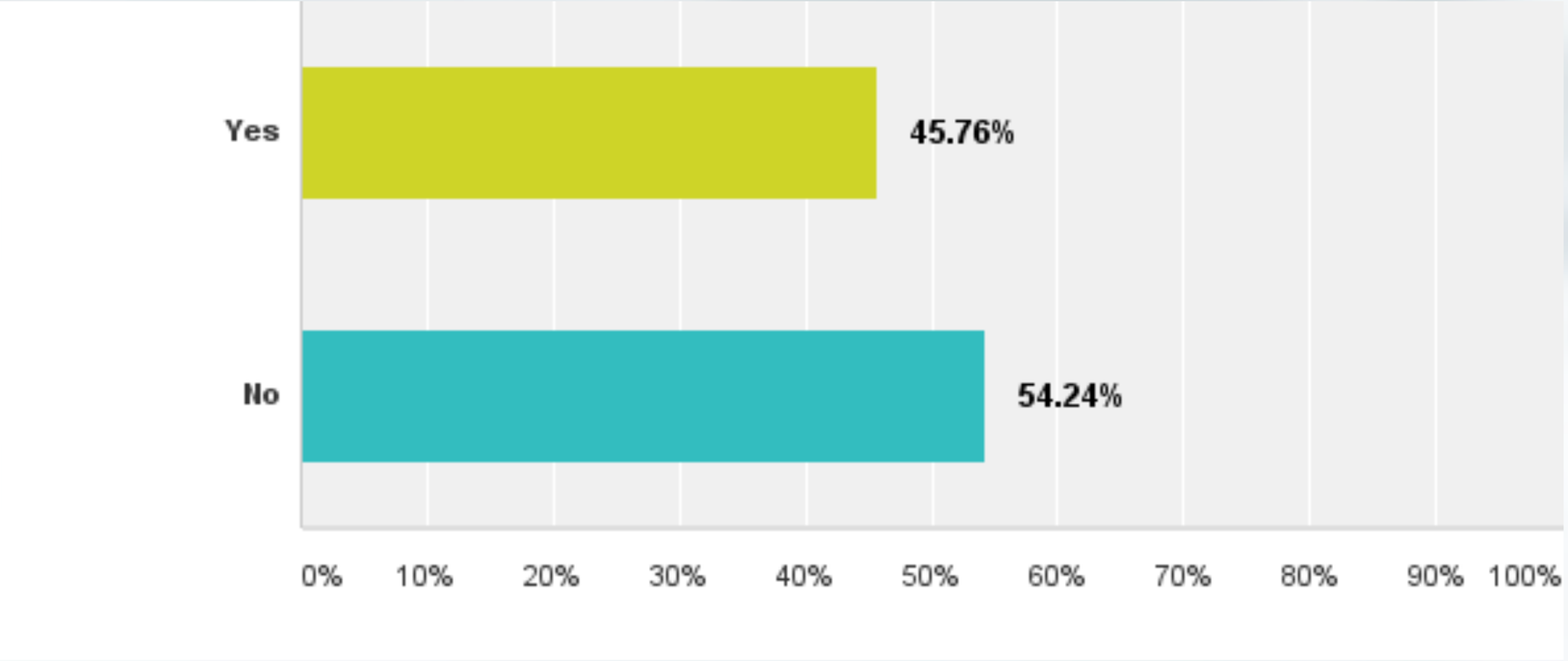
Copyright © 2014 Juniper Networks, Inc.

您是否有一个网络门户，客户可以在其中向您的IBGP注入BGP Flowspec路由？



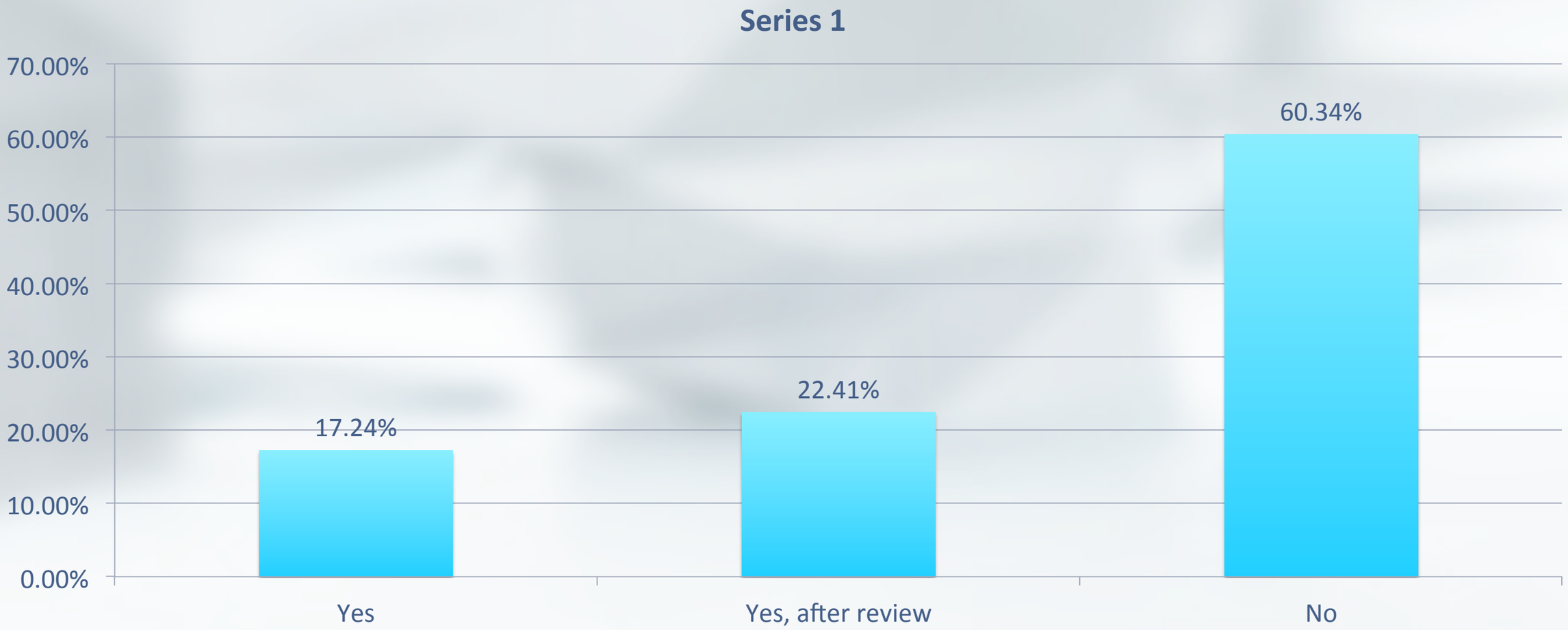
Copyright © 2014 Juniper Networks, Inc.

您是否具有从中注入BGP Flowspec路由的中央路由器？



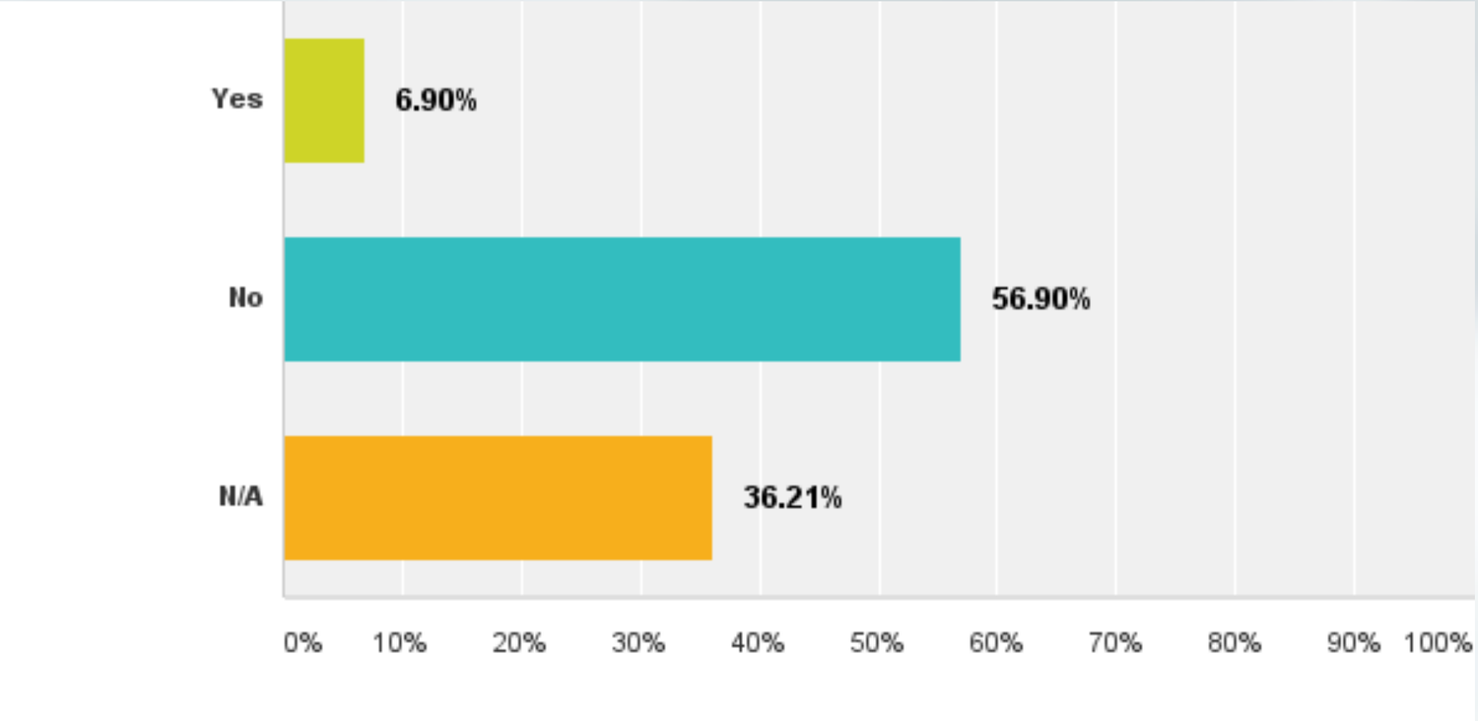
Copyright © 2014 Juniper Networks, Inc.

是否允许分布式拒绝服务检测工具（如Arbor）将BG P Flowspec路由发送到IBGP？



Copyright © 2014 Juniper Networks, Inc.

您是否使用BGP Flowspec进行分布式拒绝服务防护？



Copyright © 2014 Juniper Networks, Inc.

评论摘要

- 好主意，并希望看到它起飞，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Flowspec路由。
  - 有些甚至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

Copyright © 2014 Juniper Networks, Inc.

References

- [1] Kaspersky Lab – 每三分之一的面向公众的公司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 News – 互联网速度急剧上升，但黑客攻击也在上升 **http://tinyurl.com/q4u2b7m**
- [4] Tech Times – 微软拒绝Xbox Live失败时，分布式拒绝服务攻击削弱了索尼PSN **http://tinyurl.com/kkdczjx**
- [5] RFC 5575 - 传播流量规范规则 **http://www.ietf.org/rfc/rfc5575.txt**
- [6] Cisco - 实施BGP Flowspec **http://tinyurl.com/mm5w7mo**
- [7] Cisco – 了解BGP Flowspec **http://tinyurl.com/l4kwb3b**

Copyright © 2014 Juniper Networks, Inc.

谢谢你！