DDoS Mitigation

Using BGP Flowspec

Justin Ryburn
Senior System Engineer

Background

- Who is this guy?
  - http://www.linkedin.com/in/justinryburn
- Why this topic?
  - Experience tracking DDoS “back in the day”.

Is DDoS Really an Issue?

"…taking down a site or preventing transactions is only the tip of the iceberg. A DDoS attack can lead to reputational losses or legal claims over undelivered services."

Kaspersky Lab [1]

Verisign [2]

"Attacks in the 10 Gbps and above category grew by 38% from Q2 … Q3."

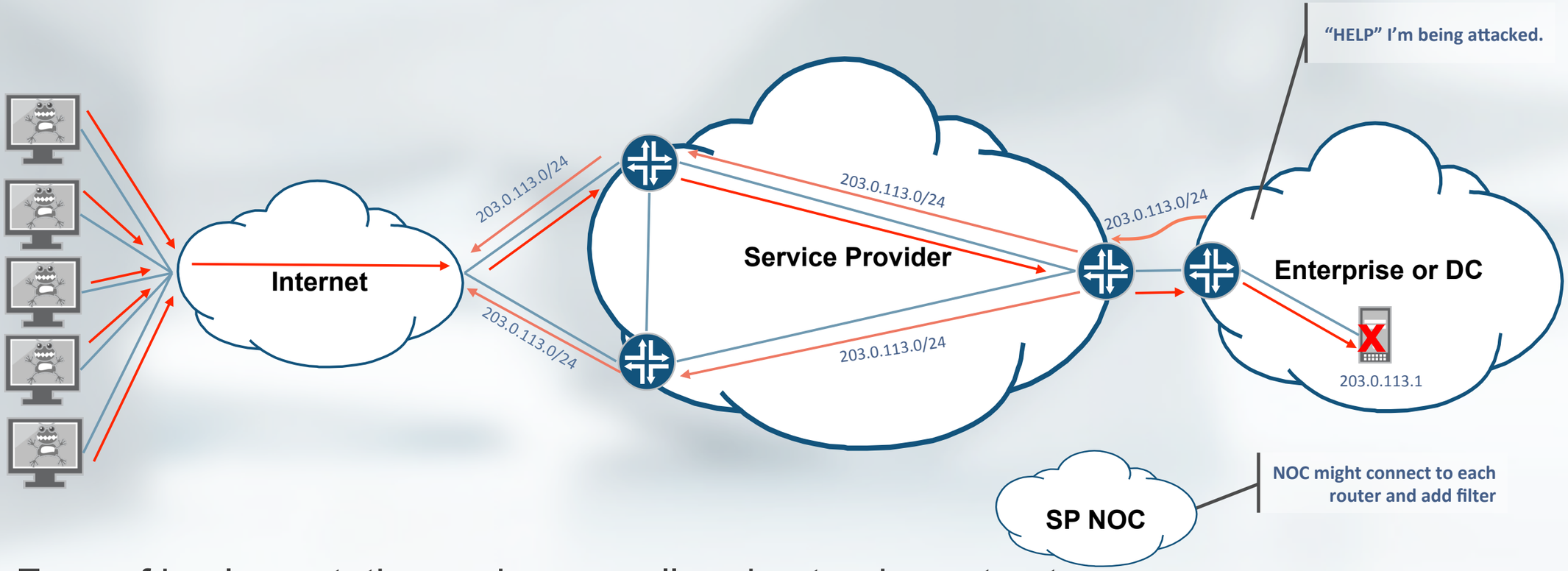
NBC News [3]

"…more than 40 percent estimated DDoS losses at more than $1 million per day."

Tech Times [4]

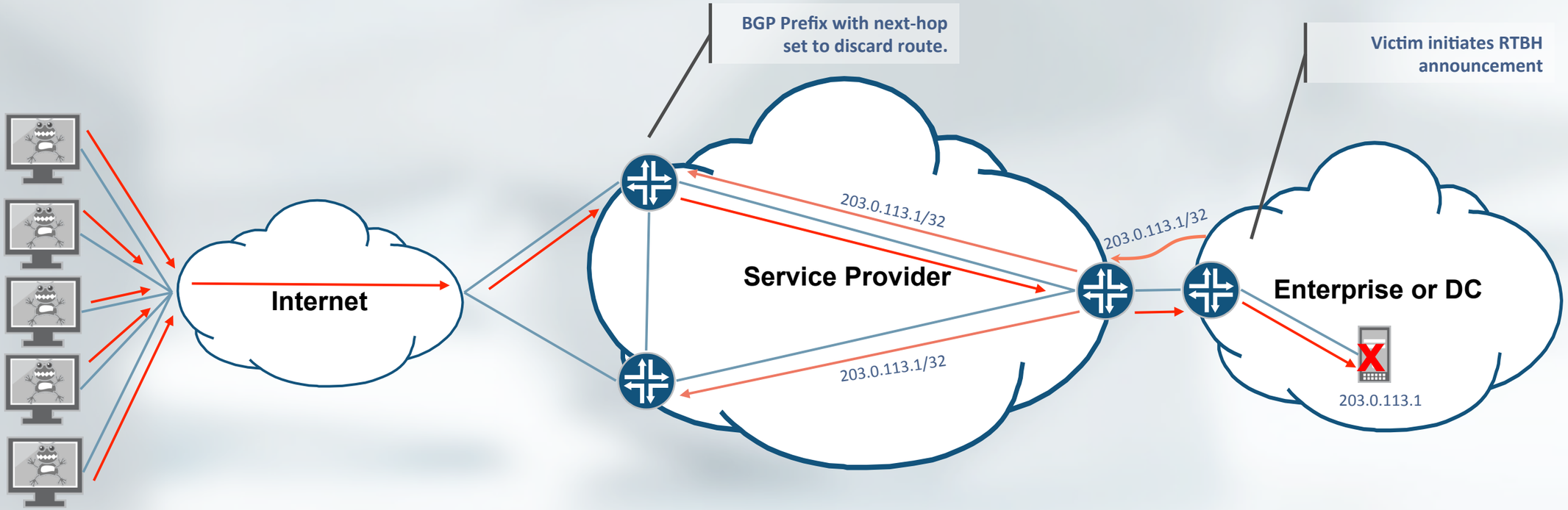
"DDoS attack cripples Sony PSN while Microsoft deals with Xbox Live woes"

Blocking DDoS in the “Old” Days



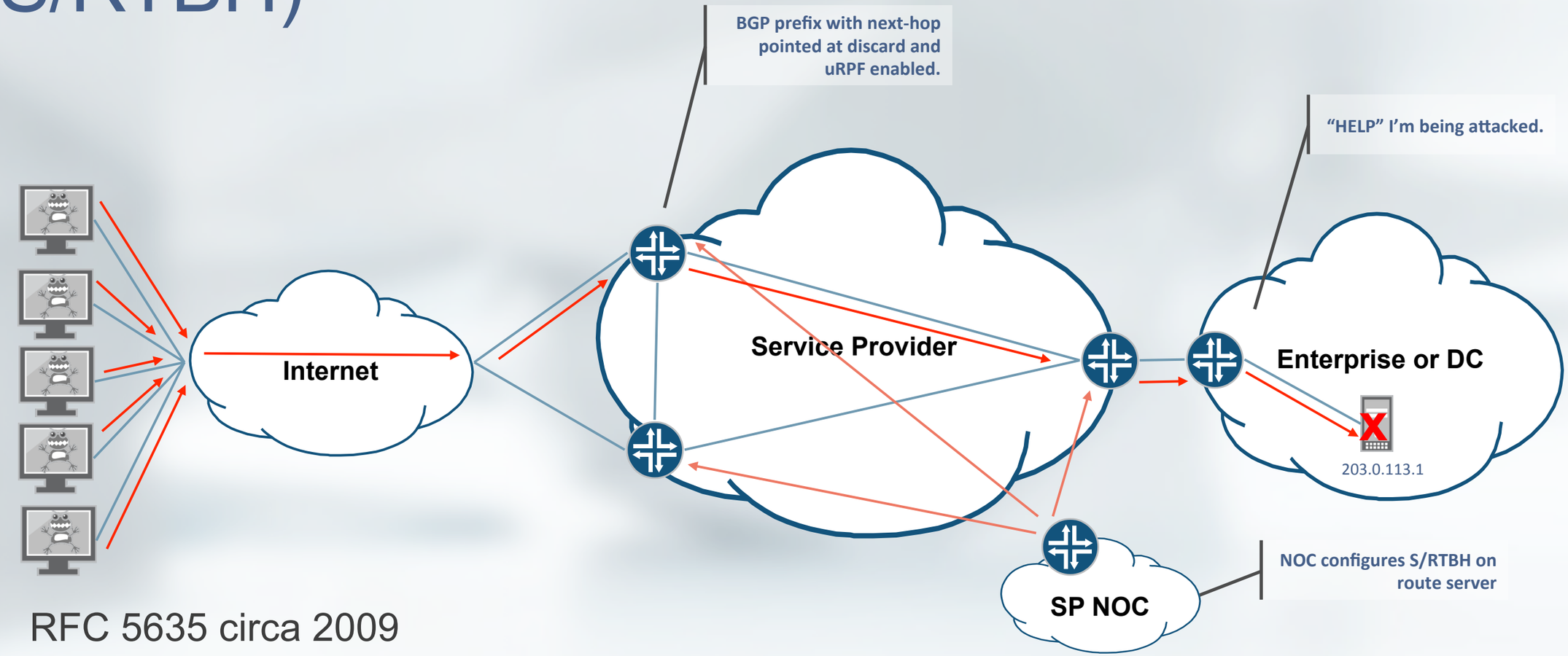
- Ease of implementation and uses well understood constructs
- Requires high degree of co-ordination between customer and provider
- Cumbersome to scale in a large network perimeter
- Mis-configuration possible and expensive

Destination Remotely Triggered Black Hole (D/RTBH)



- RFC 3882 circa 2004
- Requires pre-configuration of discard route on all edge routers
- Victim's destination address is completely unreachable but attack (and collateral damage) is stopped.

Source Remotely Triggered Black Hole (S/RTBH)



- RFC 5635 circa 2009
- Requires pre-configuration of discard route and uRPF on all edge routers
- Victim's destination address is still useable
- Only works for single (or small number) source.

BGP Flow Specification

- Specific information about a flow can now be distributed using a BGP NLRI defined in RFC 5575 [5] circa 2009
  - AFI/SAFI = 1/133: Unicast Traffic Filtering Applications
  - AFI/SAFI = 1/134: VPN Traffic Filtering Applications
- Flow routes are automatically validated against unicast routing information or via routing policy framework.
  - Must belong to the longest match unicast prefix.
- Once validated, firewall filter is created based on match and action criteria.

BGP Flow Specification

- BGP Flowspec can include the following information:
  - Type 1 - Destination Prefix
  - Type 2 - Source Prefix
  - Type 3 - IP Protocol
  - Type 4 – Source or Destination Port
  - Type 5 – Destination Port
  - Type 6 - Source Port
  - Type 7 – ICMP Type
  - Type 8 – ICMP Code
  - Type 9 - TCP flags
  - Type 10 - Packet length
  - Type 11 – DSCP
  - Type 12 - Fragment Encoding

BGP Flow Specification

- Actions are defined using BGP Extended Communities:
  - 0x8006 – traffic-rate (set to 0 to drop all traffic)
  - 0x8007 – traffic-action (sampling)
  - 0x8008 – redirect to VRF (route target)
  - 0x8009 – traffic-marking (DSCP value)

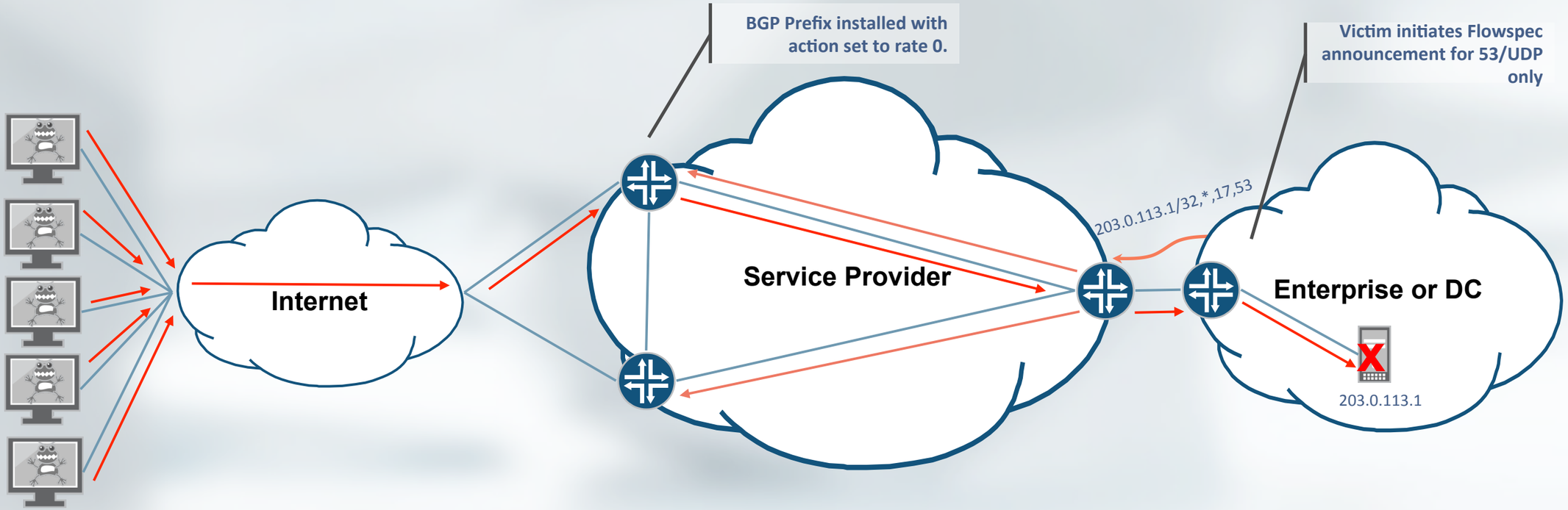
Vendor Support

- DDoS Detection Vendors:
  - Arbor Peakflow SP 3.5
  - Juniper DDoS Secure 5.14.2-0
- Router Vendors:
  - Alcatel-Lucent SR OS 9.0R1
  - Juniper JUNOS 7.3
  - Cisco 5.2.0 for ASR and CRS [6]

What Makes BGP Flowspec Better?

- Same granularity as ACLs
  - Based on n-tuple matching
- Same automation as RTBH
  - Much easier to propagate filters to all edge routers in large networks
- Leverages BGP best practices and policy controls
  - Same filtering and best practices used for RTBH can be applied to BGP Flowspec

Inter-domain DDoS Mitigation Using Flowspec



- Allows ISP customer to initiate the filter.
- Requires sane filtering at customer edge.

Edge Router Configuration

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
```

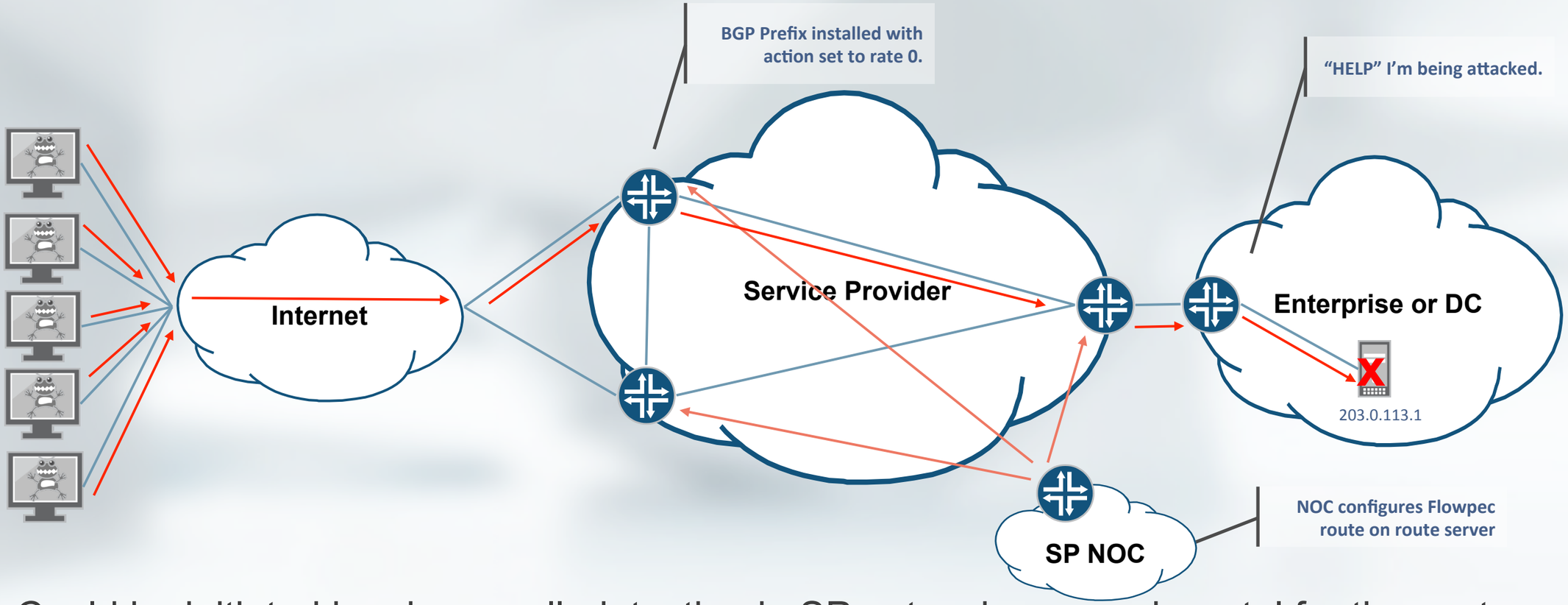
Cisco [7]

```
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;
    }
}
```

Intra-domain DDoS Mitigation Using Flowspec



- Could be initiated by phone call, detection in SP network, or a web portal for the customer.
- Requires co-ordination between customer and provider.

Edge Router Configuration

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;
    }
}
```

Route Server Configuration

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;
            }
        }
    }
}
```

Route Server Configuration

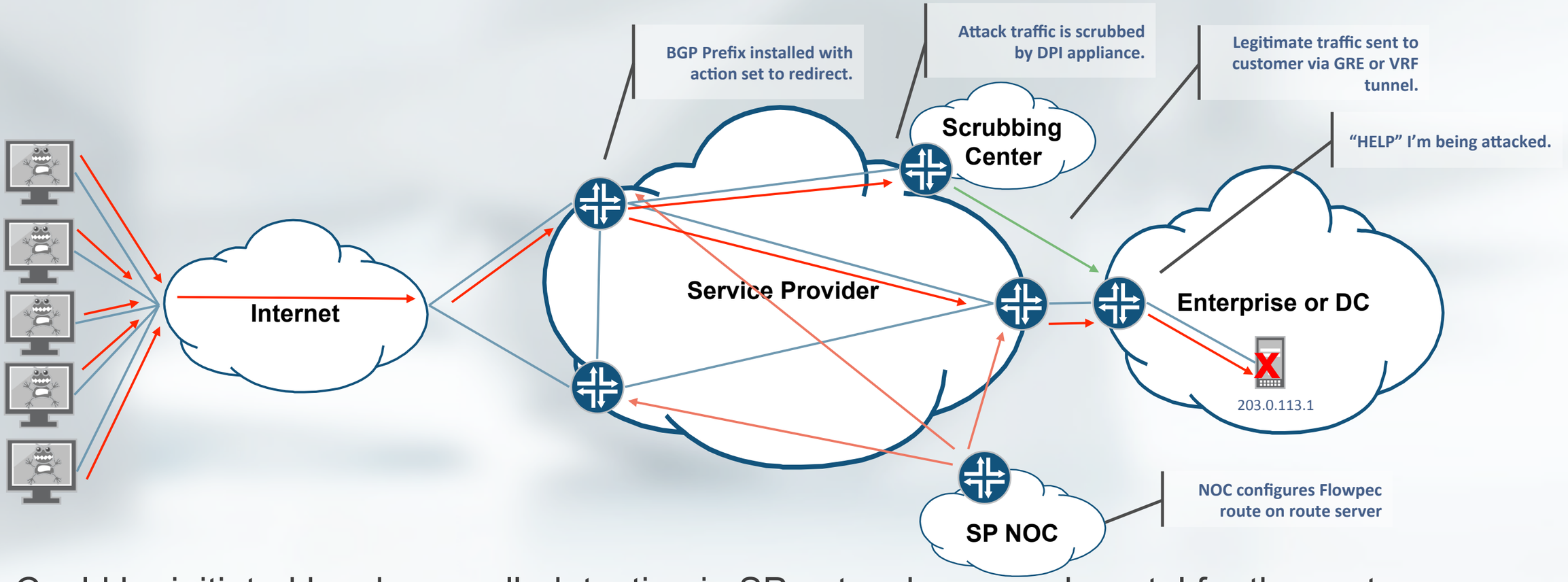
Cisco [7]

```
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;
    }
}
```

DDoS Mitigation Using Scrubbing Center



- Could be initiated by phone call, detection in SP network, or a web portal for the customer.
- Allows for mitigating application layer attacks without completing the attack.

Edge Router Configuration

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;
    }
}
```

Route Server Configuration

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;
            }
        }
    }
}
```

Route Server Configuration

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;
        }
    }
}
```

How Do I Know It Is Working?

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

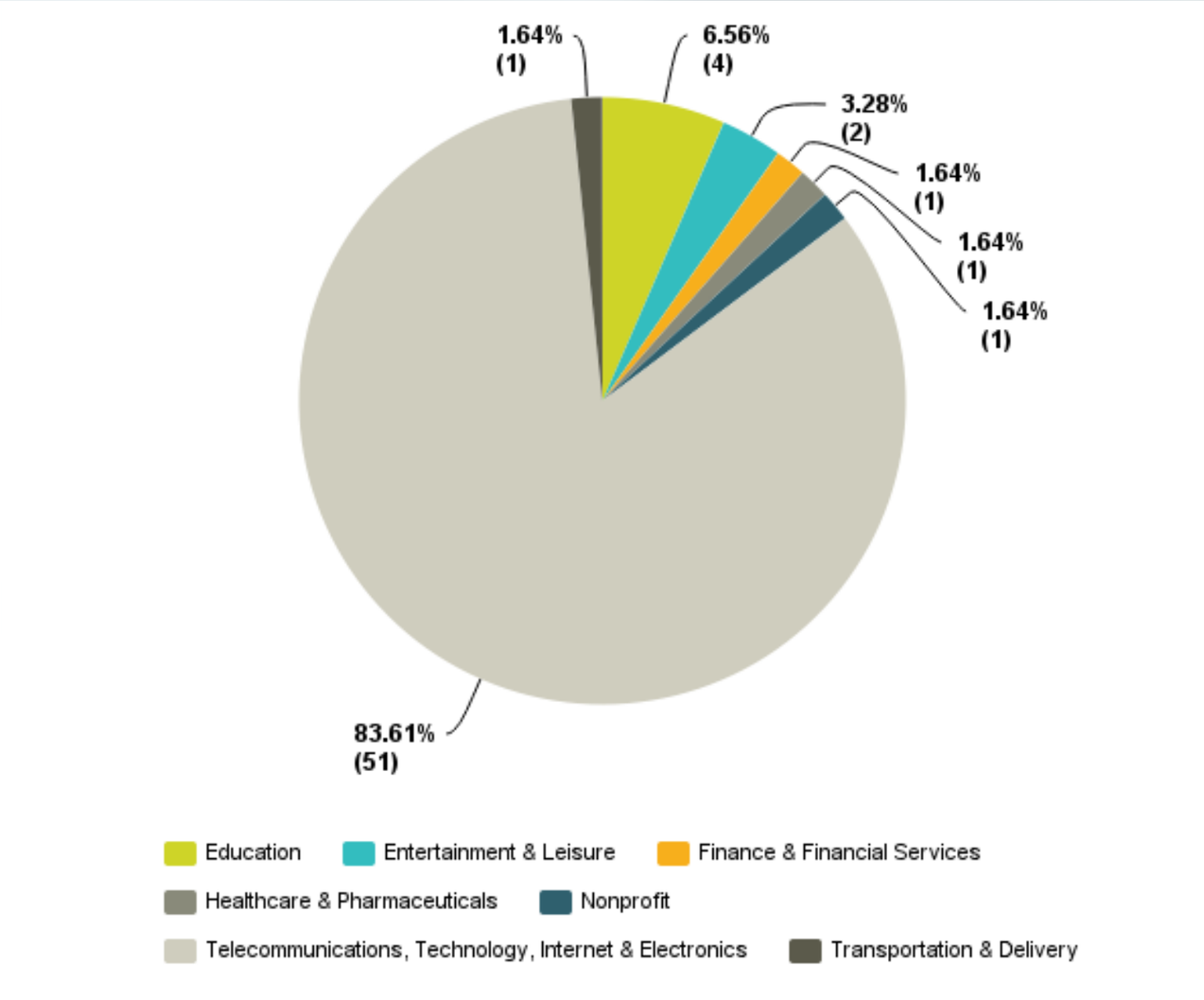
- show bgp neighbor <neighbor> | match inet-flow
- show route table inetflow.0 extensive
- show firewall filter __flowspec_default_inet__

Where Are We Going?

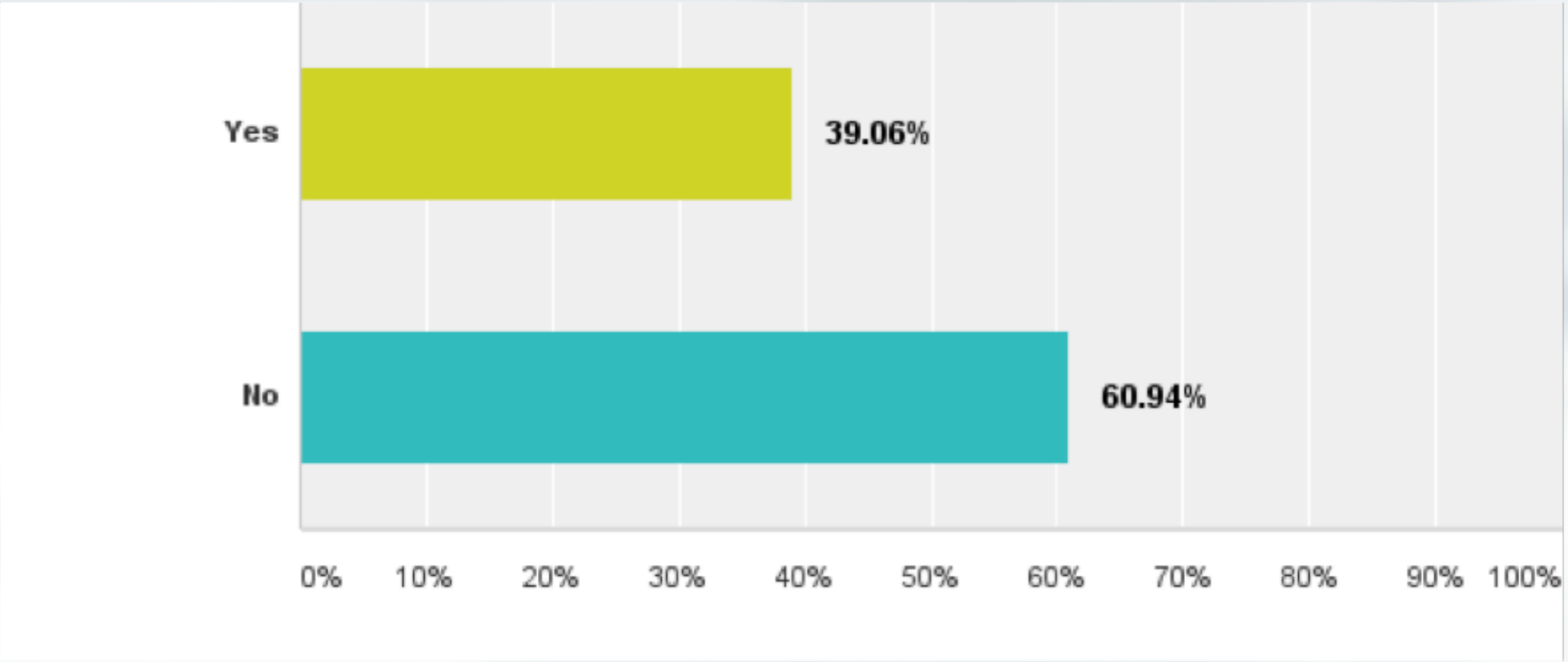
- IPv6 Support
  - http://tools.ietf.org/html/draft-ietf-idr-flow-spec-v6-03
- Relaxing Validation
  - http://tools.ietf.org/html/draft-ietf-idr-bgp-flowspec-oid-00
- Redirect to IP Next-Hop Action
  - http://tools.ietf.org/html/draft-simpson-idr-flowspec-redirect-02

State of the Union

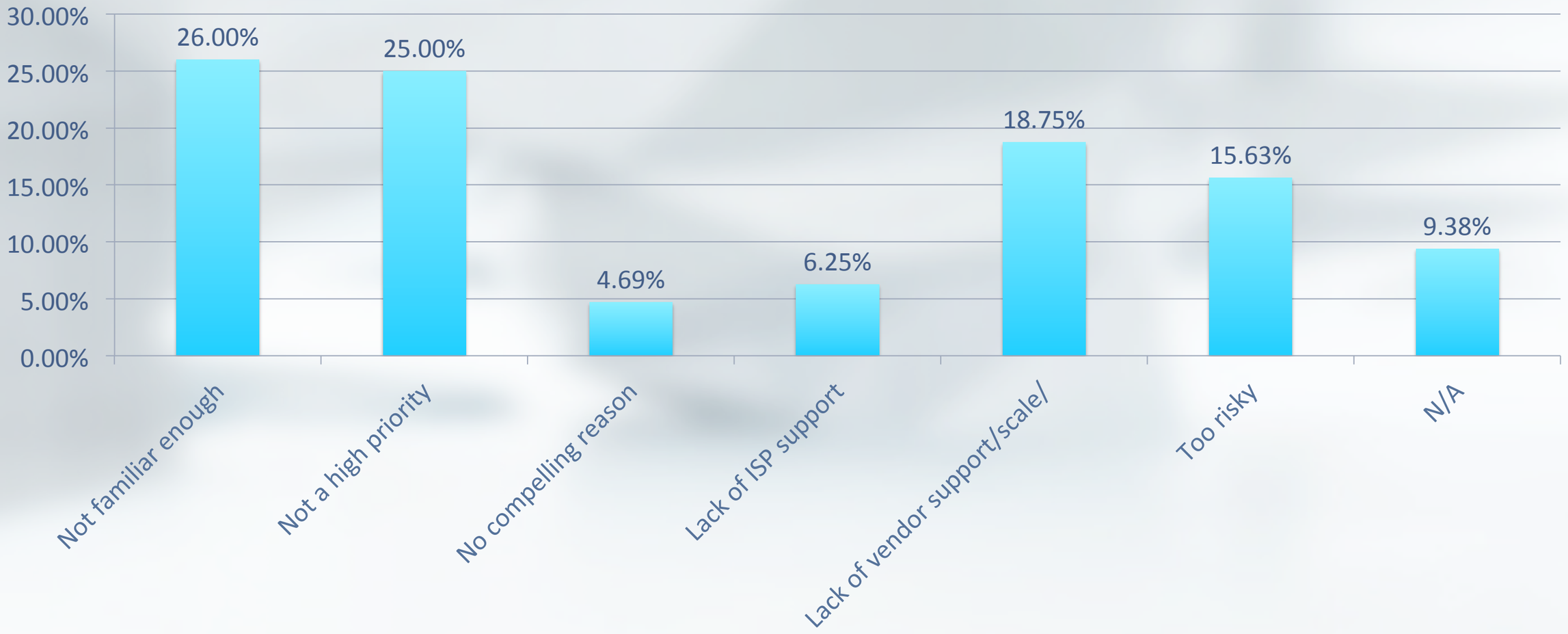
Industries Responding



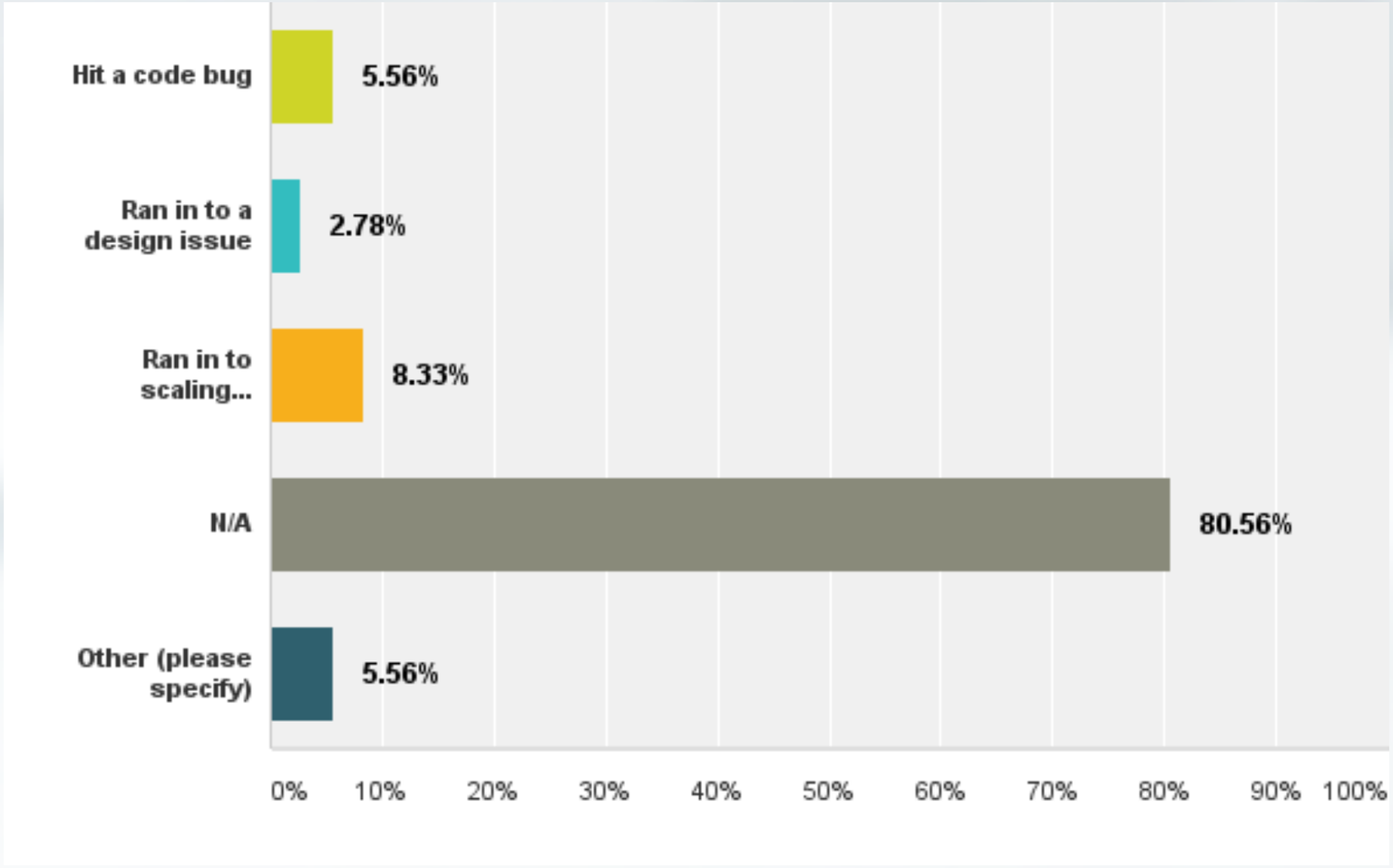
Do you have, or have you ever had, BGP Flowspec enabled in any part of your network?



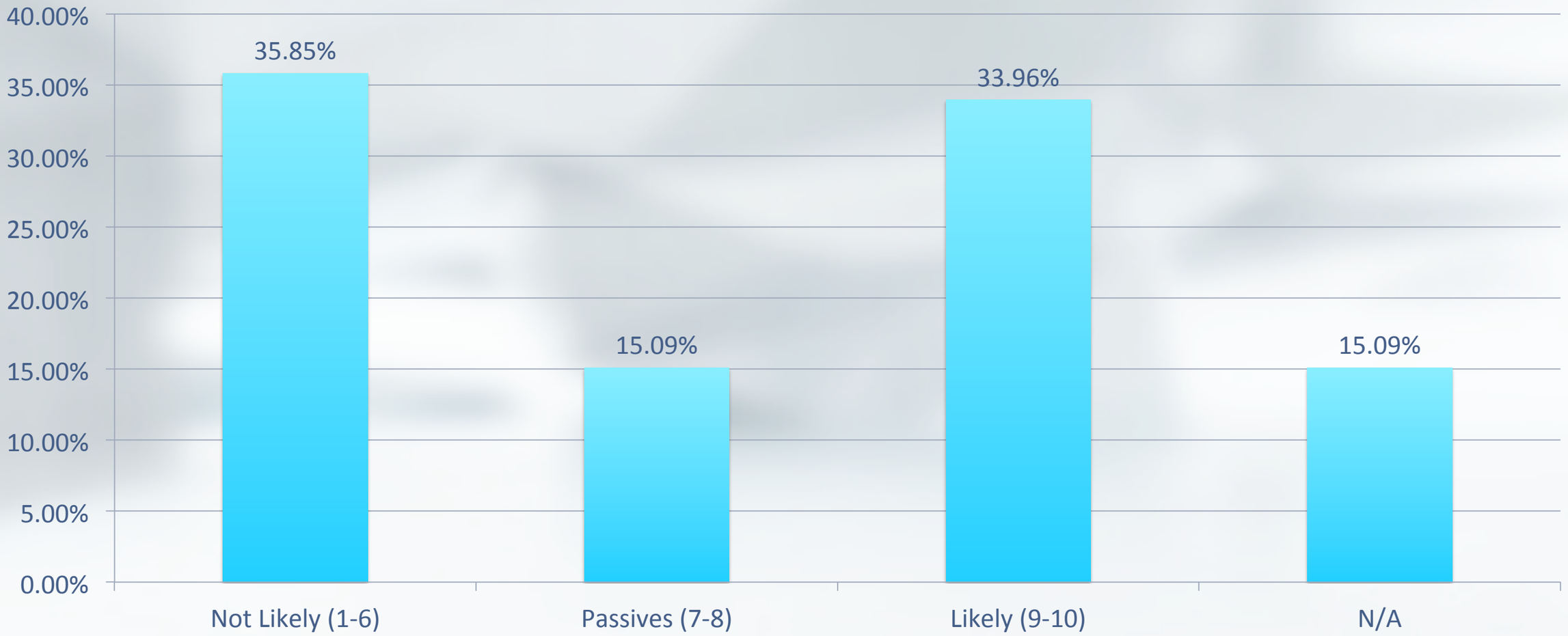
If you have not enabled it, why not?



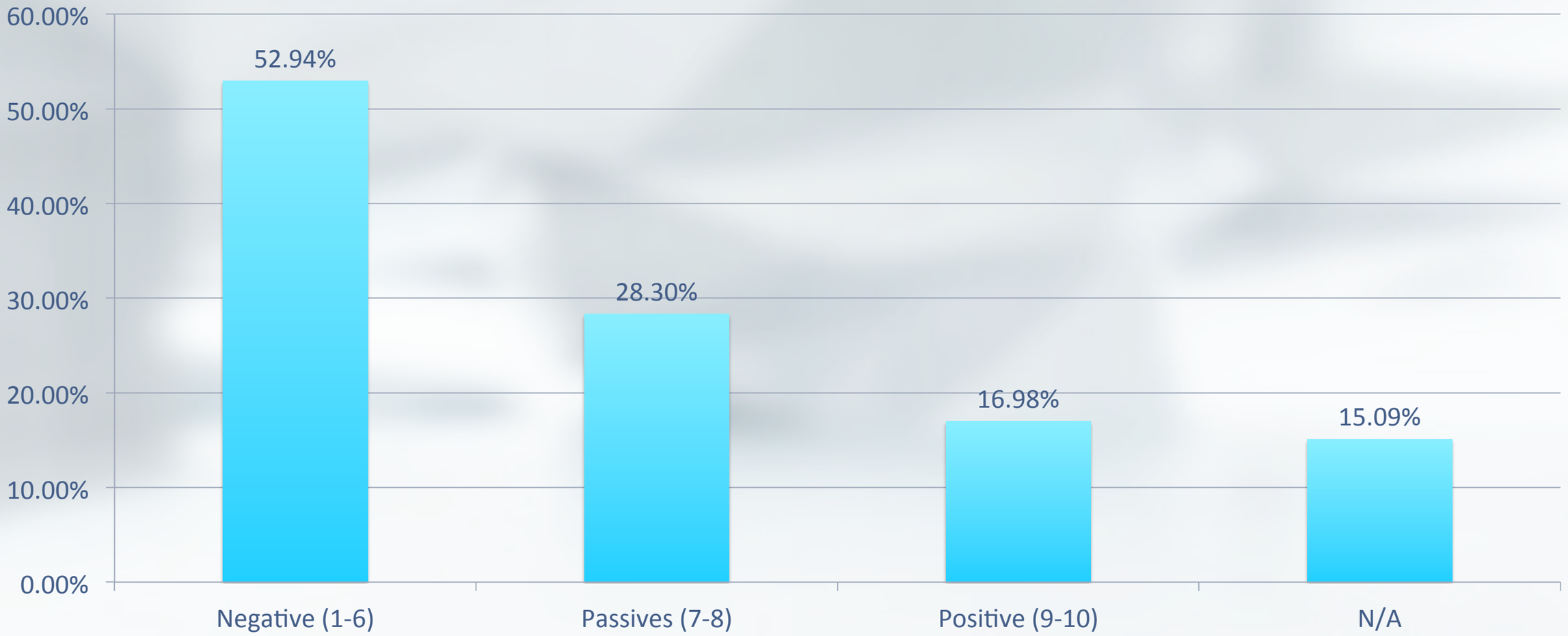
If you enabled it but have since disabled it, why?



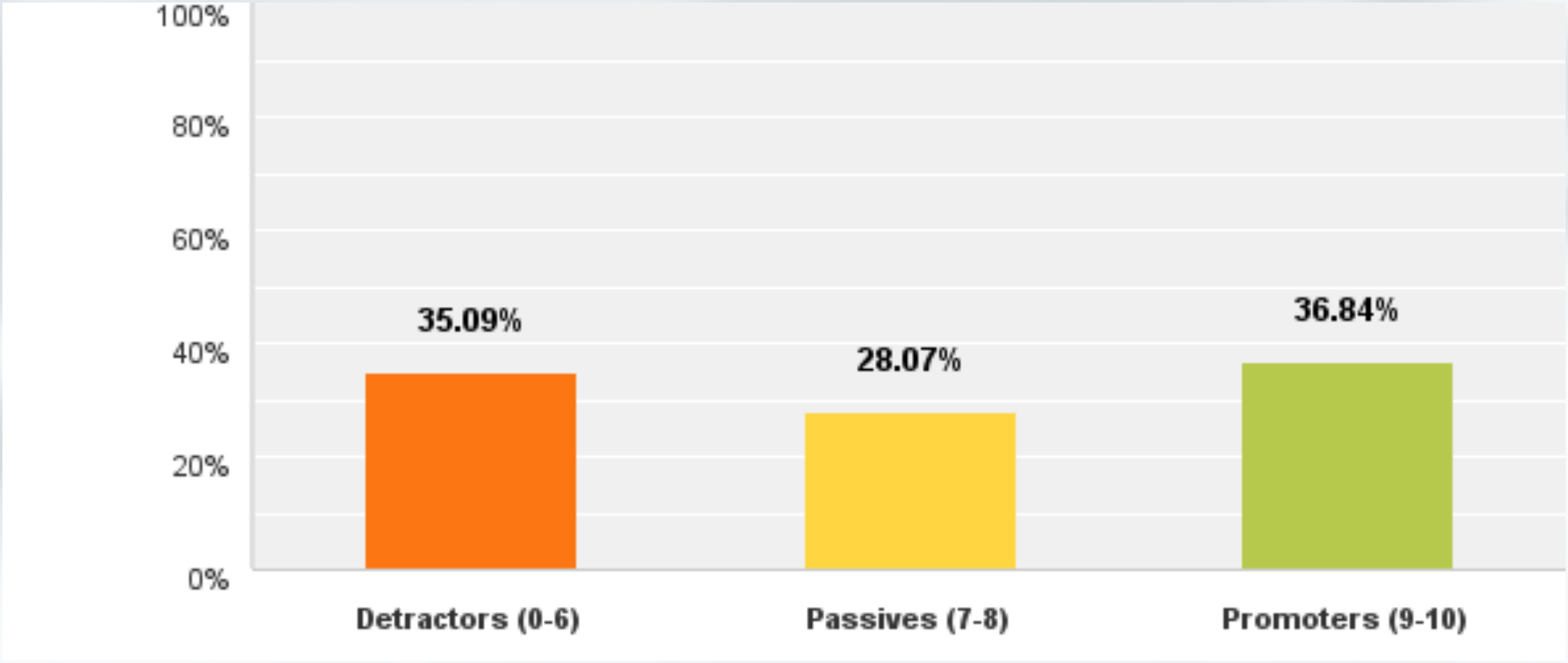
If you do not have it enabled currently, how likely are you to enable BGP Flowspec in the future?



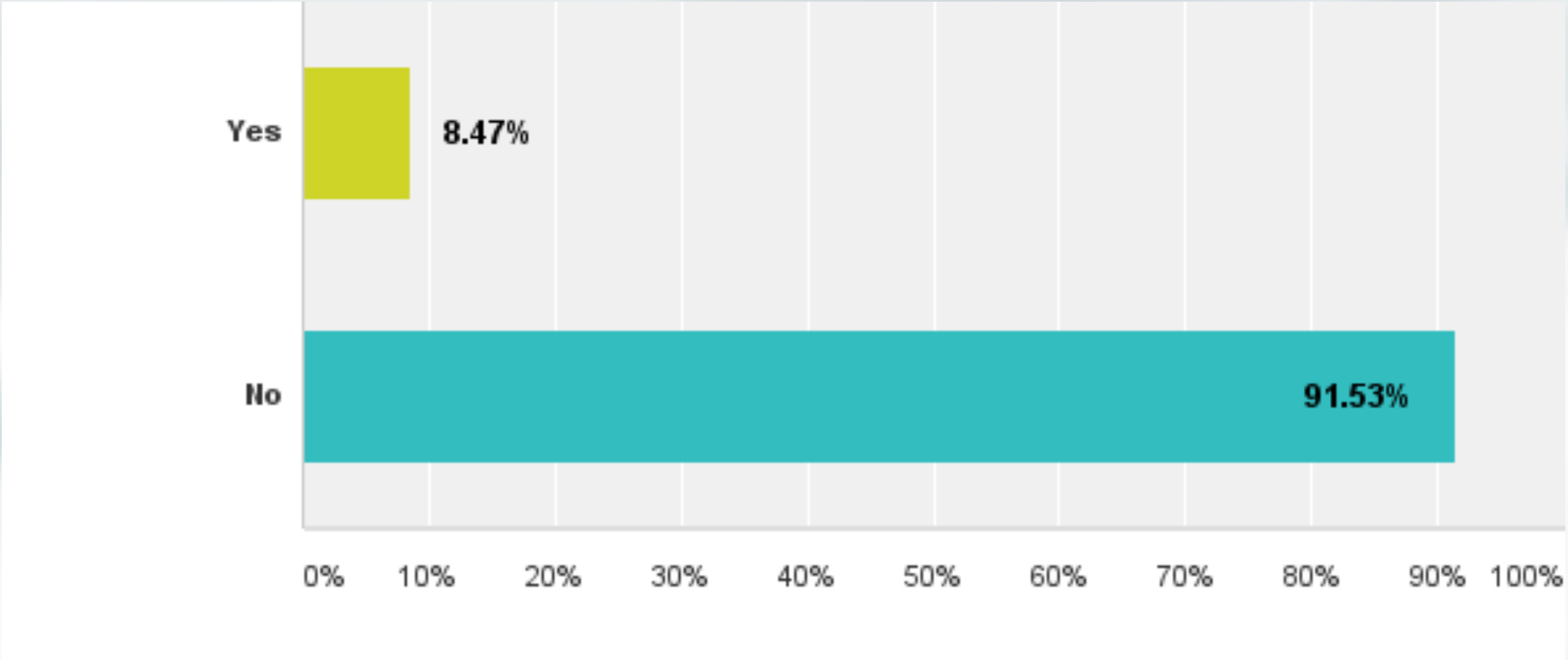
Overall, how would you rate your experience with BGP Flowpsec?



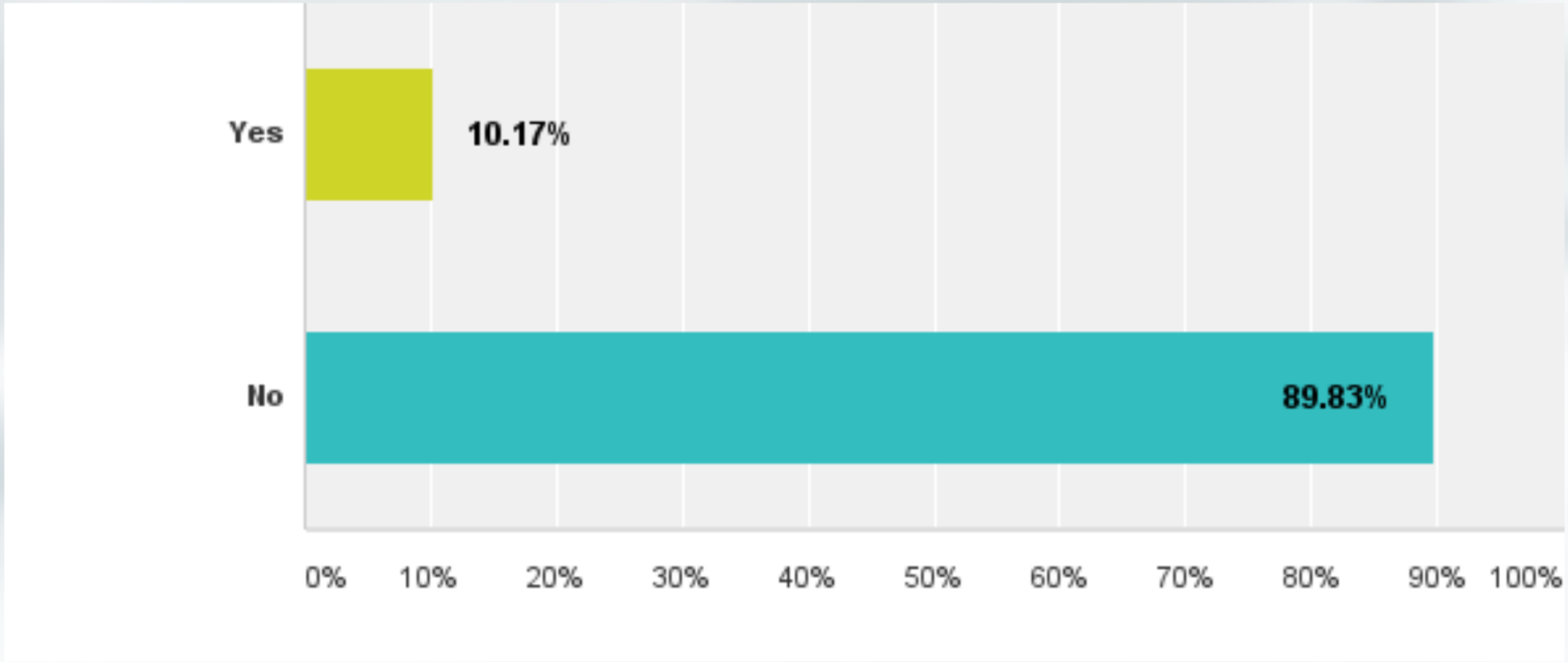
How likely is it that you would recommend BGP Flowspec to a friend or colleague?



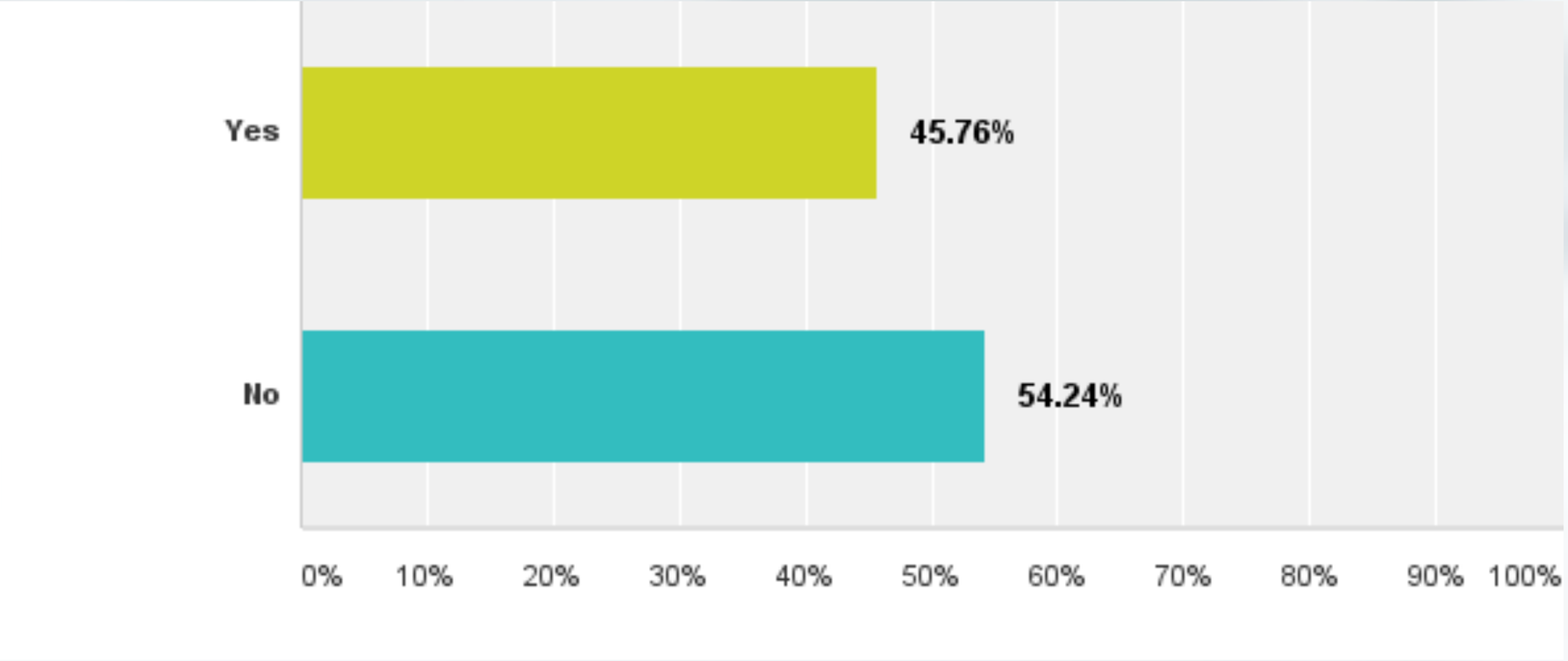
Do you allow your customers to send you BGP Flowspec routes via BGP?



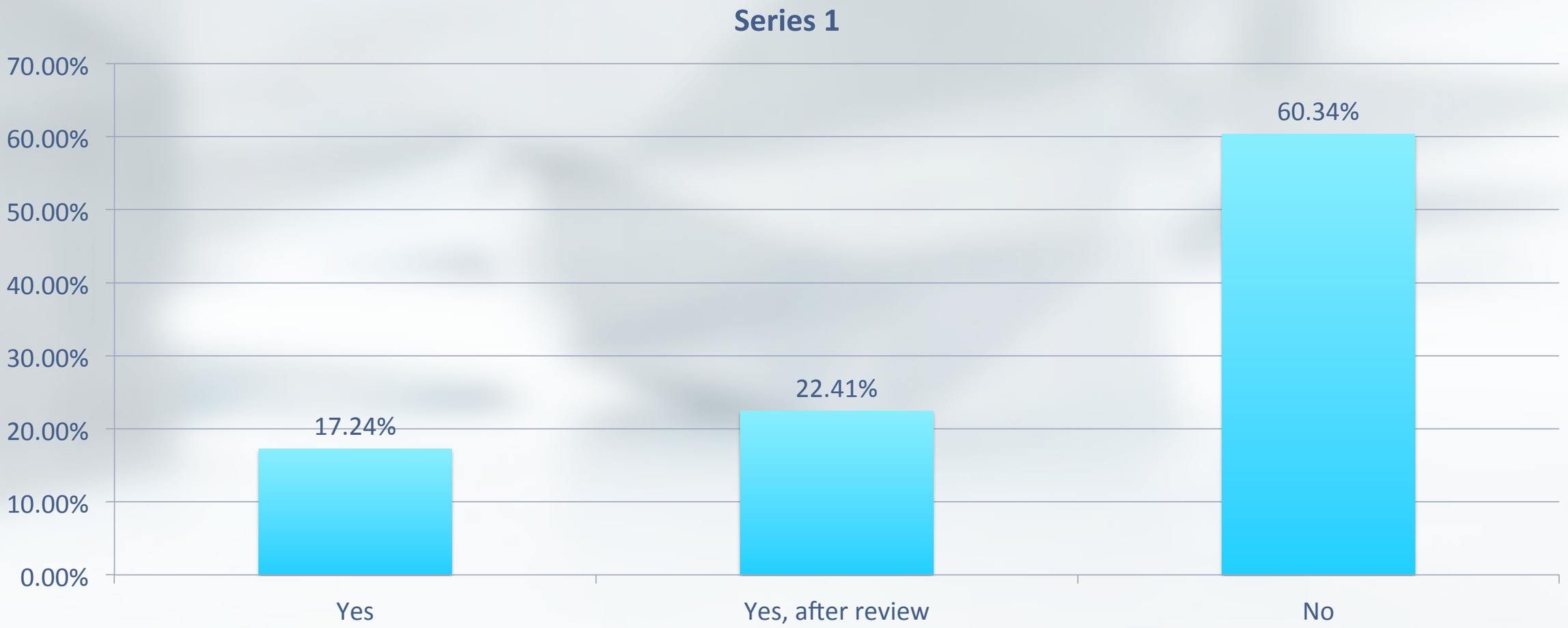
Do you have a web portal where customers can inject BGP Flowspec routes into your IBGP?



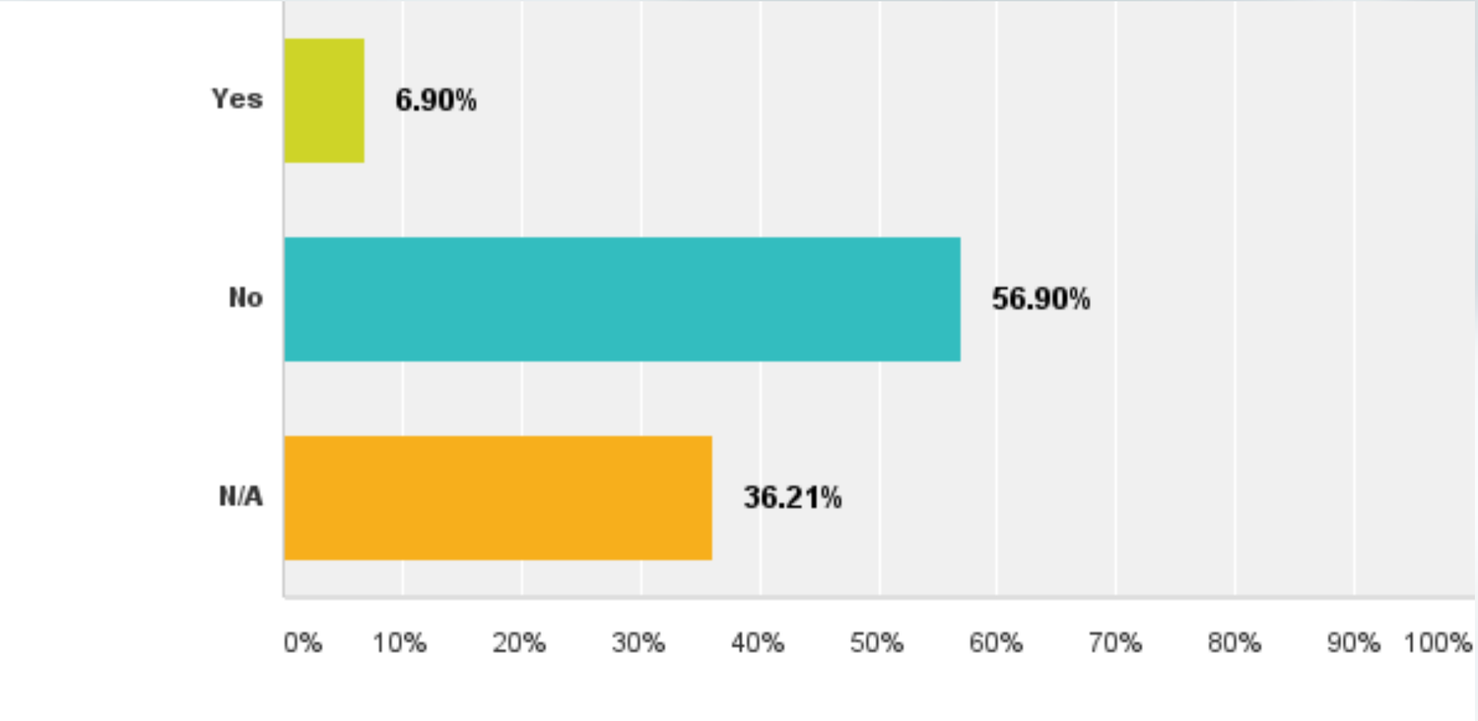
Do you have a central router from which you inject your BGP Flowspec routes?



Do you allow a DDoS detection tool (e.g. Arbor) to send BGP Flowspec routes into your IBGP?



Do you charge for DDoS mitigation using BGP Flowspec?



Summary of Comments

- Great idea and would love to see it take off but…
- Enterprises and Content Providers are waiting for ISPs to accept their Flowspec routes.
  - Some would even be willing to switch to an ISP that did this.
- ISPs are waiting for vendors to support it.
  - More vendors supporting it
  - Specific features they need for their environment
  - Better scale or stability

References

- [1] Kaspersky Lab – Every Third Public Facing Company Encounters DDoS Attacks **http://tinyurl.com/neu4zzr**
- [2] Verisign – 2014 DDoS Attack Trends **http://tinyurl.com/oujgx94**
- [3] NBC News – Internet Speeds are Rising Sharply, But So Are Hack Attacks **http://tinyurl.com/q4u2b7m**
- [4] Tech Times – DDoS Attack Cripples Sony PSN While Microsoft Deals with Xbox Live Woes **http://tinyurl.com/kkdczjx**
- [5] RFC 5575 - Dissemination of Flow Specification Rules **http://www.ietf.org/rfc/rfc5575.txt**
- [6] Cisco - Implementing BGP Flowspec **http://tinyurl.com/mm5w7mo**
- [7] Cisco – Understanding BGP Flowspec **http://tinyurl.com/l4kwb3b**

Thank You!