Atténuation des DDoS

Utilisation de BGP Flowspec

Justin Ryburn

Ingénieur système senior

Contexte

- Qui est ce type ?
  - http://www.linkedin.com/in/justinryburn
- Pourquoi ce sujet ?
  - Expérience du suivi des DDoS "à l'époque".

Les DDoS sont-ils vraiment un problème ?

"...faire tomber un site ou empêcher des transactions n'est que la partie émergée de l'iceberg. Une attaque DDoS peut entraîner des pertes de réputation ou des actions en justice pour des services non fournis."

Kaspersky Lab [1]

Verisign [2]

"Les attaques dans la catégorie des 10 Gbps et plus ont augmenté de 38 % entre le deuxième et le troisième trimestre."

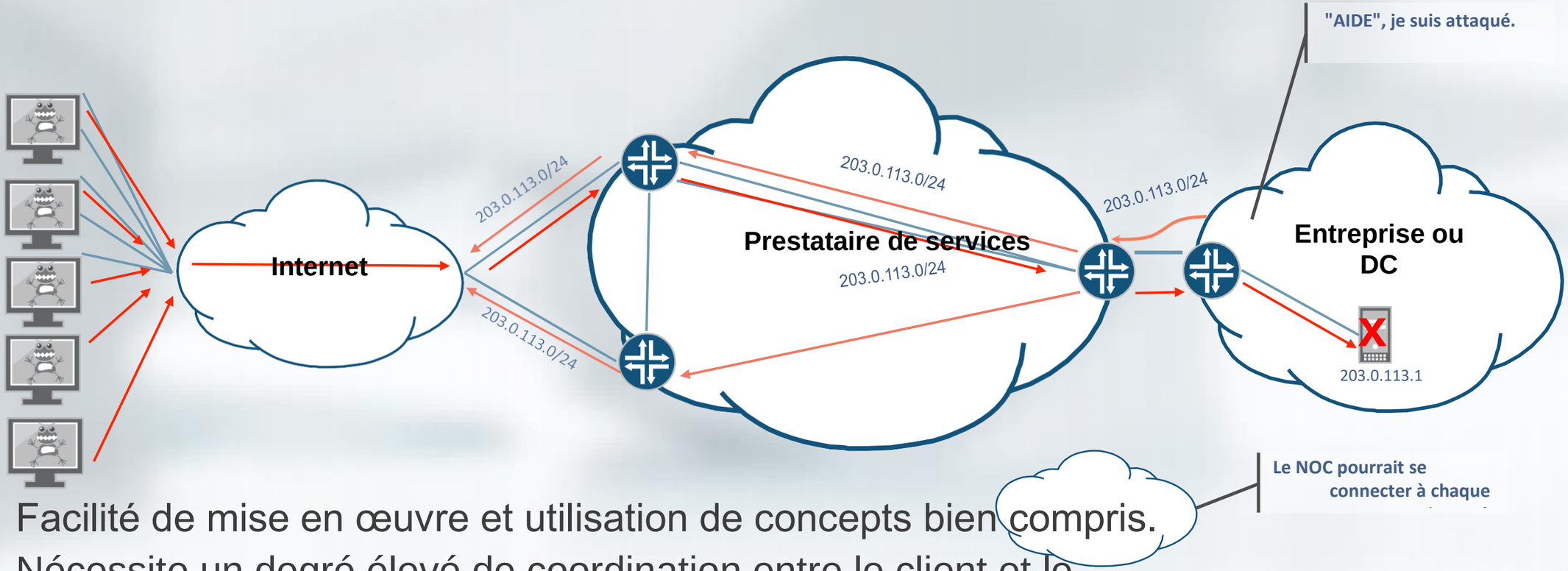
NBC News [3]

"...plus de 40 % ont estimé les pertes dues aux DDoS à plus d'un million de dollars par jour."

Tech Times [4]

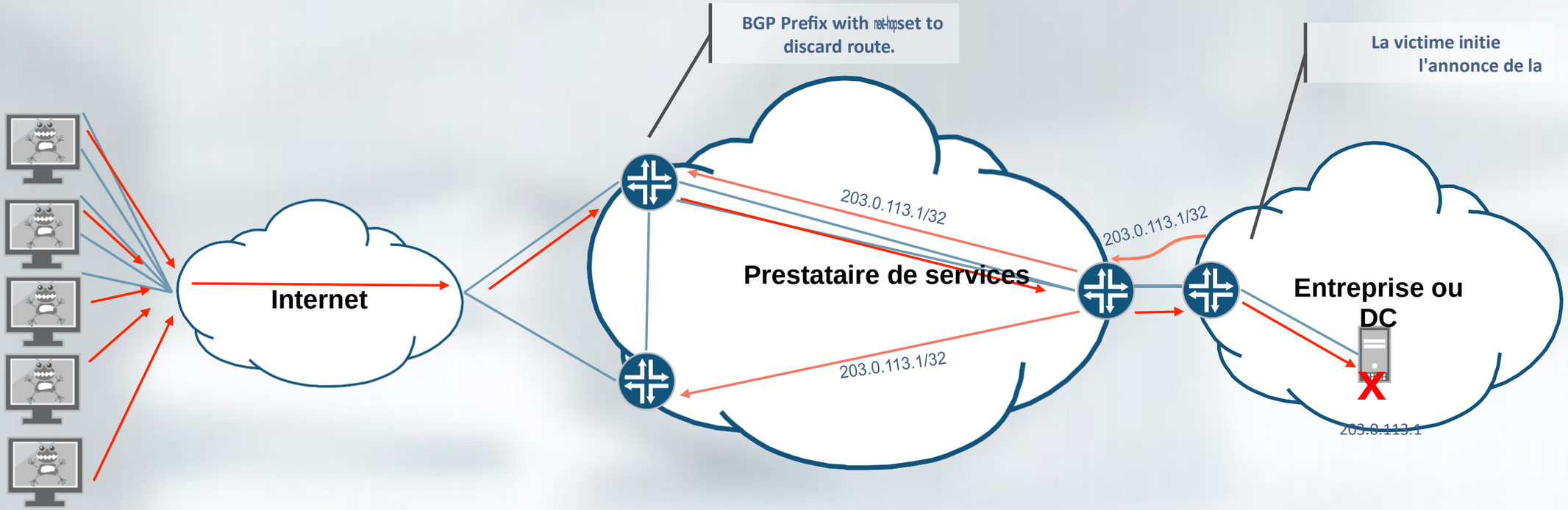
"Une attaque DDoS paralyse le PSN de Sony tandis que Microsoft s'occupe des problèmes du Xbox Live".

Bloquer les DDoS dans le "bon vieux" temps



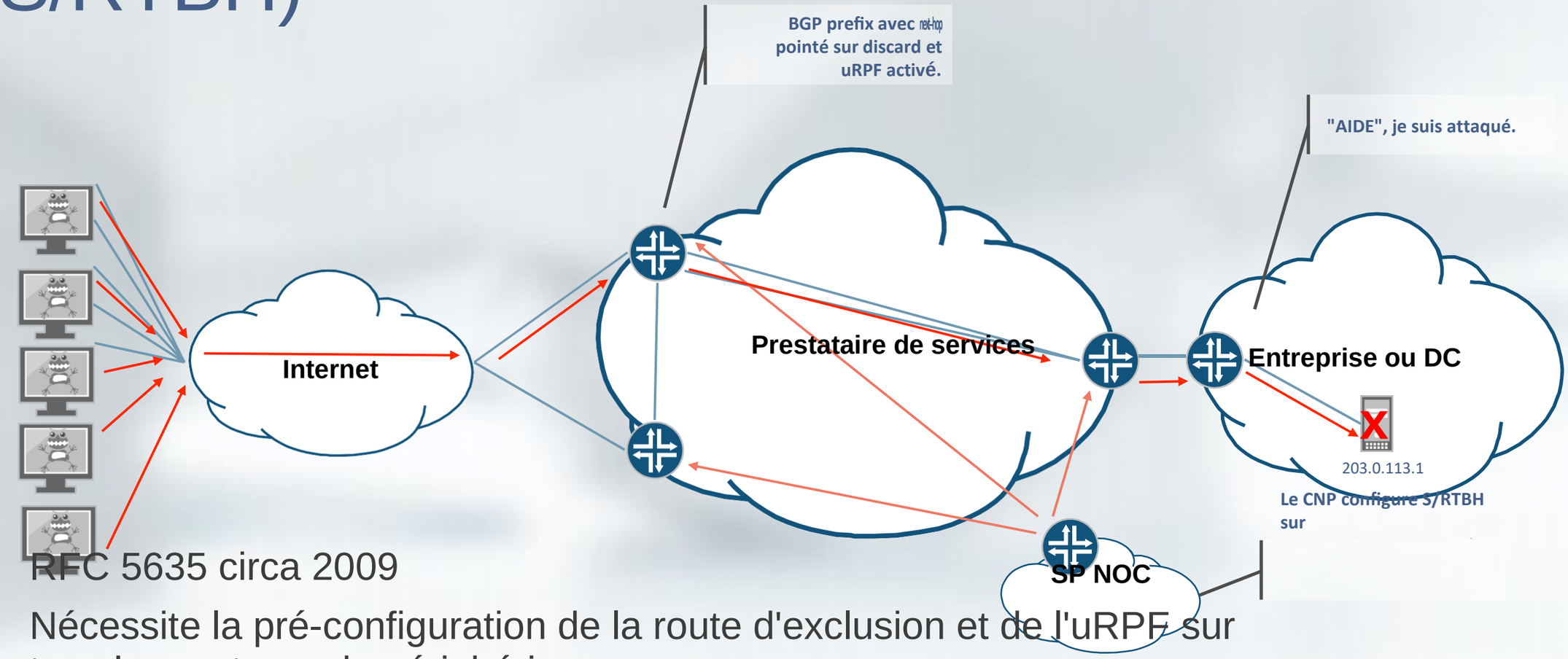
- Facilité de mise en œuvre et utilisation de concepts bien compris.
- Nécessite un degré élevé de coordination entre le client et le fournisseur.
- Il est difficile de faire évoluer le périmètre d'un grand réseau.
- Mauvaise configuration possible et coûteuse

Trou noir déclenché à distance par la destination (D/RTBH)



- RFC 3882 circa 2004
- Nécessite la pré-configuration de la route de rejet sur tous les routeurs de périphérie
- L'adresse de destination de la victime est totalement inaccessible mais l'attaque (et les dommages collatéraux) est arrêtée.

Trou noir déclenché à distance par la source (S/RTBH)



- RFC 5635 circa 2009
- Nécessite la pré-configuration de la route d'exclusion et de l'uRPF sur tous les routeurs de périphérie.
- L'adresse de destination de la victime est encore utilisable.
- Ne fonctionne que pour une source unique (ou un petit nombre).

Spécification du flux BGP

- Des informations spécifiques sur un flux peuvent maintenant être distribuées à l'aide d'un NLRI BGP défini dans la RFC 5575 [5] vers 2009.
  - AFI/SAFI = 1/133 : Applications de filtrage du trafic unicast
  - AFI/SAFI = 1/134 : Applications de filtrage du trafic VPN
- Les routes de flux sont automatiquement validées par rapport aux informations de routage unicast ou via le cadre de politique de routage.
  - Doit appartenir au préfixe de monodiffusion le plus long.
- Une fois validé, le filtre du pare-feu est créé sur la base des critères de correspondance et d'action.

Spécification du flux BGP

- BGP Flowspec peut inclure les informations suivantes :
  - Type 1 - Préfixe de destination
  - Type 2 - Préfixe de la source
  - Type 3 - Protocole IP
  - Type 4 - Port source ou destination
  - Type 5 - Port de destination
  - Type 6 - Port source
  - Type 7 - Type ICMP
  - Type 8 - Code ICMP
  - Type 9 - drapeaux TCP
  - Type 10 - Longueur du paquet
  - Type 11 - DSCP
  - Type 12 - Codage des fragments

Spécification du flux BGP

- Les actions sont définies à l'aide des communautés étendues BGP :
  - 0x8006 - traffic-rate (défini à 0 pour abandonner tout le trafic)
  - 0x8007 - traffic-action (échantillonnage)
  - 0x8008 - redirection vers le VRF (route target)
  - 0x8009 - marquage du trafic (valeur DSCP)

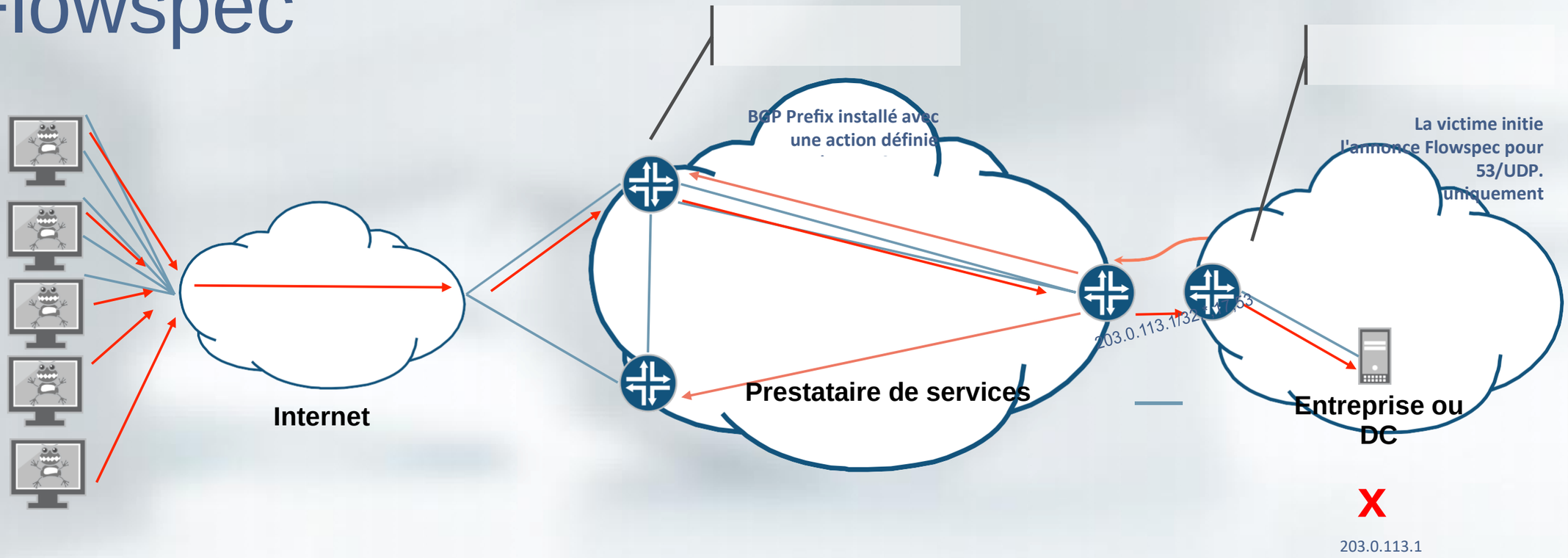
Soutien aux fournisseurs

- Fournisseurs de détection des DDoS :
  - Arbor Peakflow SP 3.5
  - Juniper DDoS Secure 5.14.2-0
- Vendeurs de routeurs :
  - Alcatel-Lucent SR OS 9.0R1
  - Juniper JUNOS 7.3
  - Cisco 5.2.0 pour ASR et CRS [6].

Qu'est-ce qui rend BGP Flowspec meilleur ?

- Même granularité que les ACL
  - Basé sur la correspondance de n-tuple
    - Même automatisation que la RTBH
      - Il est beaucoup plus facile de propager les filtres à tous les routeurs de périphérie dans les grands réseaux.
    - Tirer parti des meilleures pratiques et des contrôles de politique de BGP
      - Le même filtrage et les meilleures pratiques utilisés pour RTBH peuvent être appliqués à BGP Flowspec.

Atténuation des DDoS inter-domaines à l'aide de Flowspec



- Permet au client du FAI d'initier le filtre.
- Nécessite un filtrage sain à la périphérie du client.

Configuration du routeur de bordure

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
```

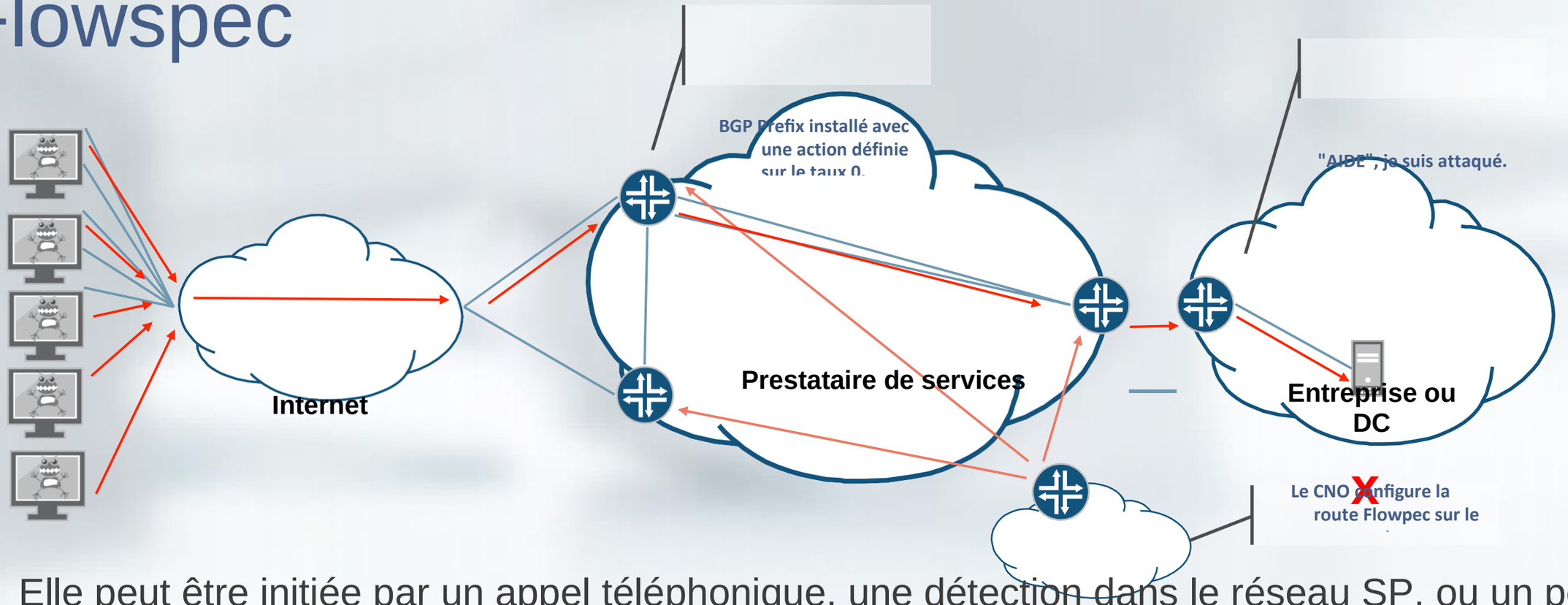
Cisco [7]

```
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;
    }
}
```

Atténuation des DDoS intra-domaine à l'aide de Flowspec



- Elle peut être initiée par un appel téléphonique, une détection dans le réseau SP, ou un portail web pour le client.
- Nécessite une coordination entre le client et le fournisseur.

Configuration du routeur de bordure

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;
    }
}
```

Configuration du serveur de routes

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;
            }
        }
    }
}
```

Configuration du serveur de routes

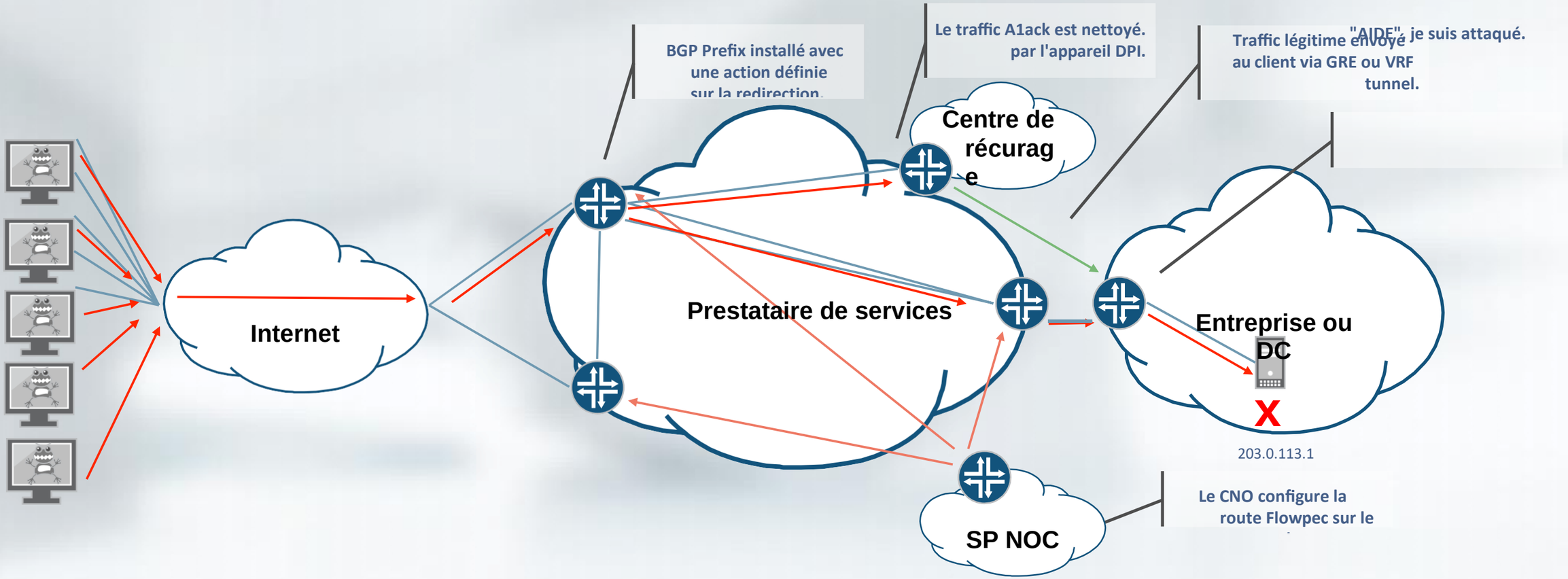
Cisco [7]

```
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;
    }
}
```

Atténuation des DDoS grâce à Scrubbing Center



- Elle peut être initiée par un appel téléphonique, une détection dans le réseau SP, ou un portail web pour le client.
- Permet d'atténuer les attaques de la couche applicative sans mener à bien l'attaque.

Configuration du routeur de bordure

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;
    }
}
```

Configuration du serveur de routes

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;
            }
        }
    }
}
```

Configuration du serveur de routes

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;
        }
    }
}
```

Comment savoir si ça marche ?

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

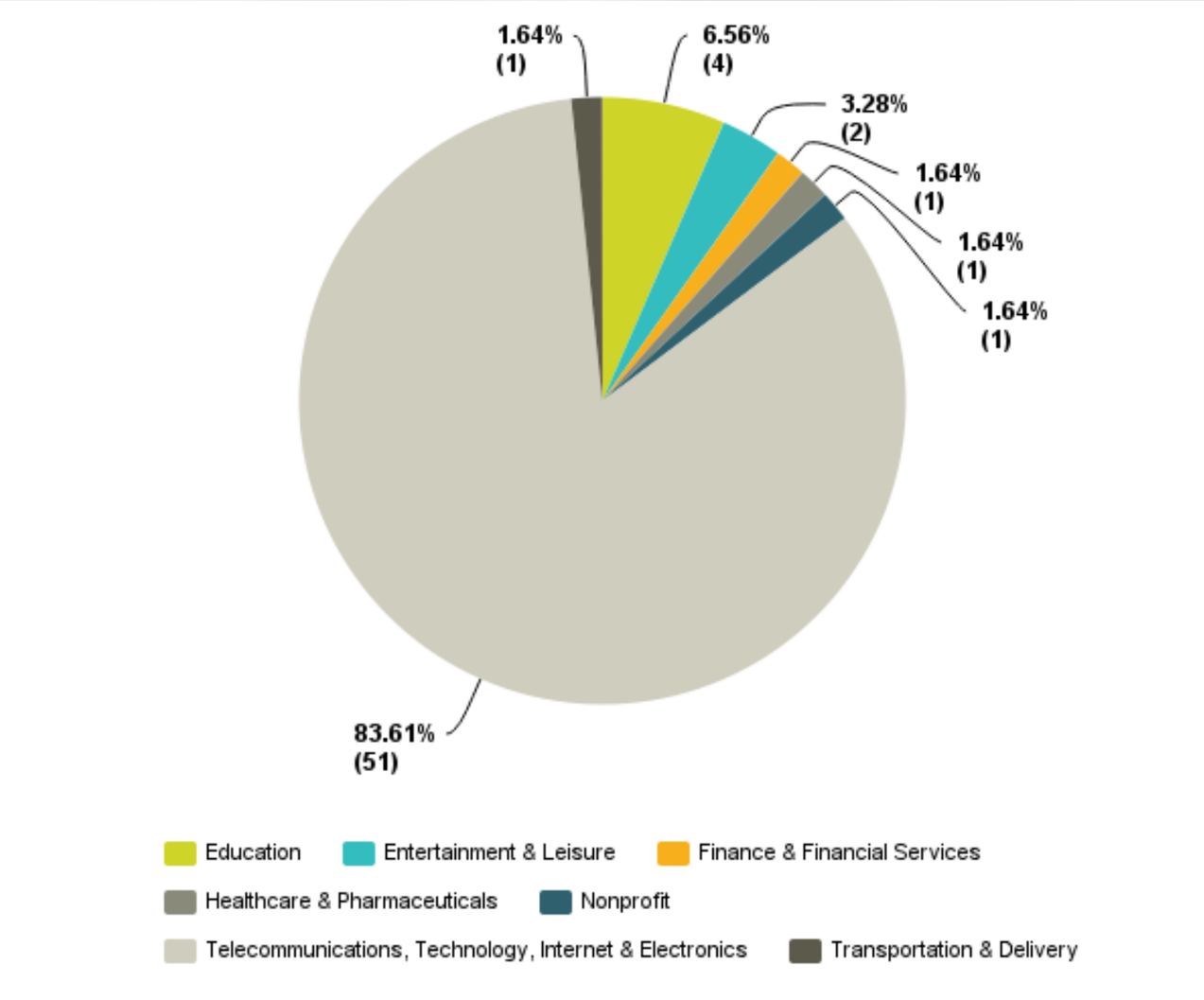
- show bgp neighbor <neighbor> | match inet-flow
- show route table inetflow.0 extensive
- show firewall filter __flowspec_default_inet__

Où allons-nous ?

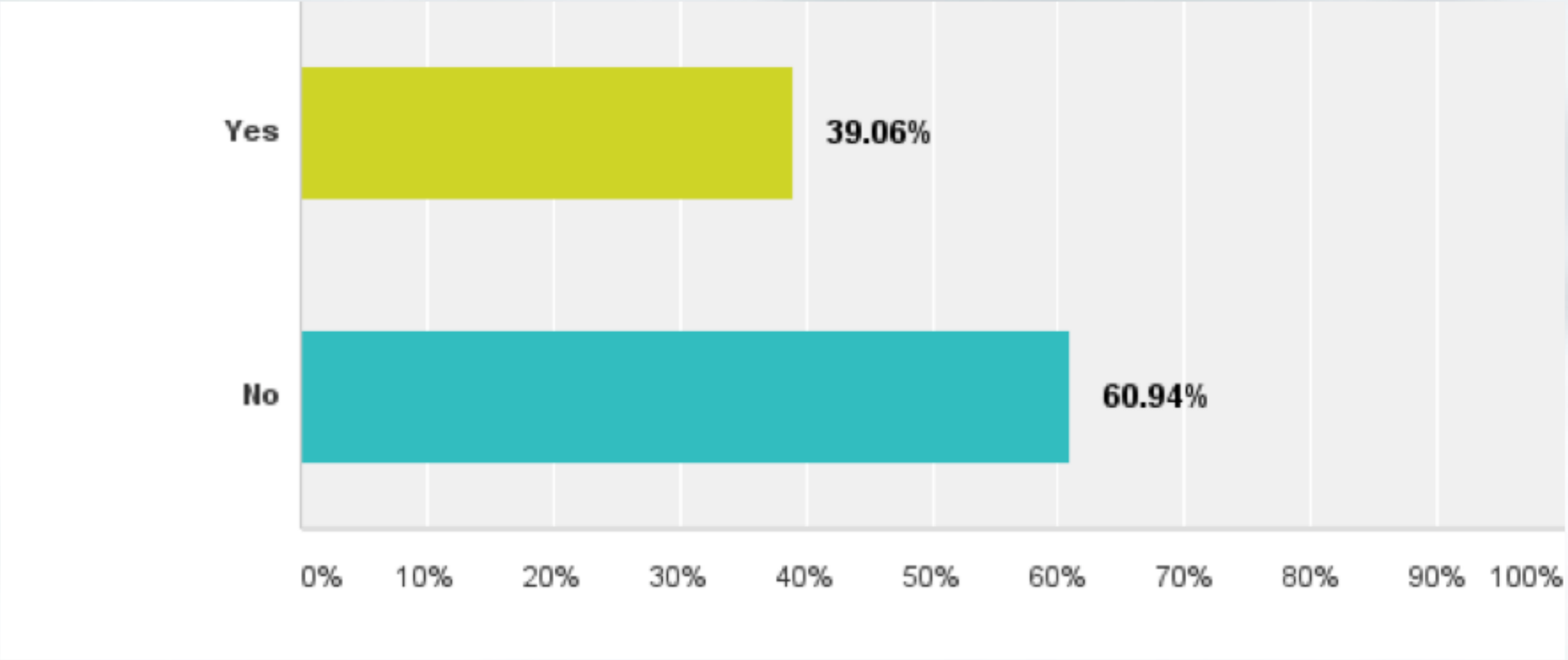
- Support IPv6
  - http://tools.ietf.org/html/draft-ietf-idr-flow-spec-v6-03
- Assouplir la validation
  - http://tools.ietf.org/html/draft-ietf-idr-bgp-flowspec-oid-00
- Redirection vers l'action IP Next-Hop
  - http://tools.ietf.org/html/draft-simpson-idr-flowspec-redirect-02

État de l'Union

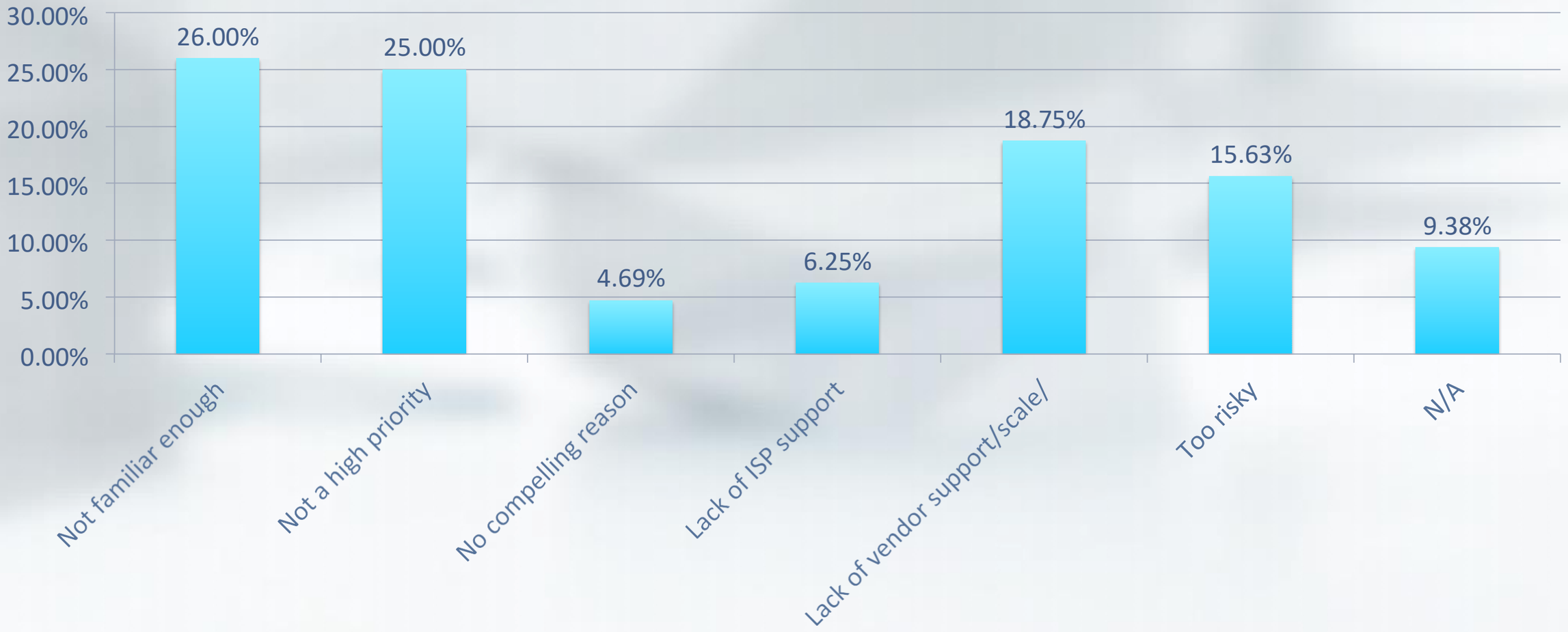
Les industries réagissent



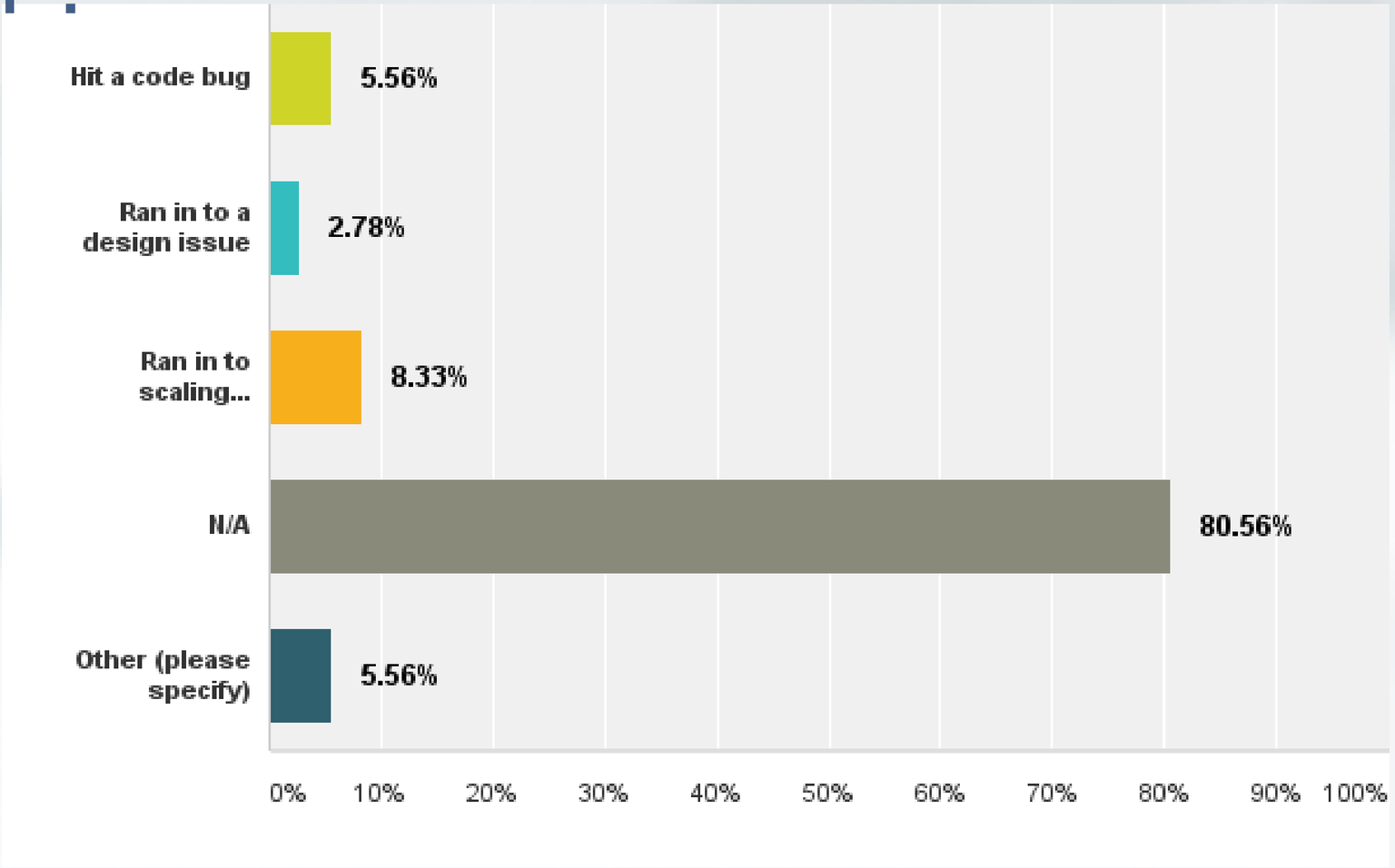
Avez-vous, ou avez-vous déjà eu, BGP Flowspec activé dans une partie de votre réseau ?



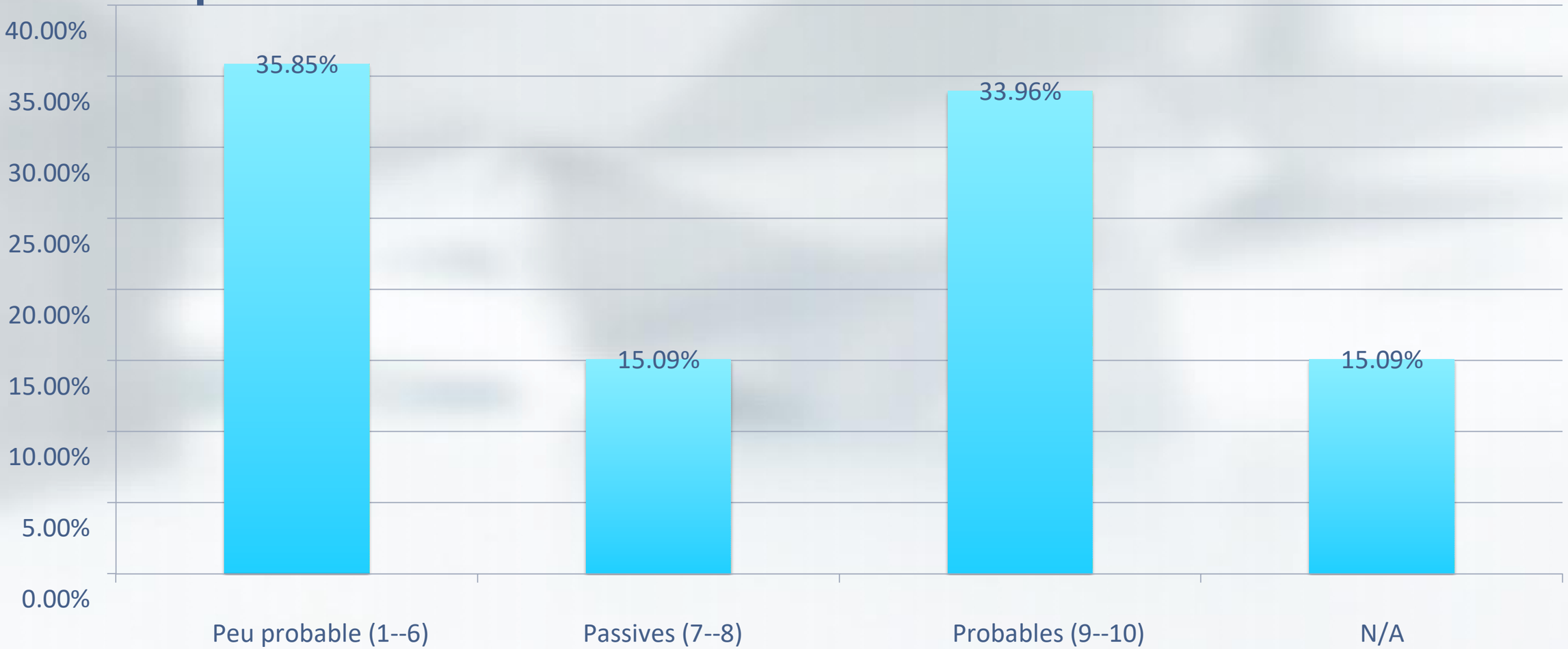
Si vous ne l'avez pas activé, pourquoi pas ?



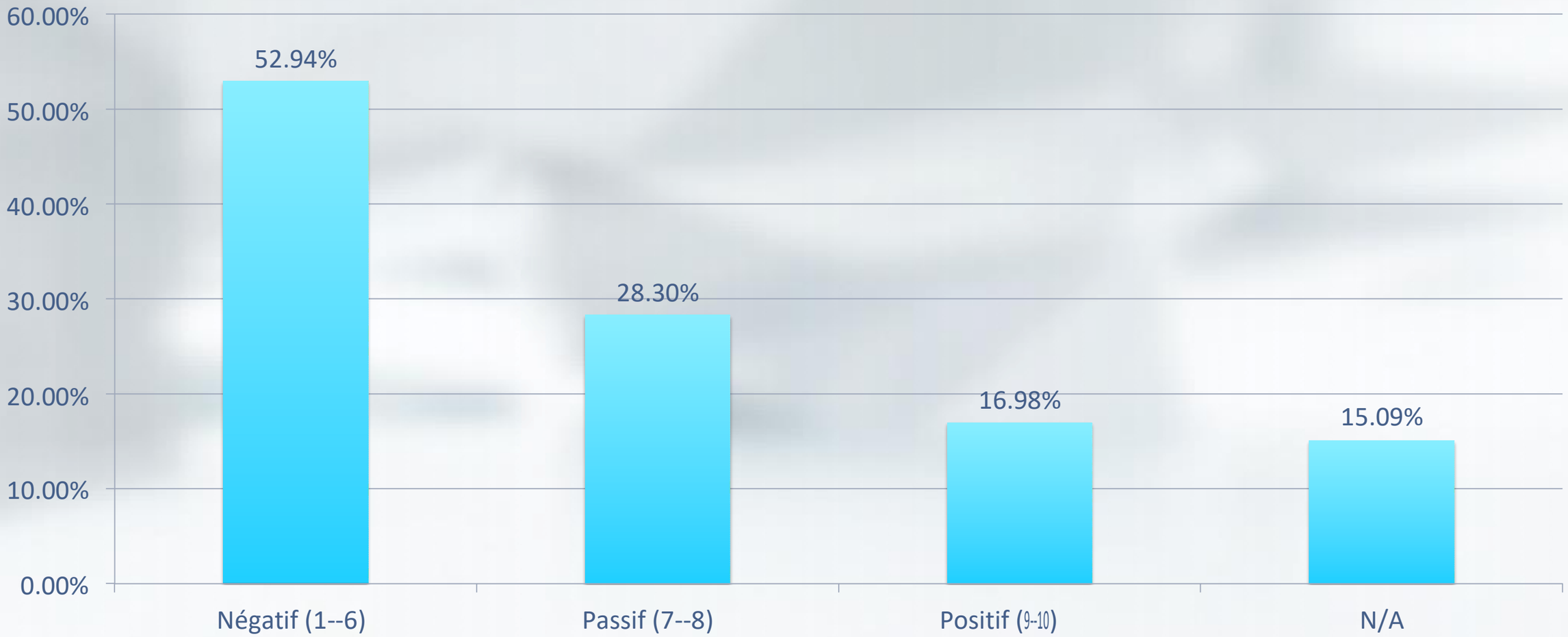
Si vous l'avez activé mais l'avez désactivé depuis, pourquoi ?



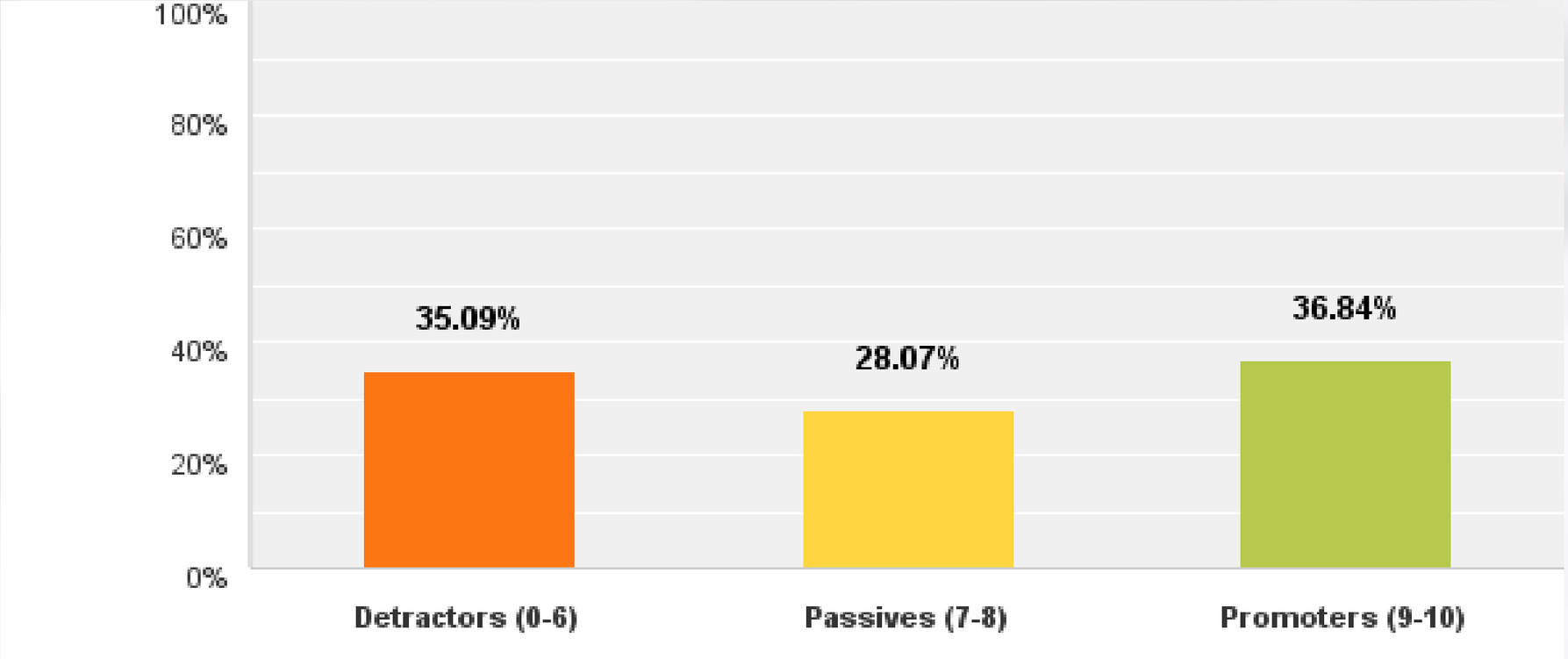
Si vous ne l'avez pas activé actuellement, quelle est la probabilité que vous activiez BGP Flowspec dans le futu



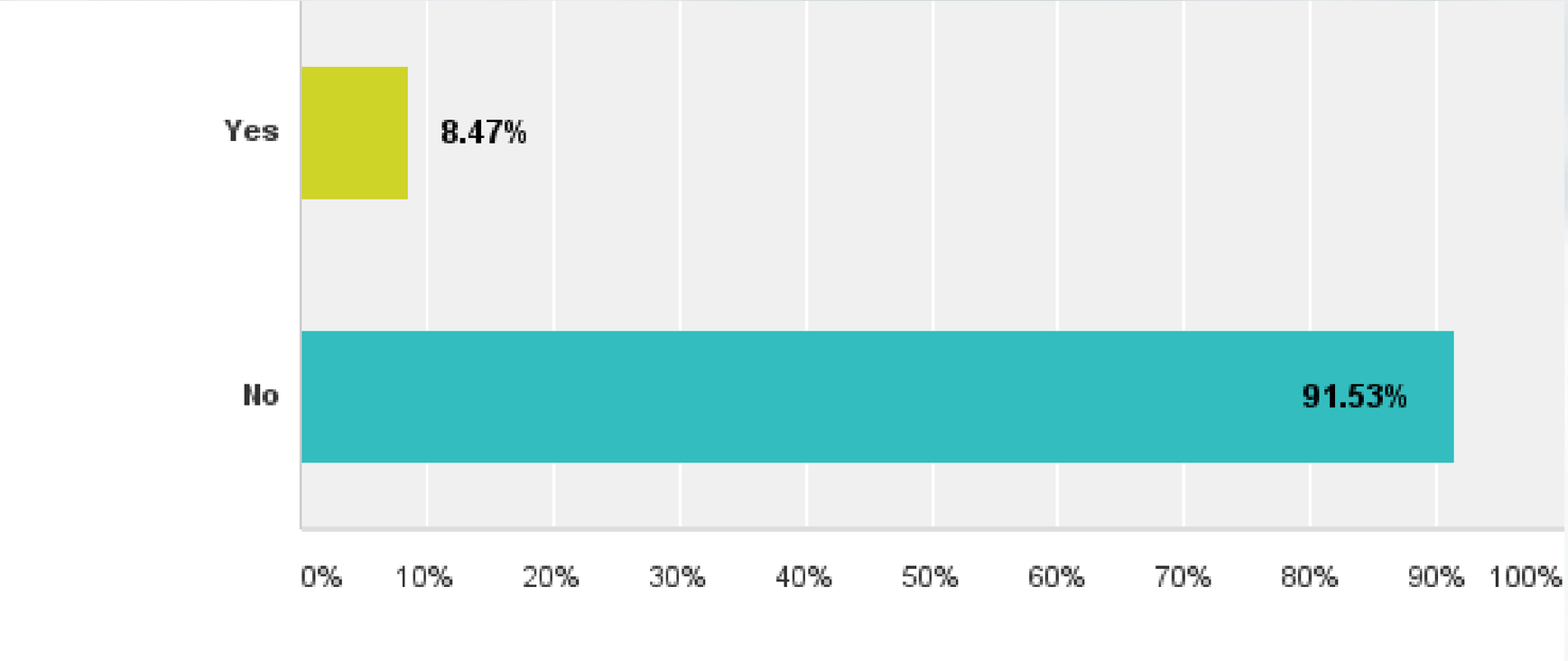
Globalement, comment évaluez-vous votre expérience avec BGP Flowpsec ?



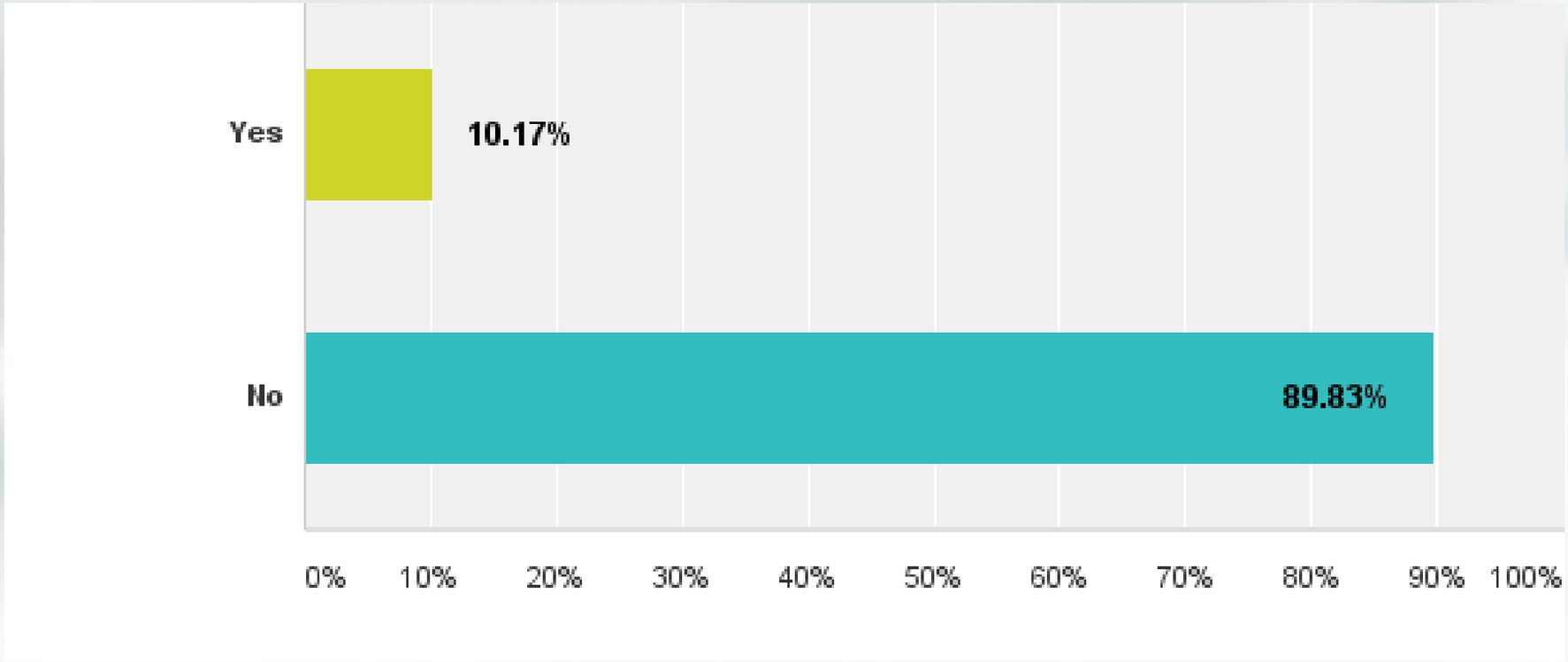
Dans quelle mesure est-il probable que vous recommandiez BGP Flowspec à un ami ou un collègue ?



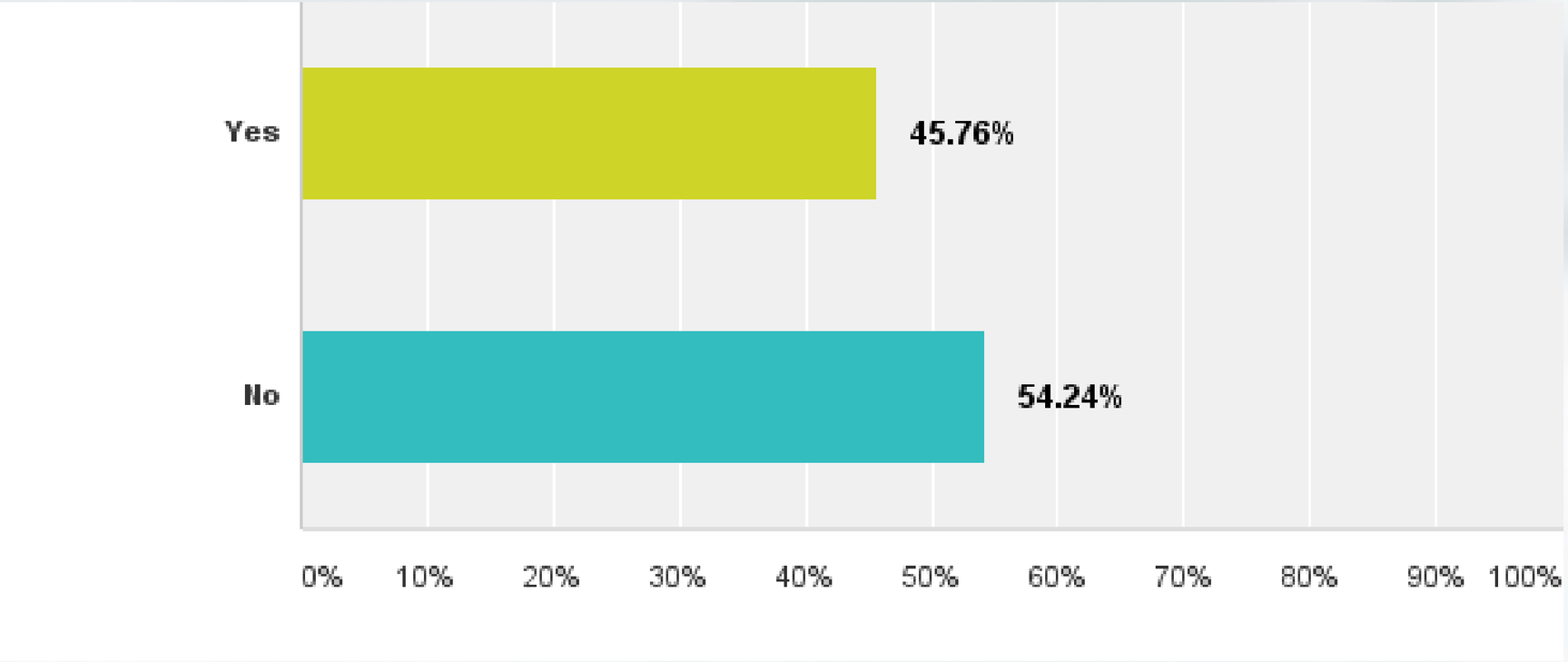
Autorisez-vous vos clients à vous envoyer des routes BGP Flowspec via BGP ?



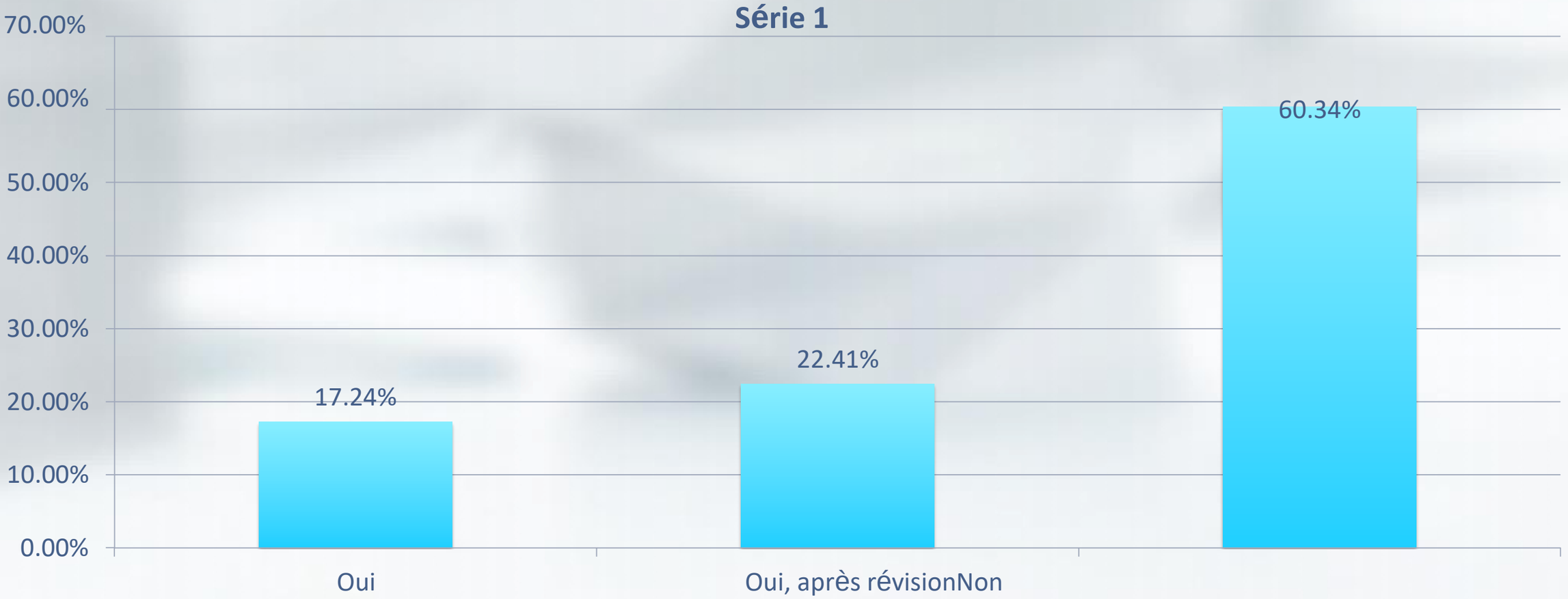
Avez-vous un portail web où les clients peuvent injecter des routes BGP Flowspec dans votre IBGP ?



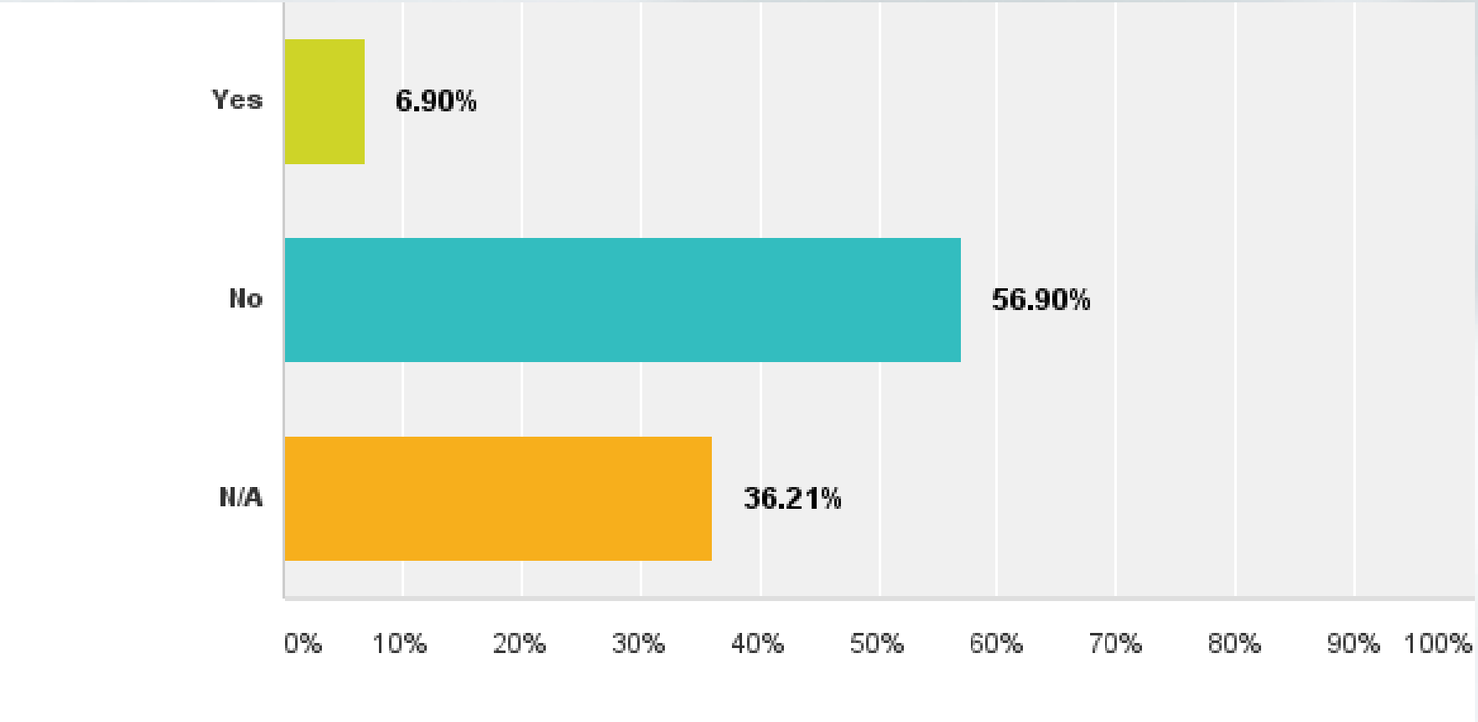
Avez-vous un routeur central à partir duquel vous injectez vos routes BGP Flowspec ?



Autorisez-vous un outil de détection DDoS (par exemple Arbor) à envoyer des routes BGP Flowspec dans votre IBGP ?



Facturez-vous l'atténuation des DDoS en utilisant BGP Flowspec ?



Résumé des commentaires

- Excellente idée et j'aimerais la voir décoller, mais...
- Les entreprises et les fournisseurs de contenu attendent que les FAI acceptent leurs routes Flowspec.
  - Certains seraient même prêts à passer à un fournisseur d'accès Internet qui le ferait.
- Les FAI attendent que les fournisseurs le prennent en charge.
  - Plus de vendeurs le supportent
  - Caractéristiques spécifiques dont ils ont besoin pour leur environnement
  - Meilleure échelle ou stabilité

Références

- 1] Kaspersky Lab - Une entreprise publique sur trois subit des attaques DDoS **http://tinyurl.com/neu4zzr**
- 2] Verisign - 2014 DDoS Attack Trends **http://tinyurl.com/oujgx94 (en anglais)**
- 3] NBC News - Les vitesses d'Internet augmentent fortement, mais les attaques par piratage aussi. **http://tinyurl.com/q4u2b7m**
- 4] Tech Times - Une attaque DDoS paralyse le PSN de Sony tandis que Microsoft s'occupe des problèmes du Xbox Live **http://tinyurl.com/kkdczjx**
- 5] RFC 5575 - Diffusion des règles de spécification de flux. **http://www.ietf.org/rfc/rfc5575.txt**
- [6] Cisco - Mise en œuvre de BGP Flowspec **http://tinyurl.com/mm5w7mo**
- [7] Cisco - Comprendre BGP Flowspec **http://tinyurl.com/l4kwb3b**

Merci !