Mitigación de DDoS

Uso de BGP Flowspec

Justin Ryburn

Ingeniero de Sistemas Senior

Antecedentes

- ¿Quién es este tipo?
  - http://www.linkedin.com/in/justinryburn
- ¿Por qué este tema?
  - Experiencia en el seguimiento de DDoS "en su día".

¿Es realmente un problema el DDoS?

"...tumbar un sitio o impedir las transacciones es sólo la punta del iceberg. Un DDoS el ataque puede provocar pérdidas de reputación o reclamaciones legales por servicios no prestados".

Kaspersky Lab [1]

Verisign [2]

"Ataques en los sectores de 10 Gbps y categoría superior creció un 38% de Q2 ... Q3".

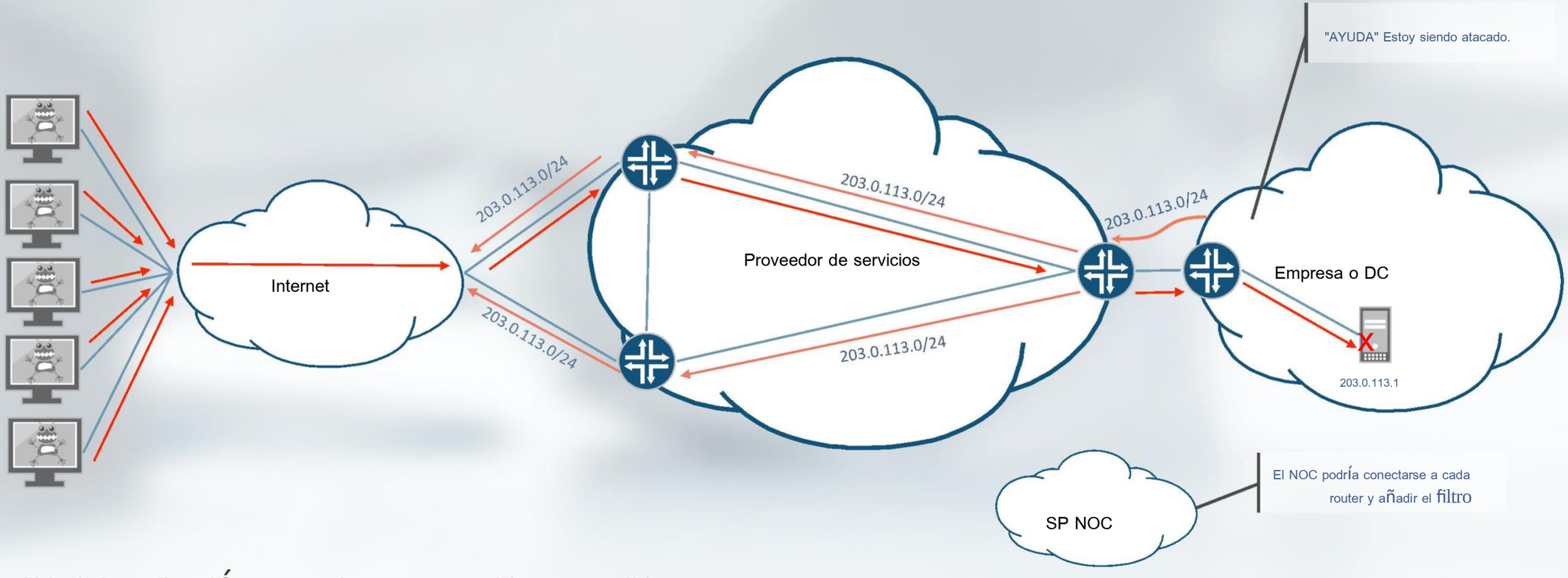
NBC News [3]

"...más del 40 por ciento estimó las pérdidas por DDoS en más de un millón de dólares al día".

Tech Times [4]

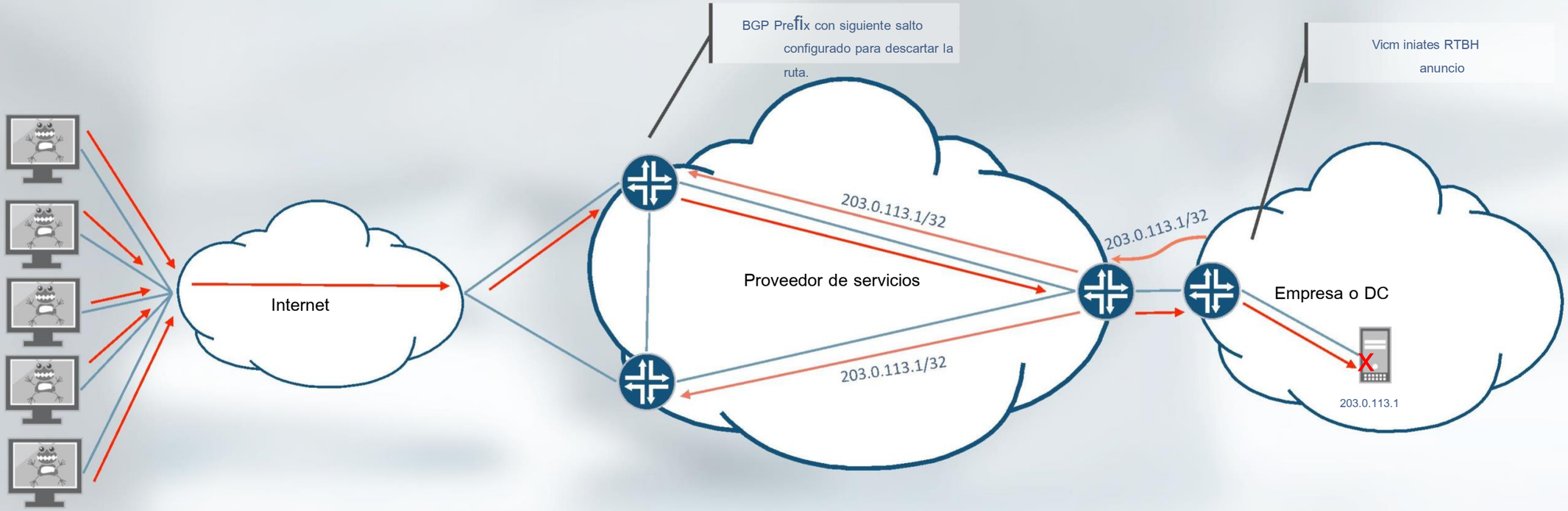
"El ataque DDoS paraliza a Sony PSN mientras Microsoft se ocupa de los problemas de Xbox Live"

Bloqueo de DDoS en los "viejos" tiempos



- Facilidad de aplicación y uso de conceptos bien entendidos
- Requiere un alto grado de coordinación entre el cliente y el proveedor
- Es difícil de escalar en un gran perímetro de red
- Posible y costoso error de configuración

Destino del agujero negro disparado a distancia (D/RTBH)

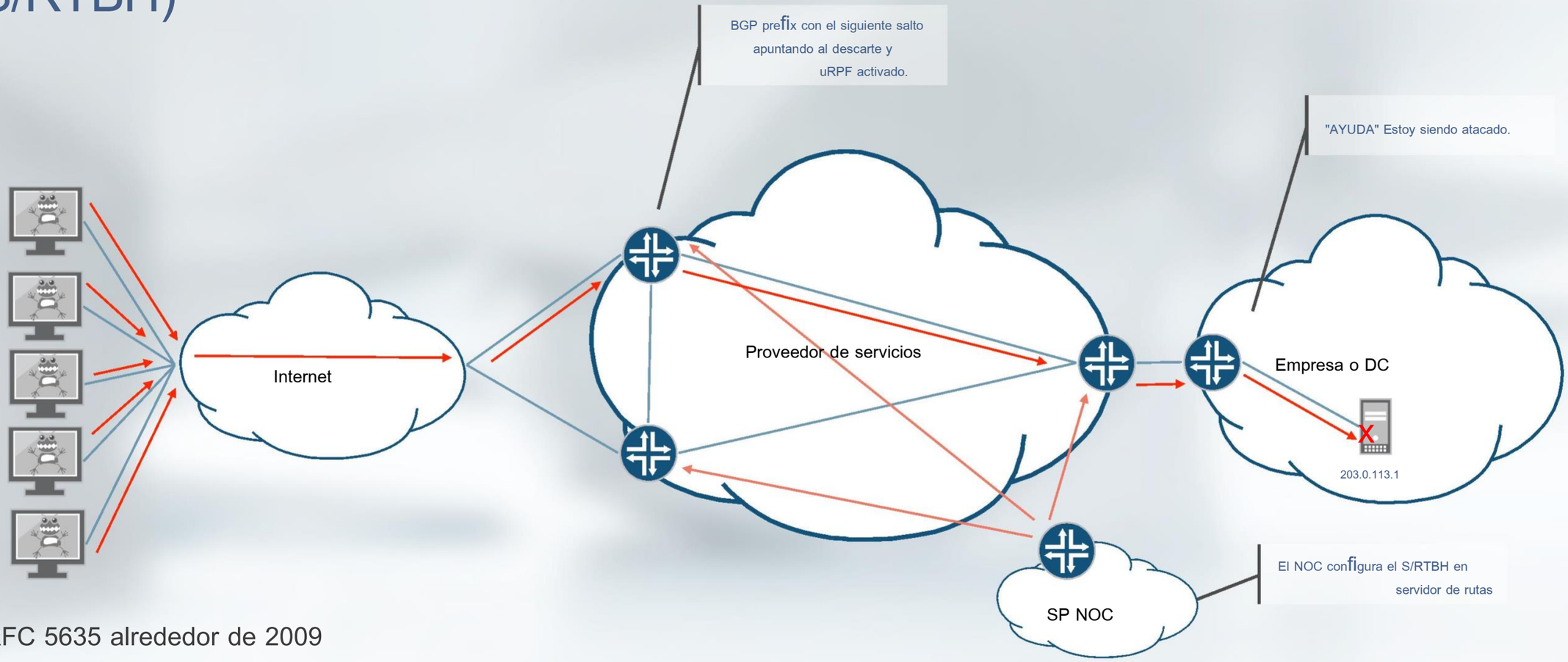


- RFC 3882 alrededor de 2004

- Requiere la preconfiguración de la ruta de descarte en todos los routers de borde

- La dirección de destino de la víctima es completamente inalcanzable pero el ataque (y los daños colaterales) es se detuvo.[5]

Fuente Agujero Negro Disparado a Distancia (S/RTBH)



- RFC 5635 alrededor de 2009
- Requiere la preconfiguración de la ruta de descarte y uRPF en todos los routers de borde
- La dirección de destino de la víctima sigue siendo utilizable
- Sólo funciona para una única (o pequeña) fuente.

Especificación de flujo BGP

- Ahora se puede distribuir información específica sobre un flujo utilizando un BGP NLRI definido en el RFC 5575 [5] hacia 2009

  - AFI/SAFI = 1/133: Aplicaciones de filtrado de tráfico unicast
  - AFI/SAFI = 1/134: Aplicaciones de filtrado de tráfico VPN

- Las rutas de flujo se validan automáticamente con el enrutamiento unicast información o a través del marco de la política de enrutamiento.

  - Debe pertenecer al prefijo unicast de mayor coincidencia.

- Una vez validado, se crea un filtro de cortafuegos basado en la coincidencia y la acción criterios.

EspecificaciÓn de flujo BGP

- BGP Flowspec puede incluir la siguiente informaciÓn:
  - Tipo 1 - Prefijo de destino
  - Tipo 2 - Prefijo de origen
  - Tipo 3 - Protocolo IP
  - Tipo 4 - Puerto de origen o destino
  - Tipo 5 - Puerto de destino
  - Tipo 6 - Puerto de origen
  - Tipo 7 - Tipo ICMP
  - Tipo 8 - CÓdigo ICMP
  - Tipo 9 - banderas TCP
  - Tipo 10 - Longitud del paquete
  - Tipo 11 - DSCP
  - Tipo 12 - CodificaciÓn de fragmentos

Especificación de flujo BGP

- Las acciones se definen utilizando las comunidades extendidas de BGP:
  - 0x8006 - traffic-rate (configurado a 0 para dejar caer todo el tráfico)
  - 0x8007 - tráfico-acción (muestreo)
  - 0x8008 - redirigir a VRF (objetivo de ruta)
  - 0x8009 - marca de tráfico (valor DSCP)

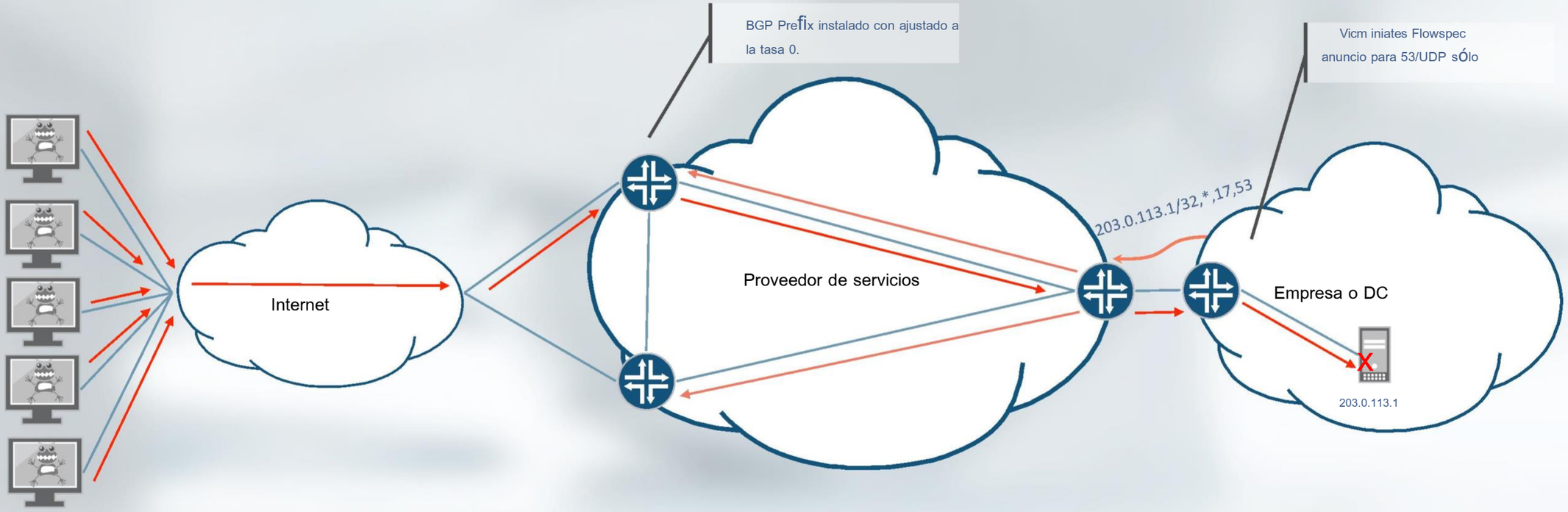
Apoyo a los proveedores

- Proveedores de detecciÓn de DDoS:
  - Arbor Peakflow SP 3.5
  - Juniper DDoS Secure 5.14.2-0
- Vendedores de routers:
  - Alcatel-Lucent SR OS 9.0R1
  - Juniper JUNOS 7.3
  - Cisco 5.2.0 para ASR y CRS [6]

¿Qué hace que BGP Flowspec sea mejor?

- La misma granularidad que las ACL
  - Basado en la coincidencia de n-tuplas
- La misma automatización que RTBH
  - Es mucho más fácil propagar los filtros a todos los routers de borde en redes grandes
- Aprovecha las mejores prácticas y controles de políticas de BGP
  - El mismo filtrado y las mejores prácticas utilizadas para RTBH pueden aplicarse a BGP Flowspec

MitigaciÓn de DDoS entre dominios mediante Flowspec



- Permite que el cliente del ISP inicie el filtro.
- Requiere un filtrado sano en el borde del cliente.

ConfiguraciÓn del router de borde

Alcatel-Lucent

```
router
        sistema autÓnomo 64496
        bgp
                grupo "CUST-FLOWSPEC"
                        vecino 192.0.2.1
                                familia ipv4 flow-ipv4
                                peer-as 64511
                                no flowspec-validate
                        salir
                salir
                no hay cierre
        salir
Salir
```

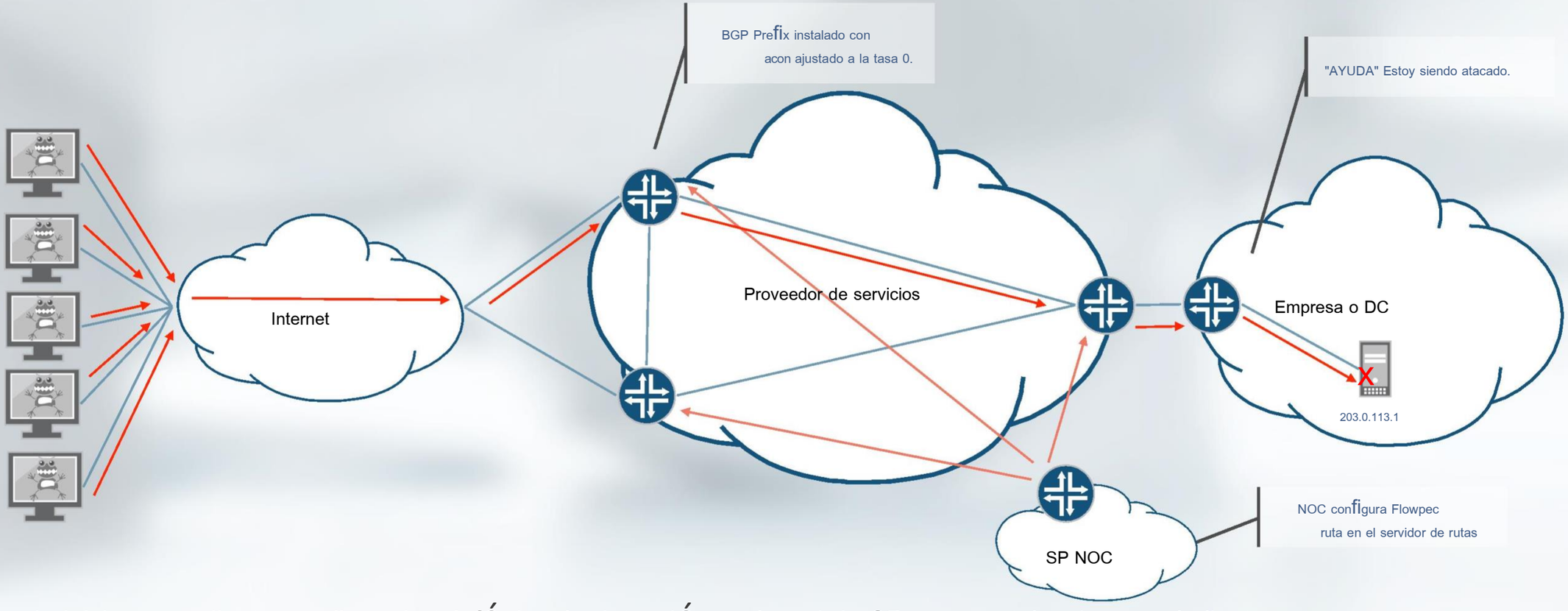
Cisco [7]

```
router bgp 64496
    ! Inicializa la familia de direcciones global
    address-family ipv4 flowspec
!
    vecino 192.0.2.1
        remote-as 64511
        ! Lo vincula a una configuraciÓn vecina
        address-family ipv4 flowspec
```

Juniper

```
protocolos {
        bgp {
                grupo CUST-FLOWSPEC {
                        peer-as 64511;
                        vecino 192.0.2.1 {
                                familia inet {
                                        flujo;
                                }
                        }
                }
        }
}
opciones de enrutamiento {
        flujo {
                norma de orden temporal;
        }
}
```

MitigaciÓn de DDoS dentro del dominio utilizando Flowspec



- Puede iniciarse mediante una llamada telefÓnica, la detecciÓn en la red de SP o un portal web para el cliente.

- Requiere la coordinaciÓn entre el cliente y el proveedor.

ConfiguraciÓn del router de borde

Alcatel-Lucent

```
router
        sistema autÓnomo 64496
        bgp
                grupo "RR-CLIENT-FLOWSPEC"
                        vecino 198.51.100.1
                                familia ipv4 flow-ipv4
                                peer-as 64496
                        salir
                salir
                no hay cierre
        salir
salir
```

Cisco [7]

```
router bgp 64496
    ! Inicializa la familia de direcciones global
    address-family ipv4 flowspec
!
    vecino 198.51.100.1
        remote-as 64496
        ! Lo vincula a una configuraciÓn vecina
        address-family ipv4 flowspec
```

Juniper

```
protocolos {
        bgp {
                grupo RR-CLIENT-FLOWSPEC {
                        tipo interno;
                        vecino 198.51.100.1 {
                                familia inet {
                                        flujo;
                                }
                        }
                }
        }
}
opciones de enrutamiento {
        flujo {
                norma de orden temporal;
        }
}
```

ConfiguraciÓn del servidor de rutas

Alcatel-Lucent

```
router
        sistema autÓnomo 64496
        bgp
                grupo "RR-CLIENT-FLOWSPEC"
                        vecino 198.51.100.2
                                familia ipv4 flow-ipv4
                                peer-as 64496
                        salir
                salir
                no hay cierre
        salir
salir
```

Cisco [7]

```
router bgp 64496
    ! Inicializa la familia de direcciones global
    address-family ipv4 flowspec
!
    vecino 198.51.100.2
        remote-as 64496
        ! Lo vincula a una configuraciÓn vecina
        address-family ipv4 flowspec
```

Juniper

```
protocolos {
        bgp {
                grupo RR-CLIENT-FLOWSPEC {
                        tipo interno;
                        vecino 198.51.100.2 {
                                familia inet {
                                        flujo;
                                }
                                export FLOWROUTES_OUT;
                        }
                }
        }
}
```

ConfiguraciÓn del servidor de rutas

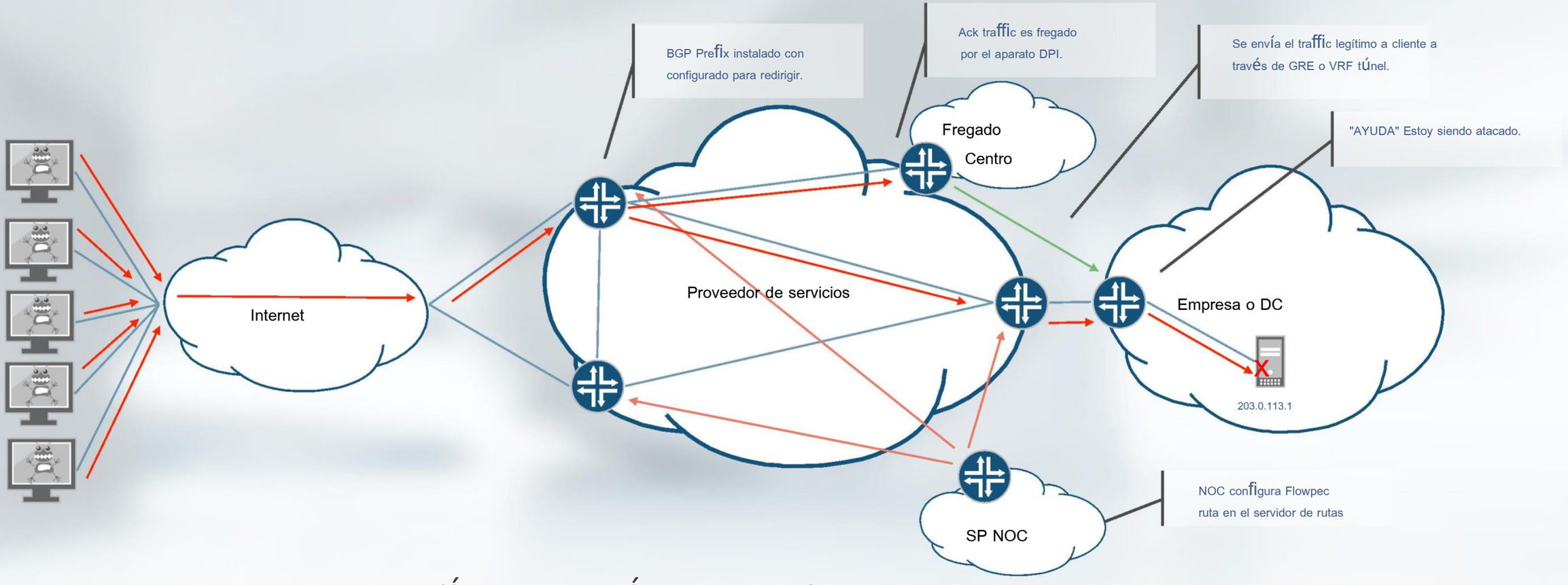
Cisco [7]

```
class-map type traffic match-all attack_fs
  match direcciÓn-destino ipv4 203.0.113.1/32
  protocolo del partido 17
  match puerto-destino 53
end-class-map
!
policy-map type pbr attack_pbr
  tipo de trÁfico attack_fs
    gota a
  clase clase-por-defecto
    gota
end-policy-map
!
flowspec
  address-family ipv4
    polÍtica de servicio tipo pbr attack_pbr
salir
```

Juniper

```
opciones de enrutamiento {
    flujo {
        norma de orden temporal;
        ruta ataque_fs {
            coincidir {
                destino 203.0.113.1/32
                protocolo udp;
                puerto de destino 53;
            }
            y luego descartar;
        }
    }
}
opciones de polÍtica {
    declaraciÓn de polÍtica FLOWROUTES_OUT {
        de {
            rib inetflow.0;
        }
        y luego aceptar;
    }
}
```

MitigaciÓn de DDoS mediante Scrubbing Center



- Puede iniciarse mediante una llamada telefÓnica, la detecciÓn en la red de SP o un portal web para el cliente.

- Permite mitigar los ataques de la capa de aplicaciÓn sin completar el ataque.

ConfiguraciÓn del router de borde

Alcatel-Lucent

```
router
        sistema autÓnomo 64496
        bgp
                grupo "RR-CLIENT-FLOWSPEC"
                        vecino 198.51.100.1
                                familia ipv4 flow-ipv4
                                peer-as 64496
                        salir
                salir
                no hay cierre
        salir
salir
```

Cisco [7]

```
router bgp 64496
    ! Inicializa la familia de direcciones global
    address-family ipv4 flowspec
!
    vecino 198.51.100.1
        remote-as 64496
        ! Lo vincula a una configuraciÓn vecina
        address-family ipv4 flowspec
```

Juniper

```
protocolos {
        bgp {
                grupo RR-CLIENT-FLOWSPEC {
                        tipo interno;
                        vecino 198.51.100.1 {
                                familia inet {
                                        flujo;
                                }
                        }
                }
        }
}
opciones de enrutamiento {
        flujo {
                norma de orden temporal;
        }
}
```

ConfiguraciÓn del servidor de rutas

Alcatel-Lucent

```
router
        sistema autÓnomo 64496
        bgp
                grupo "RR-CLIENT-FLOWSPEC"
                        vecino 198.51.100.2
                                familia ipv4 flow-ipv4
                                peer-as 64496
                        salir
                salir
                no hay cierre
        salir
salir
```

Cisco [7]

```
router bgp 64496
    ! Inicializa la familia de direcciones global
    address-family ipv4 flowspec
!
    vecino 198.51.100.2
        remote-as 64496
        ! Lo vincula a una configuraciÓn vecina
        address-family ipv4 flowspec
```

Juniper

```
protocolos {
        bgp {
                grupo RR-CLIENT-FLOWSPEC {
                        tipo interno;
                        vecino 198.51.100.2 {
                                familia inet {
                                        flujo;
                                }
                                export FLOWROUTES_OUT;
                        }
                }
        }
}
```

ConfiguraciÓn del servidor de rutas

Cisco [7]

```
class-map type traffic match-all attack_fs
  match direcciÓn-destino ipv4 203.0.113.1/32
  protocolo del partido 17
  match puerto-destino 53
end-class-map
!
policy-map type pbr attack_pbr
  tipo de trÁfico attack_fs
    redirigir nexthop 192.0.2.7
  clase clase-por-defecto
end-policy-map
!
flowspec
  address-family ipv4
    polÍtica de servicio tipo pbr attack_pbr
salir
```

Juniper

```
opciones de enrutamiento {
    flujo {
        norma de orden temporal;
        ruta ataque_fs {
            coincidir {
                destino 203.0.113.1/32
                protocolo udp;
                puerto de destino 53;
            }
            y luego descartar;
        }
    }
}
opciones de polÍtica {
    declaraciÓn de polÍtica FLOWROUTES_OUT {
        de {
            rib inetflow.0;
        }
        entonces {
            next-hop 192.0.2.7;
            aceptar;
        }
    }
}
```

¿Cómo sé que está funcionando?

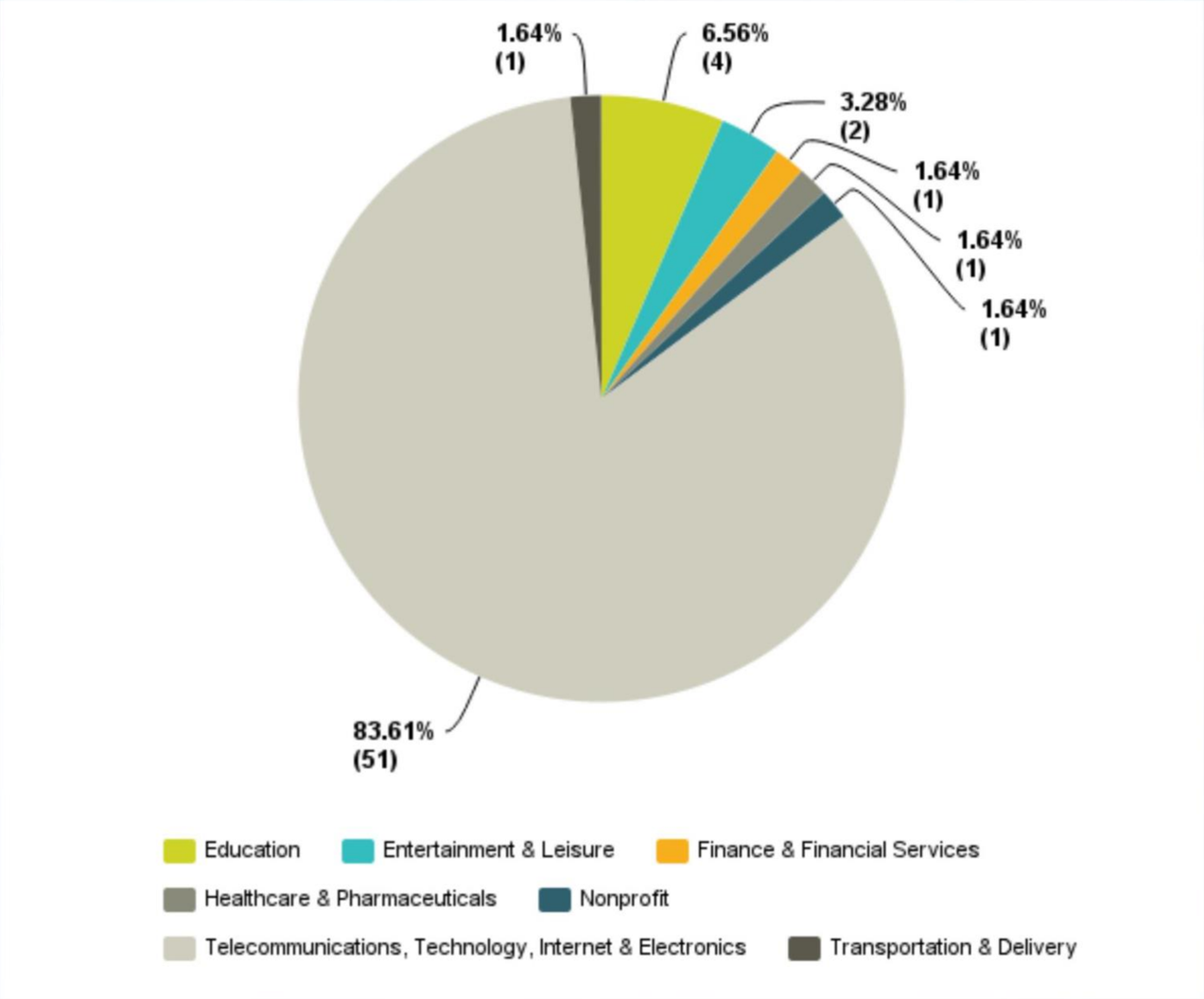
Alcatel-Lucent	Cisco [7]	Juniper
- show router bgp routes flow-ipv4 - show router bgp routes flow-ipv6 - show filter ip fSpec-0 - show filter ip fSpec-0 associations - show filter ip fSpec-0 counters - show filter ip fSpec-0 entry <entry-id>	- show processes flowspec_mgr location all - mostrar resumen de flujo - show flowspec vrf all - show bgp ipv4 flowspec	- show bgp neighbor <vecino> | match inet-flow - mostrar tabla de rutas inetflow.0 extensa - mostrar filtro de firewall __flowspec_default_inet__

¿Hacia dÓnde vamos?

- Soporte de IPv6
  - http://tools.ietf.org/html/draft-ietf-idr-flow-spec-v6-03
- ValidaciÓn relajante
  - http://tools.ietf.org/html/draft-ietf-idr-bgp-flowspec-oid-00
- AcciÓn de redireccionamiento al siguiente punto de acceso IP
  - http://tools.ietf.org/html/draft-simpson-idr-flowspec-redirect-02

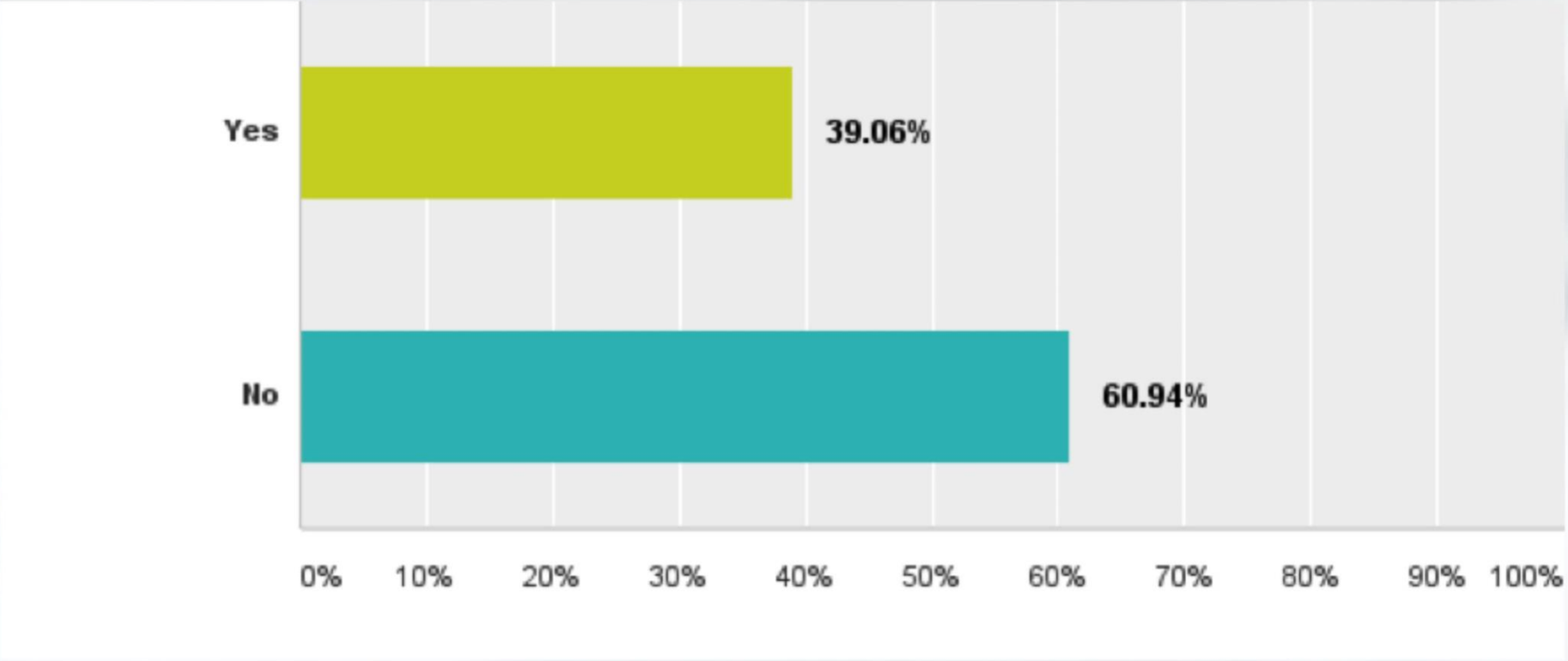
Estado de la UniÓn

Industrias que responden

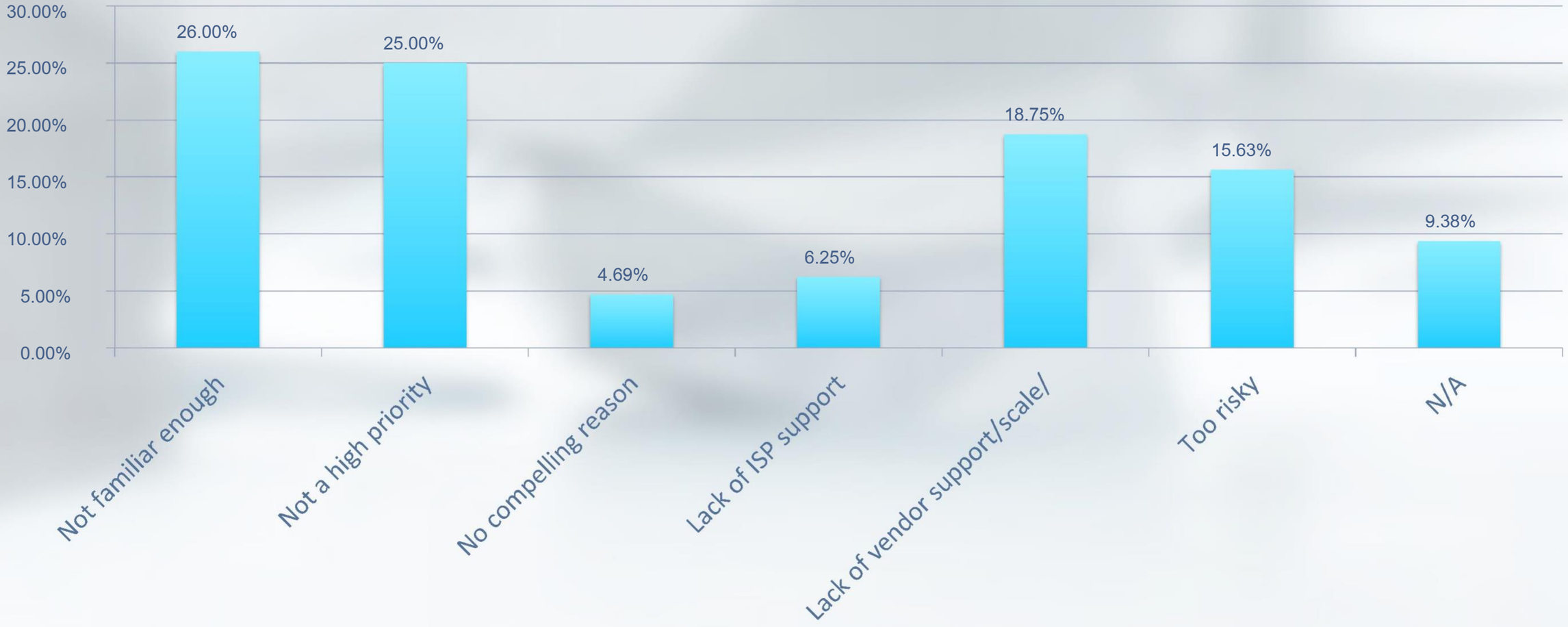


¿Tiene o ha tenido alguna vez BGP

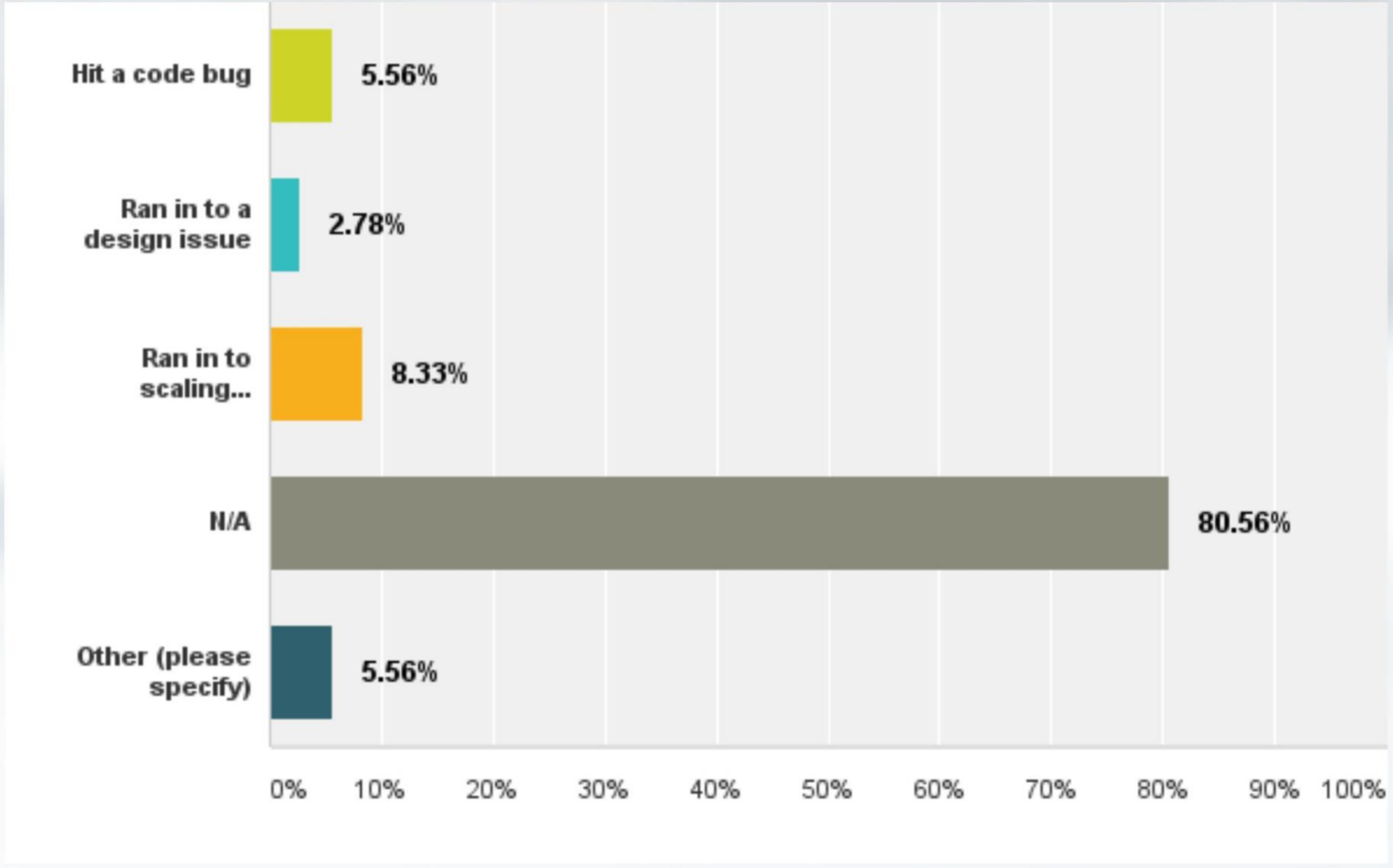
¿FlowSpec activado en alguna parte de su red?



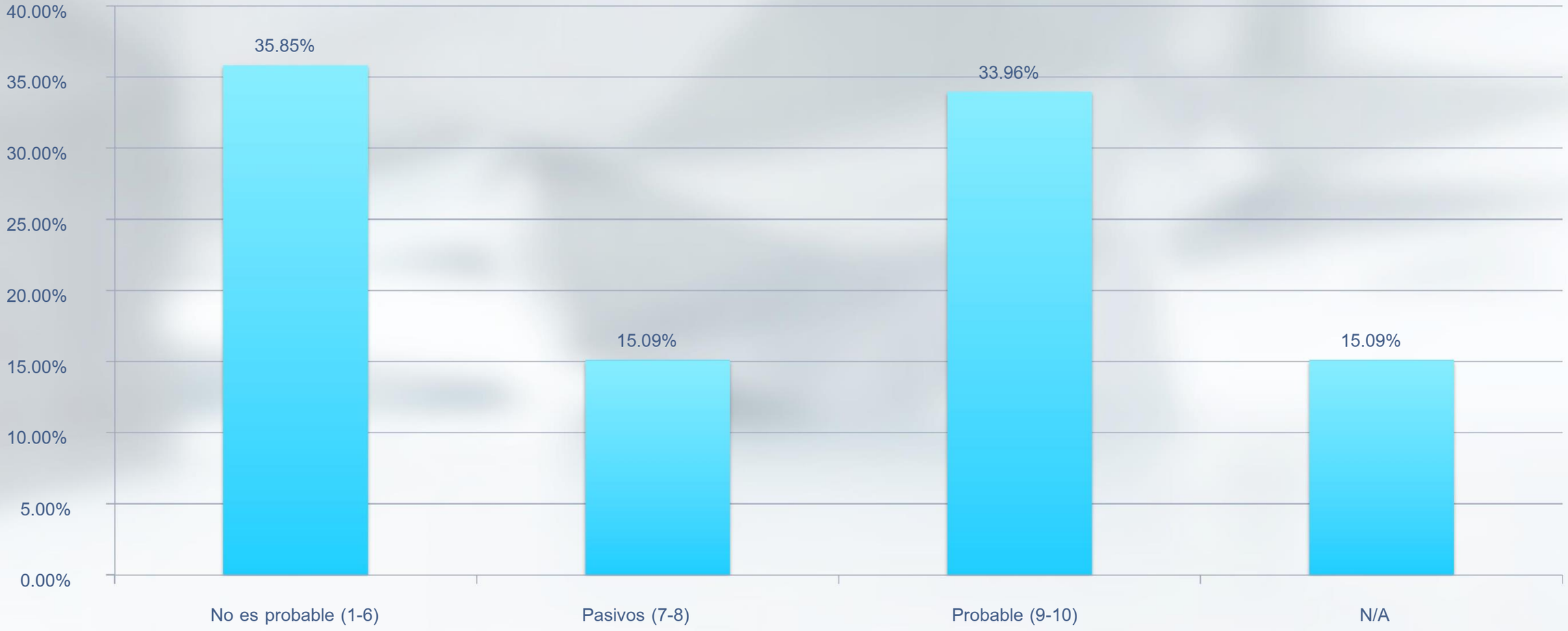
Si no lo has habilitado, ¿por qué no?



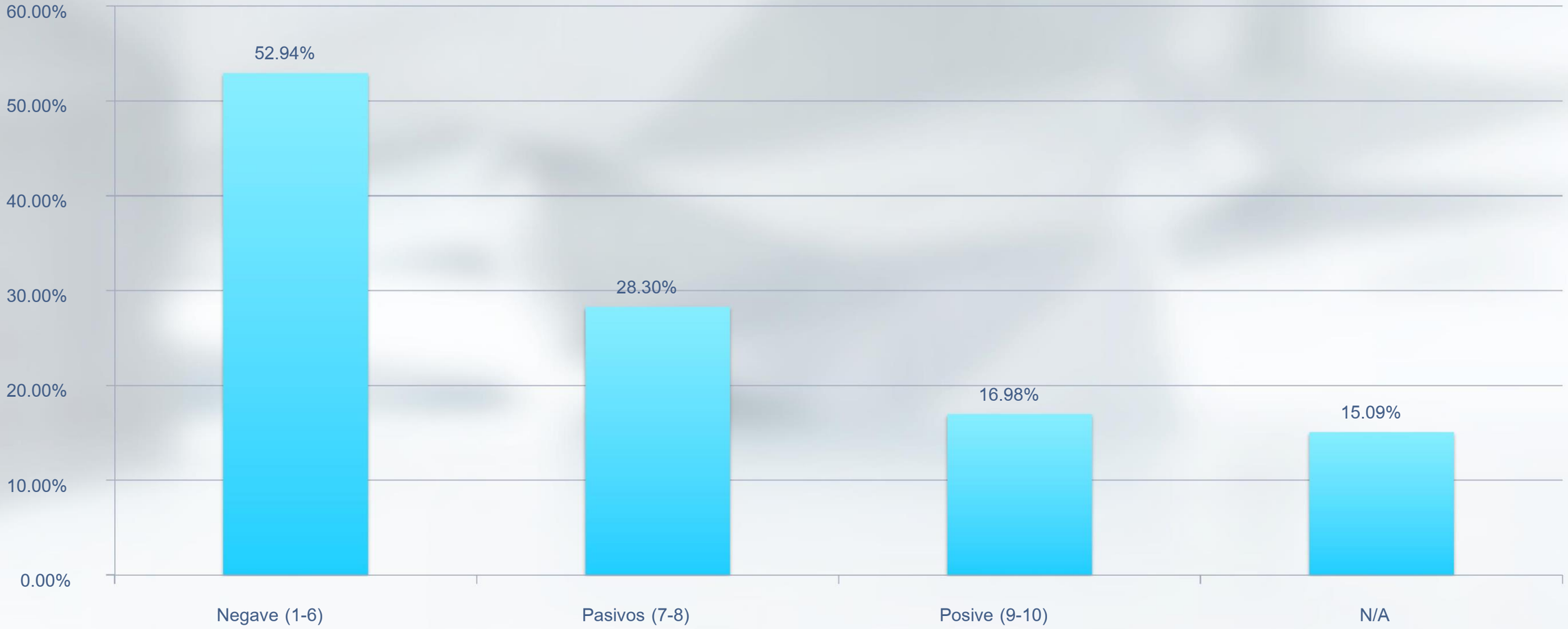
Si lo has activado pero lo has desactivado, ¿por qué?



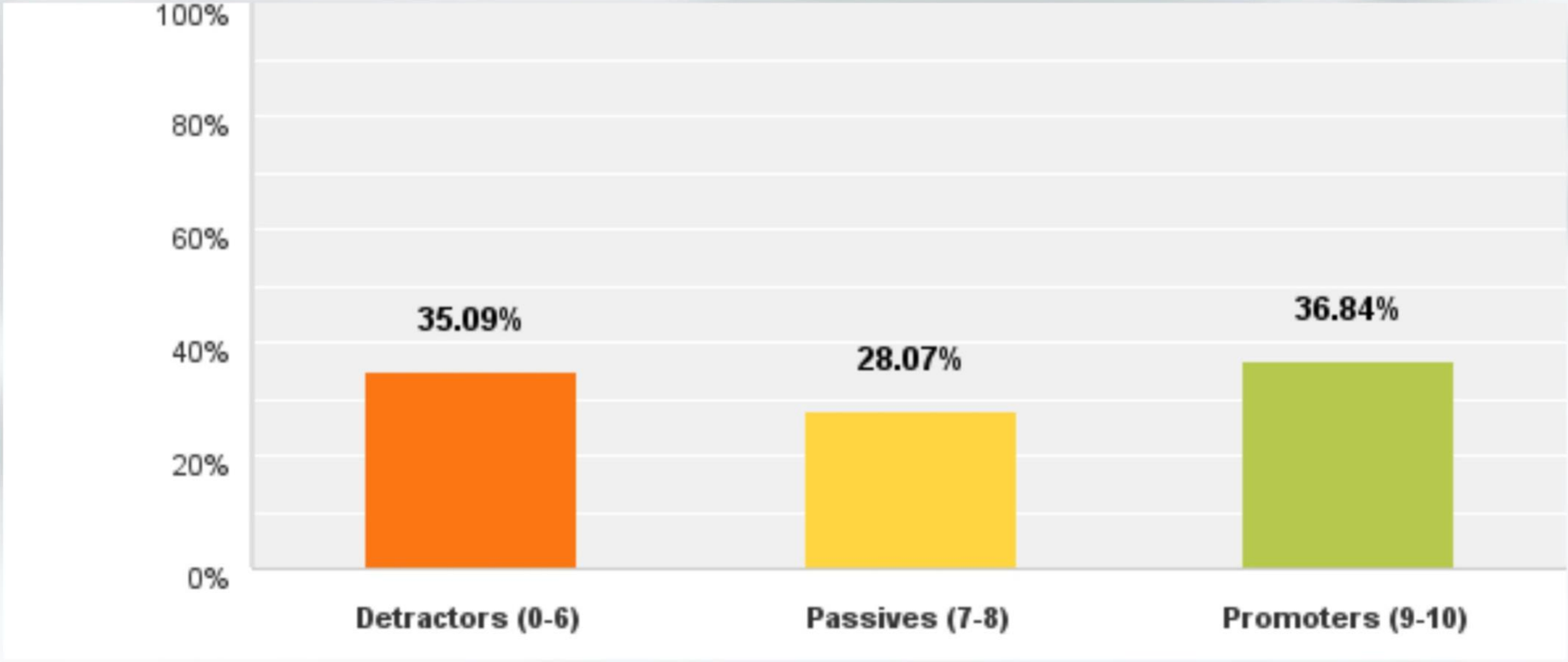
Si no lo tiene activado actualmente, ¿qué probabilidad hay de que ¿va a habilitar BGP Flowspec en el futuro?



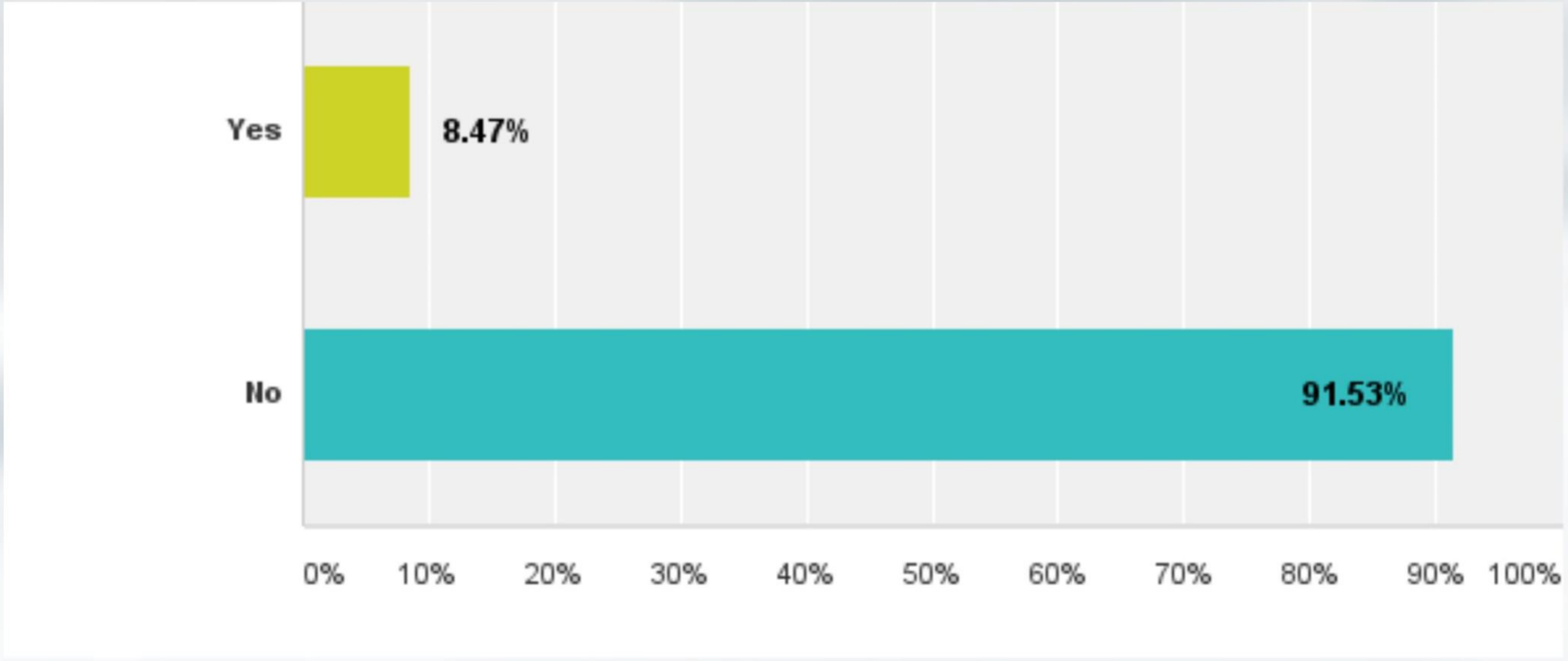
En general, ¿CÓmo calificaría su experiencia con BGP Flowpsec?



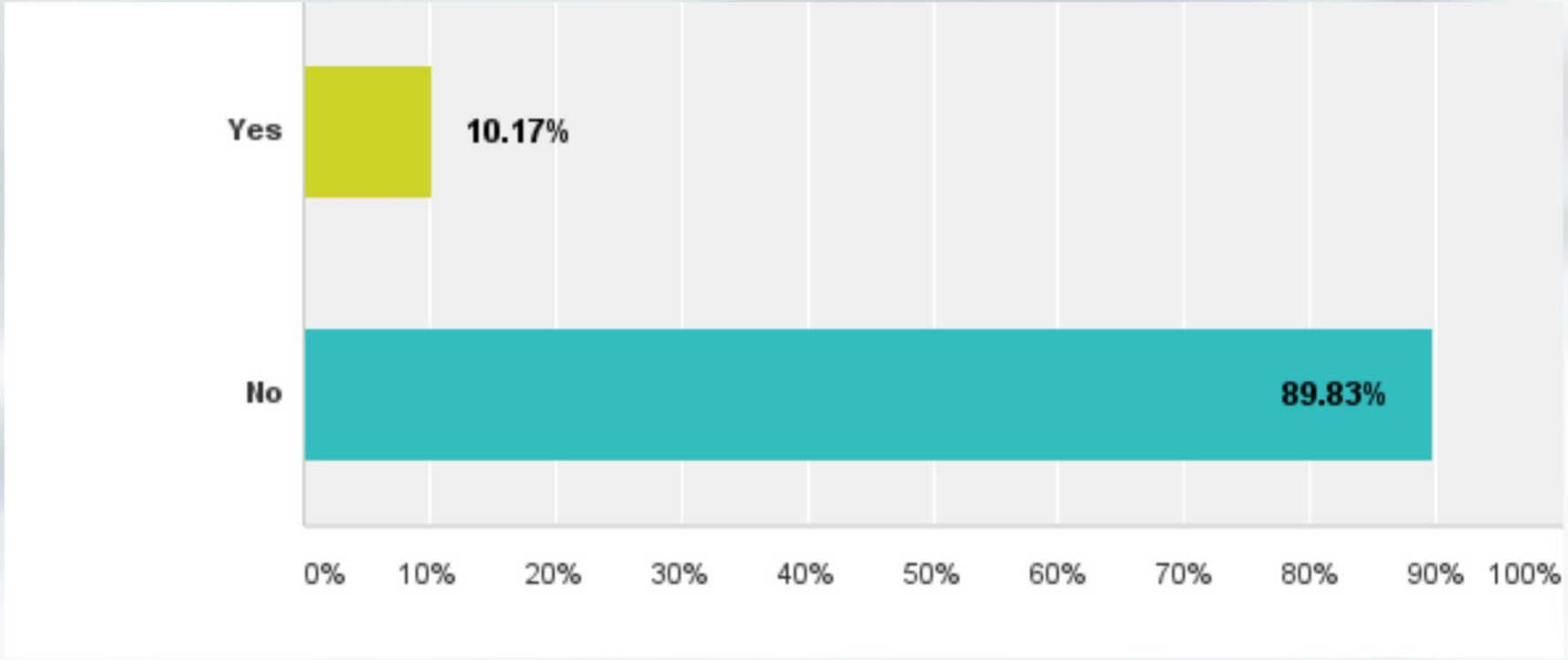
¿Qué probabilidad hay de que recomiende BGP ¿Flowspec a un amigo o colega?



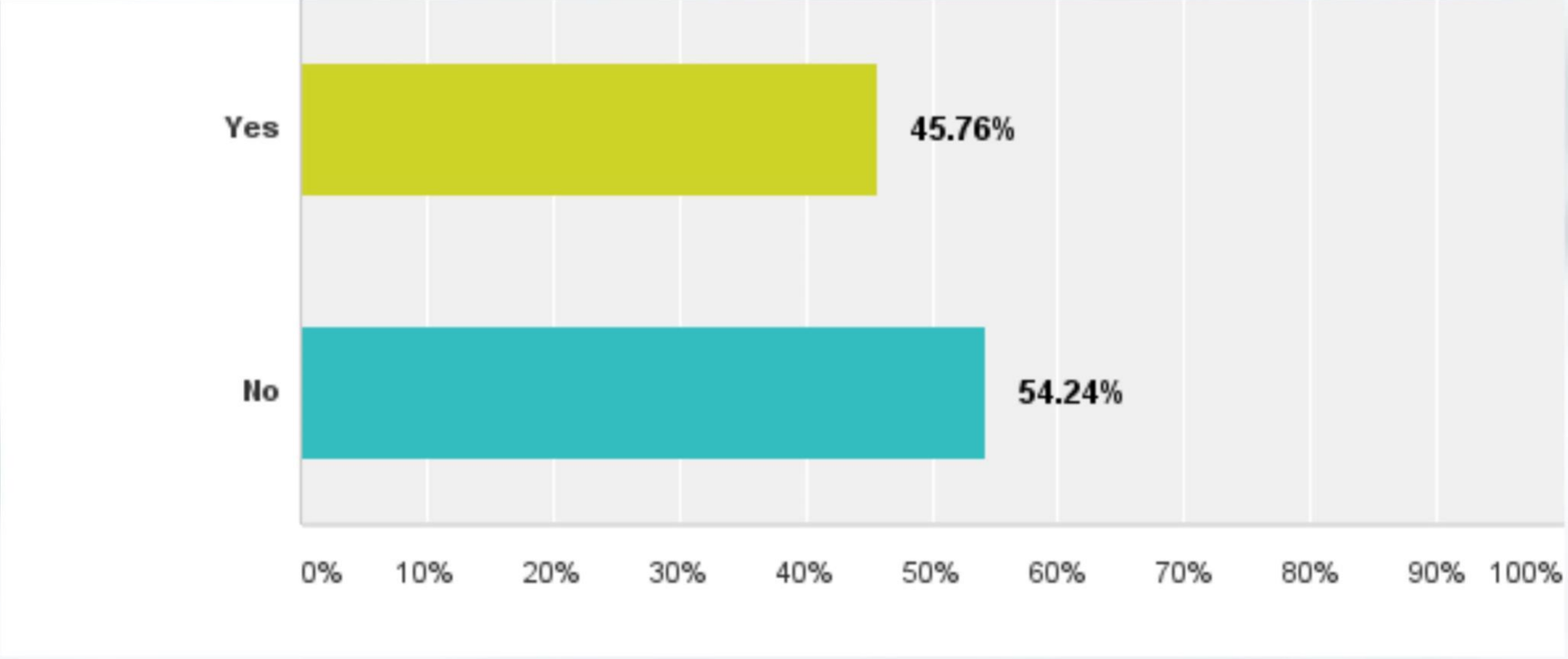
¿Permite que sus clientes le envíen BGP ¿Rutas Flowspec a través de BGP?



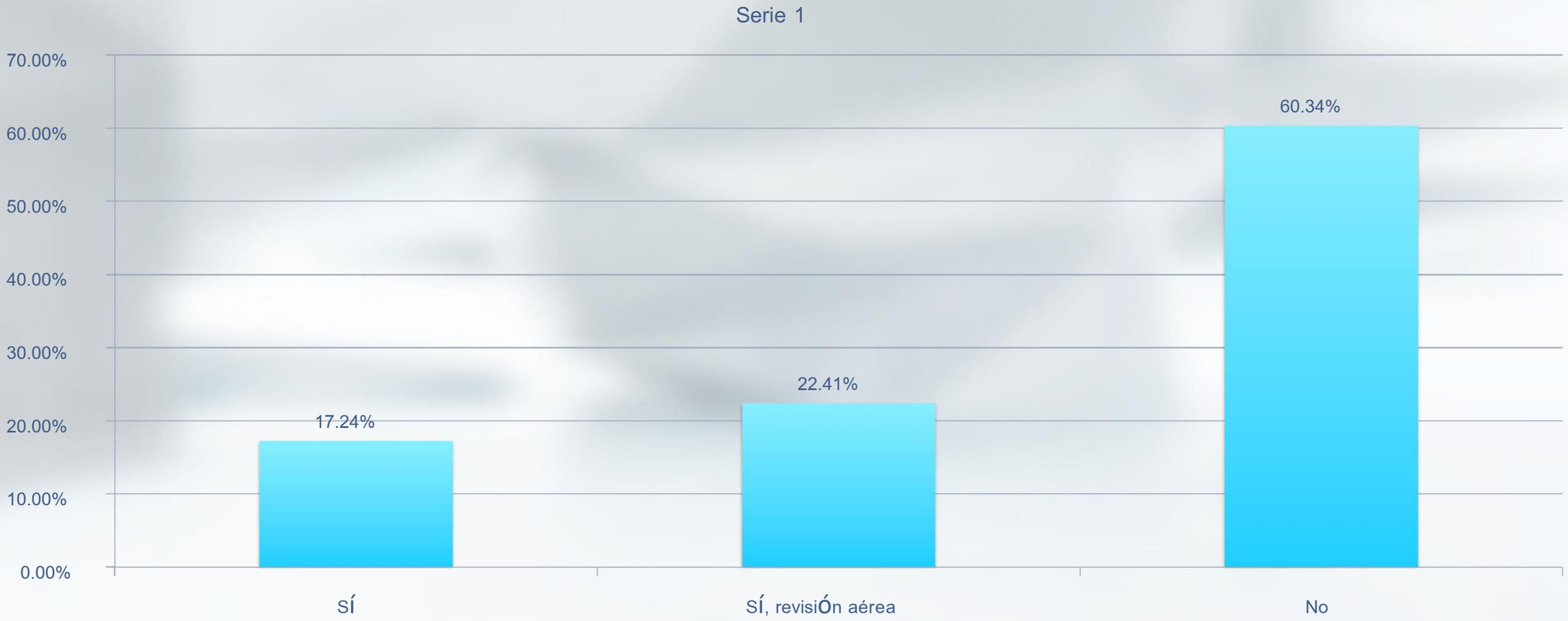
¿Tiene un portal web donde los clientes puedan ¿inyectar rutas BGP Flowspec en su IBGP?



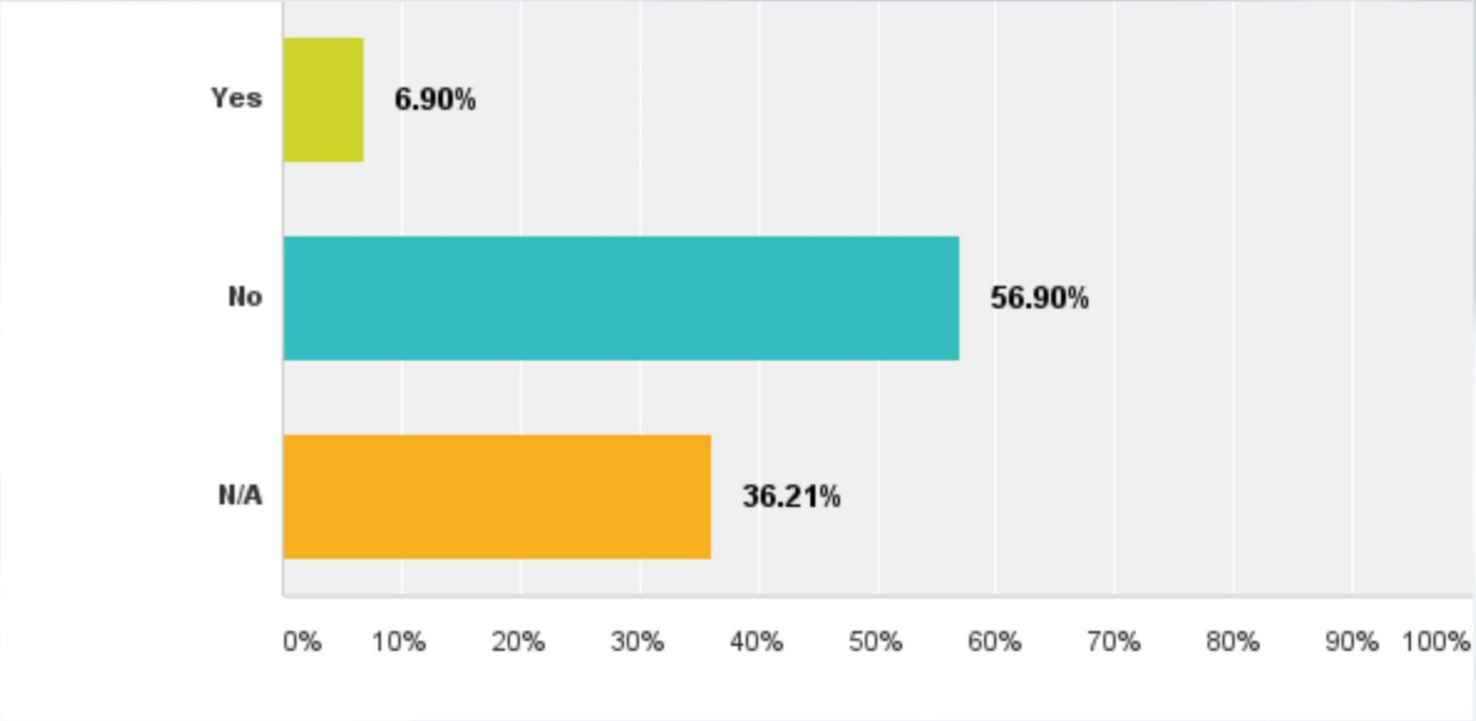
¿Tiene un router central desde el que inyectar sus rutas BGP Flowspec?



¿Permite una herramienta de detección de DDoS (por ejemplo, Arbor) enviar rutas BGP Flowspec a su IBGP?



¿Cobran por la mitigaciÓn de DDoS mediante BGP Flowspec?



Resumen de los comentarios

- Es una gran idea y me encantaría que despegara, pero...
- Las empresas y los proveedores de contenidos están esperando que los ISP acepten su Rutas Flowspec.
    - Algunos incluso estarían dispuestos a cambiar a un ISP que lo hiciera.
- Los ISP están esperando a que los proveedores lo soporten.
    - Más vendedores que lo apoyan
    - Características específicas que necesitan para su entorno
    - Mejor escala o estabilidad

Referencias

- 1] Kaspersky Lab - Una de cada tres empresas de cara al público se enfrenta a un DDoS Ataques http://tinyurl.com/neu4zzr

- 2] Verisign - 2014 DDoS Attack Trends http://tinyurl.com/oujgx94

- 3] NBC News - La velocidad de Internet aumenta considerablemente, pero también lo hacen los ataques informáticos http://tinyurl.com/q4u2b7m

- 4] Tech Times - Un ataque DDoS paraliza la PSN de Sony mientras Microsoft lidia con Problemas de Xbox Live http://tinyurl.com/kkdczjx

- 5] RFC 5575 - Difusión de reglas de especificación de flujo http://www.ietf.org/rfc/rfc5575.txt

- 6] Cisco - Implementación de BGP Flowspec http://tinyurl.com/mm5w7mo

- 7] Cisco - Comprensión de BGP Flowspec http://tinyurl.com/l4kwb3b

Gracias.