Best Practices para Proveedores de Internet

Ariel S. Weher

Ariel S. Weher | <ariel@weher.net> | @arielweher

Objetivo:

"Brindar una serie de ideas que permitan mejorar la calidad de los servicios prestados y que a su vez nos den la capacidad de generar nuevos negocios, manteniendo un ecosistema de competencia productivo, respetuoso y justo".

"Aclaración":

Yo trabajo para una compañía que quizás sea diferente de la suya. Esto puede dar un cierto matiz de color a mis apreciaciones y usted puede (y tiene todo el derecho de) no estar de acuerdo. **Todas las consultas y sugerencias son bienvenidas.** En cualquiera de los casos, le pido participe de la sesión aportando su propia experiencia, a fin de que todos saquemos provecho de este evento.

Ariel S. Weher | <ariel@weher.net> | @arielweher

Reglas Generales:

- Siempre hay excepciones a cada regla.
- Tal vez, a lo mejor, quizás de casualidad yo no cumpla todas las recomendaciones que se estarán presentando.
- Debido al tiempo acotado, los contenidos aquí presentados se muestran a vuelo de pájaro.
- Las preguntas son bienvenidas y casi obligatorias. Si se le ocurren más tarde, me puede encontrar durante toda la semana.

Best Practices Sociales

Formas de comunicación de los operadores.

Ariel S. Weher | <ariel@weher.net> | @arielweher

Best Practices Sociales:

- Participar en los eventos y las listas de correo:
  - Participar en tutoriales y webinars.
  - Exponer ideas.
  - Presentar temas “taboo”.
  - Fomentar las charlas de pasillo.
  - Animarse a preguntar.

@Listas
-->

#Eventos
<--

Links Útiles:

- LACNOG
  - http://www.lacnog.org
  - IPv6 WG
    - http://bit.ly/lacnog-ipv6
  - BCOP WG
    - http://bit.ly/lacnog-bcop
  - IETF WG
    - http://bit.ly/lacnog-ietf
- ArNOG
  - http://www.arnog.com.ar
  - http://bit.ly/lista-arnog

Best Practices Sociales:

- Mantener canales de comunicación actualizados, válidos y consistentes para que cualquier persona pueda contactarse con los responsables de la empresa.
- Esto incluye:
  - Datos de WHOIS / RDAP.
  - Casillas de correo del NOC.
  - Datos de denuncias de Abuso.
- Idealmente se debe responder los incidentes reportados con un número de ticket que permite hacer un seguimiento de cada caso.

Algunas direcciones de mail recomendadas en RFC2142:

- Relacionadas al negocio:
  - info@empresa.tld
  - marketing@empresa.tld
- Operaciones de red:
  - abuse@empresa.tld *(Conductas inapropiadas)*
  - noc@empresa.tld *(Centro de Operaciones)*
  - security@empresa.tld *(CSIRT)*
- Soporte de servicios específicos:
  - postmaster@empresa.tld *(Correo)*
  - hostmaster@empresa.tld *(DNS)*
  - webmaster@empresa.tld *(Web)*

Política de Uso Aceptable:

- Se debe mantener publicada una PUA acerca de los servicios que se prestan.
  - La PUA debe ser lo más específica posible acerca de las cosas que se permiten o no en la red del prestador.
  - Deben también especificarse las sanciones que se tomarán en caso de no cumplir con la PUA.
- Debe estar publicada en un apartado del sitio web de la empresa que sea de fácil acceso.
- Cualquier cambio en la PUA debe ser informado a los clientes.

Políticas de servicio:

- Se debe anunciar y (mantener actualizada) toda la información referente a la forma de dar servicio:
  - Políticas de ruteo:
    - Whois.
    - RADb.
    - PeeringDB.
  - SLA's (si los hay).
  - Políticas de seguridad en servicios:
    - Límites de envío de correo.
    - Configuraciones de seguridad y requerimientos mínimos para los sistemas de los clientes.

Best Practices Técnicas

Consejos que todos deberíamos cumplir.

Ariel S. Weher | <ariel@weher.net> | @arielweher

Abuse.IO

- Paquete de herramientas Open Source para automatizar los procesos de atención de reportes de incidentes.
  - Trabaja con direcciones IPv4 e IPv6.
    - Se puede integrar con los sistemas IPAM.
  - Traduce reclamos en tickets internos.
  - Permite delegar el trabajo a los helpdesk.
  - Procesa varios feeds:
    - ShadowServer, SpamCop, Netcraft, Google Safe Browsing, IP Echelon, C-SIRT, Project Honey Pot, Abuse-IX, entre otros.
- Más información en: https://abuse.io

Fin de las excusas: TLS sin complicaciones

- LetsEncrypt (.org)
  - Ofrece certificados digitales x.509 válidos GRATIS.
  - Respaldado por varias organizaciones internacionales a fin de promover el uso de TLS.
  - Hay implementaciones de clientes en Python que auto-configuran los servicios en un par de minutos.
  - Pueden usarse en cualquier tipo de servicio con soporte TLS.
  - Actualmente en etapa beta, los certificados sólo duran tres meses, pero se pueden renovar automáticamente usando los scripts provistos.

Hoy existe una BCP para BGP

RFC7454: "BGP Operations and Security"

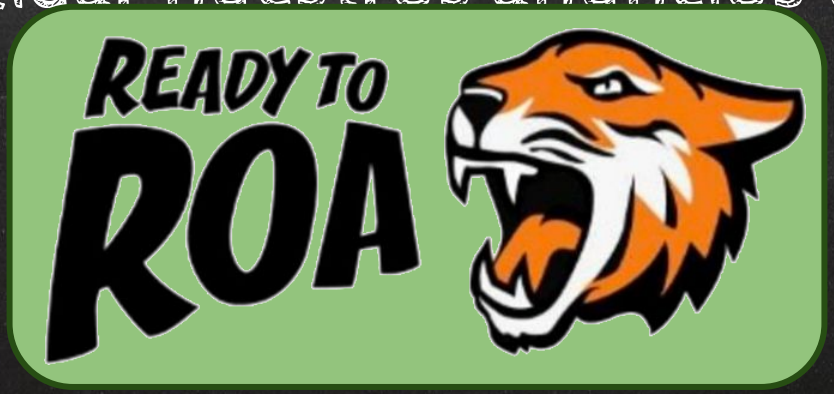
Ariel S. Weher | <ariel@weher.net> | @arielweher

BGP #1:

- Habilitar MD5 Auth siempre que sea posible.
- Habilitar *dampening* para ayudar a la estabilidad de las tablas.
  - RFC7196 recomienda cambiar suppress timer a 6000 segundos (2000 por default).
- Usar *ttl-security* en lugar de *ebgp-multihop*.
- Hacer publicaciones con rutas estáticas blackhole + comando network (nailed routes).
  - En lo posible evitar el uso de redistribución, salvo en ambientes muy controlados.
- Usar alguna implementación de RPKI.
  - Aunque no se considere viable el descarte de rutas inválidas...

BGP #2:

- Limitar máximo de prefijos permitidos:
  - Si es posible, que no se caiga la sesión BGP.
- Limitar el largo de prefijo permitido:
  - En IPv4: hasta /24 (RIPE-399)
  - En IPv6: hasta /48 (RIPE-523)
- Generar los ROA para que el resto del mundo pueda validar nuestros anuncios usando RPKI.



Ariel S. Weher | <ariel@weher.net> | @arielweher

BGP #3:

- Siempre debemos tratar de publicar pocas redes hacia internet.
  - En caso de necesitar ingeniería de tráfico, hacerla con bloques que sean idealmente /22 o menor.
  - Para evitar asimetría de tráfico entre carriers podemos sumar la publicación de prefijos cortos con community “no-export”.
    - Cuidado con esto, algunos carriers quitan las communities y se pueden producir errores.
- Si estamos conectados a un IXP:
  - Todas las redes que se reciben deberían tener mayor local-preference.
    - Siempre considerar que el local-preference de una ruta debe ser: Cliente > IXP > = Internet.

BGP #3':

Malas publicaciones de BGP generan caminos sub-óptimos para los paquetes o visibilidad limitada de los prefijos.

En algunos casos "malas publicaciones" es publicar "/24's"

http://visibility.it.uc3m.es/

Ariel S. Weher | <ariel@weher.net> | @arielweher

BGP #4: IRR's

```
user@box:~$ bgpq3 -4 -A -s -l miembro-cern as513
no ip prefix-list miembro-cern
ip prefix-list miembro-cern seq 1 permit 128.141.0.0/16
ip prefix-list miembro-cern seq 2 permit 128.142.0.0/16
ip prefix-list miembro-cern seq 3 permit 137.138.0.0/16
ip prefix-list miembro-cern seq 4 permit 188.184.0.0/15
[...]
ip prefix-list miembro-cern seq 17 permit 192.91.240.0/22
ip prefix-list miembro-cern seq 18 permit 192.91.244.0/23
ip prefix-list miembro-cern seq 19 permit 192.91.246.0/24
ip prefix-list miembro-cern seq 20 permit 194.12.128.0/18
```

- https://github.com/snar/bgpq3

(Tener en cuenta que los IRR a veces no tienen toda la información)

- http://irrexplorer.nlnog.net/

BGP #5: Comunidades

- Todos los ASN de tránsito deberían implementar communities.
  - Facilita la distribución de subsets de prefijos.
  - Permite a los clientes hacer ingeniería de tráfico.
    - Transmitir estado de validación de rutas.
    - Permiten políticas de forwarding flexibles en SDN.
    - Evitar la desagregación.
  - Posibilita mitigar algunos ataques [D]DOS.
- Listado público de comunidades por ASN:
  - http://onesc.net/communities/

Componentes del Secure Inter Domain Routing:

- https://datatracker.ietf.org/wg/sidr

Infraestructura de RPKI

Validación de Origen

- Estándares ratificados.
- Código existente.
- Se necesitan cambios menores en los routers.
- Resuelven los incidentes más frecuentes.
- Corren en servidores externos para no comprometer el procesamiento de los routers.
- Amplia adopción en la región de LAC(*).

BGPSEC

- Está propuesto en IETF y se está trabajando en el tema.
  - WG SIDR
- Consiste en poner firmas en el atributo AS-PATH.

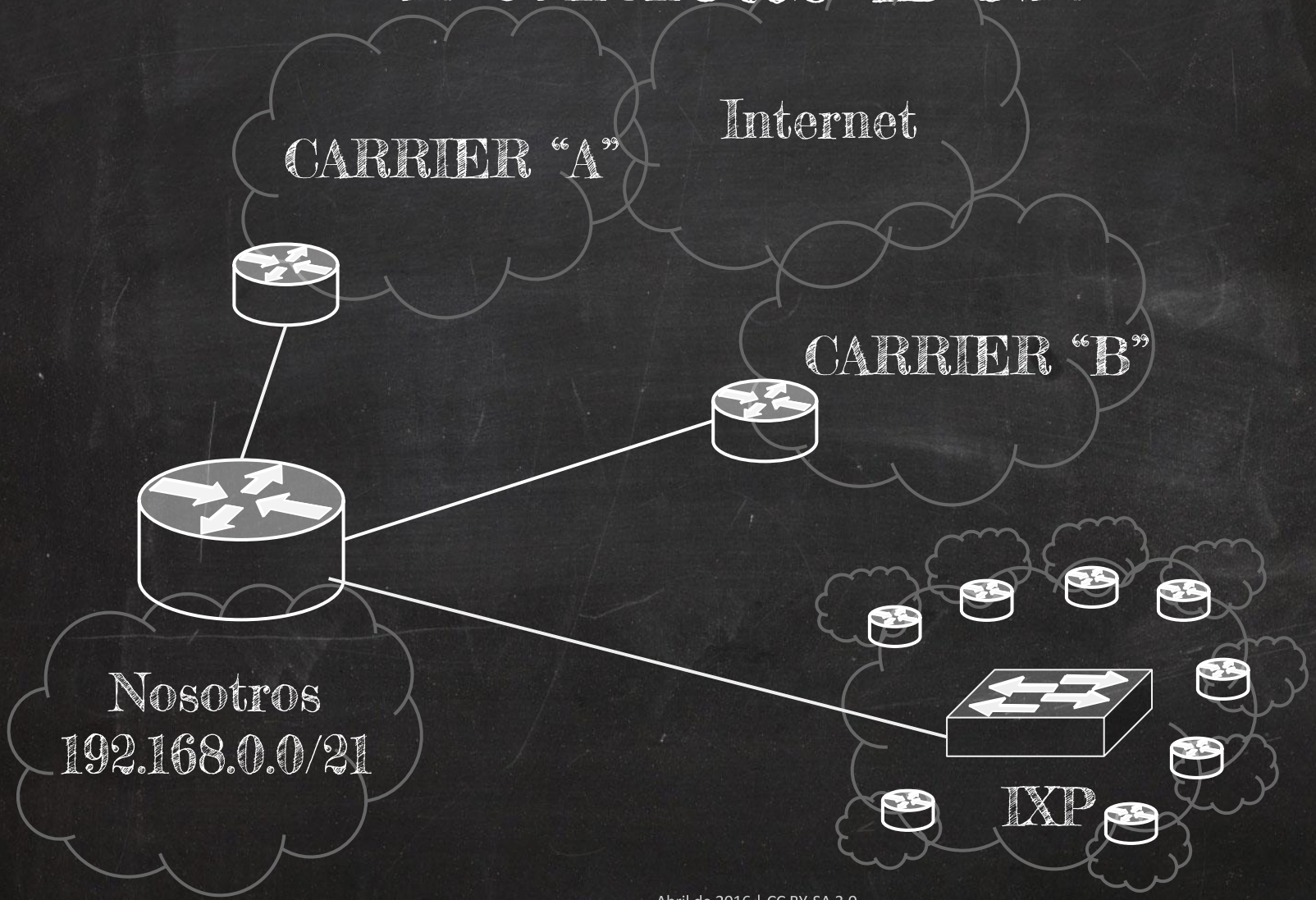
(*) Fuente: http://rpki.surfnet.nl/perrir.html

Para agendar y participar:

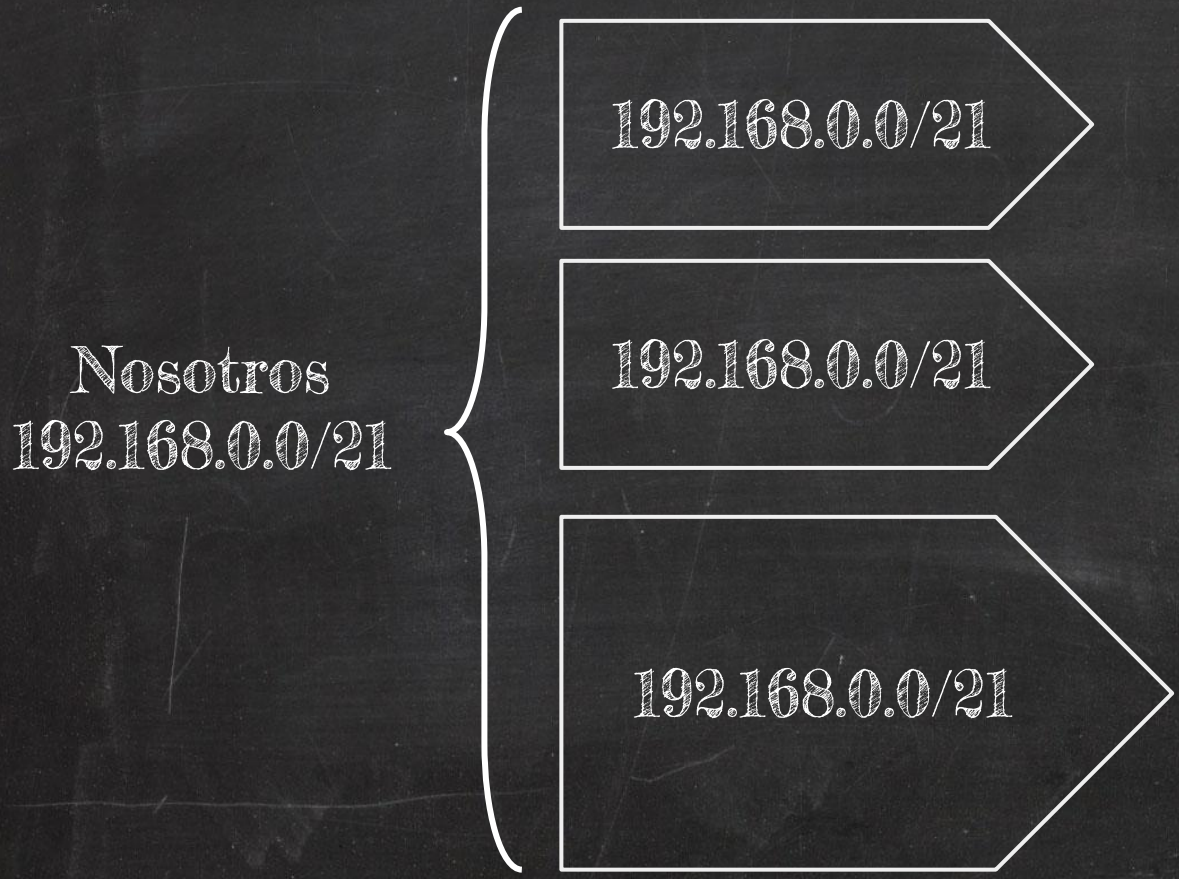
Proyecto UTRS del Team Cymru

http://www.team-cymru.org/UTRS/

Casos de Uso: Políticas BGP



BGP sin T.E.:



Este esquema deja librado el downstream a los valores de Local Preference que tengan los vecinos.

BGP con T.E.:

Chequear siempre que el carrier permita communities y las respete.

Nosotros
192.168.0.0/21

192.168.0.0/21
192.168.0.0/22
(192.168.4.0/22 + No-Export)

CARRIER "A"
+ 3 Prepends

192.168.0.0/21
192.168.4.0/22
(192.168.0.0/22 + No-Export)

CARRIER "B"
+ 3 Prepends

192.168.0.0/22
192.168.4.0/22

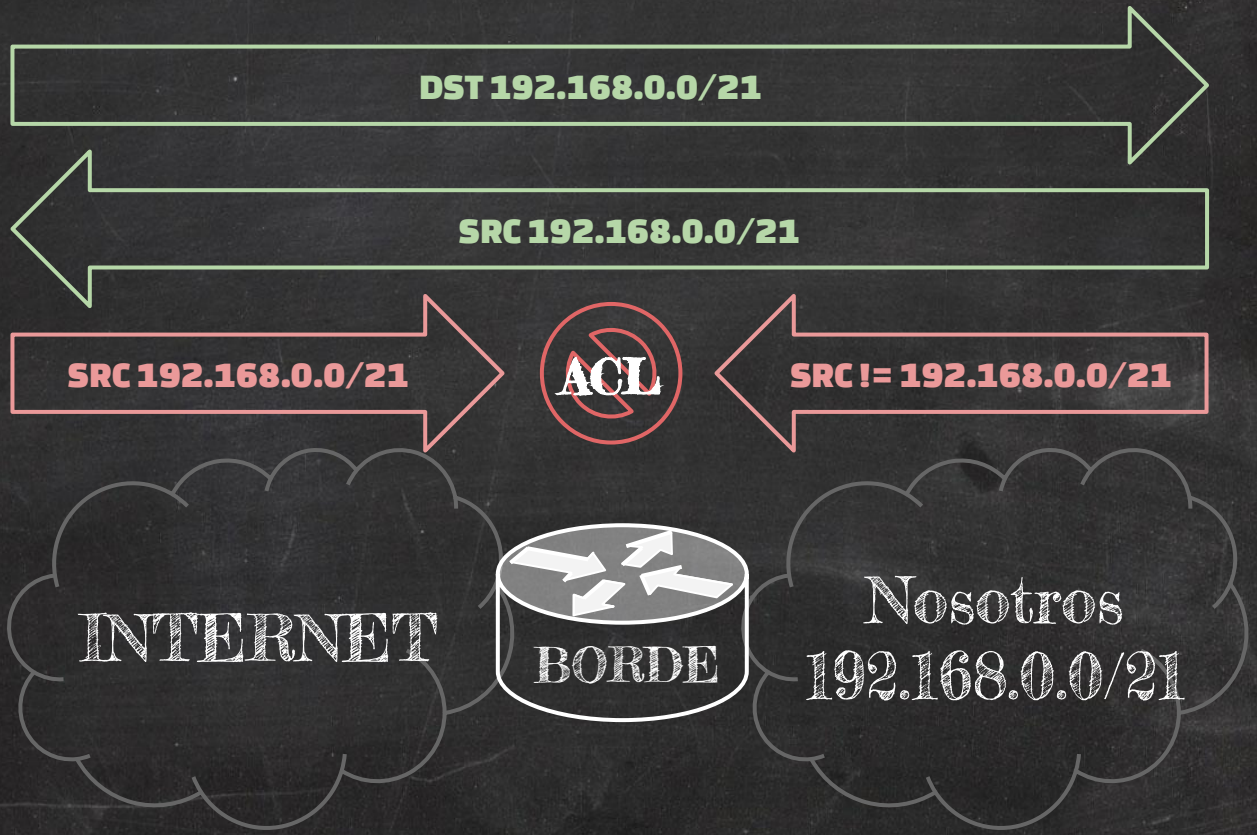
IXP
Sin Prepends

BCP38:

- La idea de este documento es que cada operador filtre tráfico originado en prefijos no propios en el borde y dentro de su red.
- Una vez implementado se logra que los usuarios de nuestras redes no puedan generar ataques de denegación de servicio desde direcciones IP falseadas *(spoofing)*.

http://bcp38.info/

BCP38:



Se recomienda también usar BCP38 dentro de nuestra red y lo más cerca posible de los clientes.

Martian Addresses:

Todos conocemos las direcciones de RFC1918:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

¿Pero qué sabemos de... ?

- 0.0.0.0/8
- 100.64.0.0/10
- 127.0.0.0/8
- 169.254.0.0/16
- 192.0.0.0/24
- 192.0.2.0/24
- 198.18.0.0/15
- 198.51.100.0/24
- 203.0.113.0/24
- 224.0.0.0/3

Fuente: https://en.wikipedia.org/wiki/Martian_packet

Martian Addresses:

También hay en IPv6:

- ::/128
- ::1/128
- ::ffff:0:0/96
- ::/96
- 100::/64
- 2001:10::/28
- 2001:db8::/32
- fc00::/7
- fe80::/10
- fec0::/10
- ff00::/8
- Equivalentes 6to4
- Equivalentes TEREDO

Fuente: https://en.wikipedia.org/wiki/Martian_packet

Martian Addresses:

Fuente Oficial:

- http://bit.ly/iana-martian-ipv4
- http://bit.ly/iana-martian-ipv6

Tip: Son los registros que tienen 'Global' == 'False'

Fuente: https://en.wikipedia.org/wiki/Martian_packet

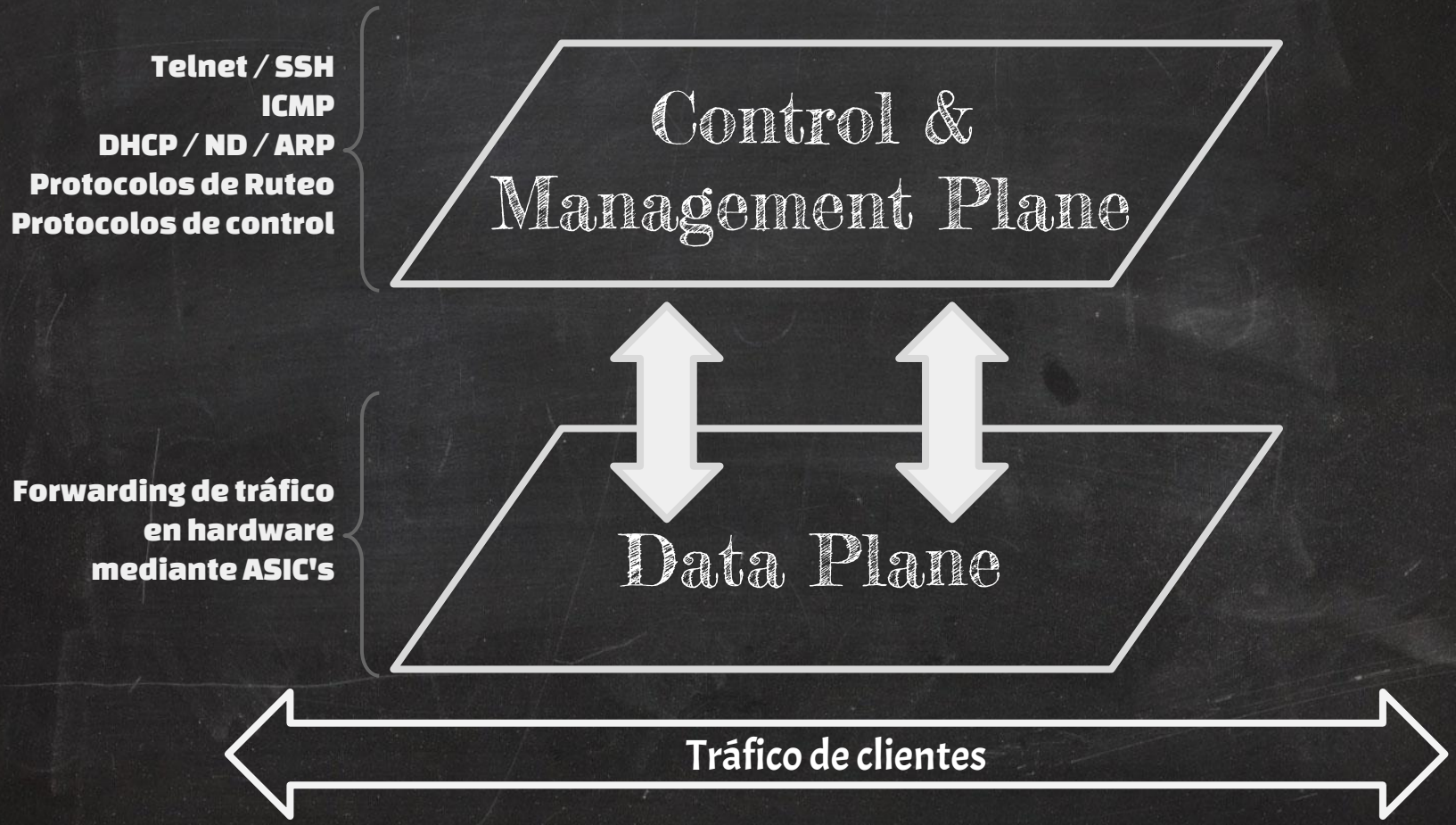
Otras cosas que podemos filtrar:

- La mayoría de los ISP vende servicios "residenciales" y/o "comerciales" y ambos suelen separarse en distintos pooles de direcciones IP y a veces en distintos equipos de acceso.
- Algunos ataques se pueden evitar teniendo en cuenta que los usuarios residenciales no deberían ofrecer algunos servicios.
- Los usuarios residenciales deberían tener direcciones IP asignadas dinámicamente.

Otras cosas que podemos filtrar:

- Servicios que se deberían filtrar a los clientes residenciales desde Internet:
  - MS SMB / CIFS / Active Directory.
  - MS SQL (SQL Worm).
  - DNS (cliente como servidor DNS).
  - SMTP (cliente como servidor SMTP).
  - IRC (Cliente como servidor IRC).
  - CHARGEN (Debería ser filtrado totalmente).
  - UDP/0 (Usado en algunos ataques).
  - Paquetes con opciones de Source-Route.
  - ¿IPv6 extension headers?

Planos de los equipos:



Protegiendo los equipos:

- Limitar la cantidad de paquetes que pueden ser enviados al Control Plane de los equipos.
- De ser posible, poner las interfaces de gestión en un VRF alternativo.
- Segurizar o desactivar los protocolos peligrosos en las interfaces de cliente:
  - CDP / LLDP / VTP / DTP.
  - STP / PAgP / LACP.
  - LDP / IGMP.
- Salvo que sea estrictamente necesario no deben llegar paquetes de saludo de protocolos de ruteo a los clientes.

Monitoreo de eventos:

- Mantener un servidor de Syslog centralizado.
  - Ver mejor opción de transporte: UDP vs TCP.
  - Generar alerta en base a strings predefinidos.
    - RSyslog + MySQL.
    - Graylog.
  - Sincronizar todos los relojes usando varios NTP.
  - Usar un sistema de AAA centralizado para gestionar los usuarios que acceden y modifican las configs:
    - RADIUS / TACACS+
  - Usar SNMP para poder medir:
    - Tráficos y errores de interfaces:
    - Tablas de vecinos y tablas de ruteo
    - Limitar los walks haciendo vistas SNMP limitadas.
  - Implementar NetFlow / IPFIX para conocer mejor el tráfico de la red.

Delays

Mayor Delay Menor Throughput

- Cuidar los delays de la red.
- Medir y mantener un histórico de mediciones del delay dentro de la red.
  - Evaluar el porqué de los cambios.
  - En lo posible usar equipos pensados para ISP y evitar equipos empresariales.
  - Evaluar la posibilidad de usar métodos de forwarding que disminuyan el delay y permitan hacer ingeniería de tráfico (MPLS).

Colaboración:

"Si entre ellos pelean los devoran los de afuera".

Ariel S. Weher | <ariel@weher.net> | @arielweher

Colaboración entre empresas:

- Generar acuerdos de interconexión con los vecinos.
- En caso de disponer de recursos, conectarse a los puntos de intercambio regionales.
- Fomentar el uso de buenas prácticas.
- Instalar instancias de servicios públicos de consulta y testing:
  - Instancias de SpeedTest.
  - RIPE Atlas.
  - Looking Glass.
  - Route-Server.

Sustentabilidad:

(Uso eficiente de los recursos)

Ariel S. Weher | <ariel@weher.net> | @arielweher

Sustentabilidad:

- Ahorro de recursos energéticos:
  - Usar luces led donde sea posible.
  - Maximizar el uso de luz natural.
  - Habilitar los gestores de administración de energía.
  - Consolidar servidores utilizando virtualización.
    - Genera un ahorro directo al usar menos espacio físico, refrigeración y energía.
- Gestión de residuos que disminuya el impacto ambiental de la empresa, separar en:
  - Residuos orgánicos (aptos para compostaje).
  - Residuos inorgánicos (reciclables).
  - Residuos no recuperables (basura normal).

Sustentabilidad:

- Las plantas purifican el aire y ayudan a tener un ambiente de trabajo más relajado.
- Disminuir el uso de insumos:
  - Consumo de papel
  - Insumos de impresión.
    - Usar fuentes de letra ecológicas para ahorrar tinta.
    - Disminuir márgenes de impresión.
    - Usar papel reciclado.

Fuentes y Agradecimientos:

"Listado de algunas de las cosas que encontré en Google".

Ariel S. Weher | <ariel@weher.net> | @arielweher

Fuentes y Agradecimientos:

- RFC3013
  - http://tools.ietf.org/html/rfc3013
- RFC 2142
  - http://tools.ietf.org/html/rfc2142
- BCP38
  - http://tools.ietf.org/html/bcp38
- "An analysis of interdomain visibility"
  - Marcelo Bagnulo, Univ. Carlos III, Madrid
- "How to Calculate TCP throughput for long distance WAN links"
  - Brad Hedlund, http://bit.ly/WcqsZz

¿Preguntas?

¡Muchas Gracias!