
socium
Su aliado seguro

IXSY Meeting 2024

Buenas Prácticas de BGP

Mérida, Yucatán

Abril 2024

SOCIUM: Nosotros

- Áreas de Acción: en DNS, DNSSEC, IPv6 y mejores prácticas internacionales
- Colaboración con LAC-IX, ISOC y LACNIC para mejorar la interconexión en la región.
- Amplia experiencia en diferentes sectores: público, ccTLD, ISP, empresarial, académico.
- Servicios administrados, asesoría, consultoría e implementación.
- Actualmente prestando servicios en 15 países de Latinoamérica, Caribe y Asia.

socium

BGP: ¿Qué es?

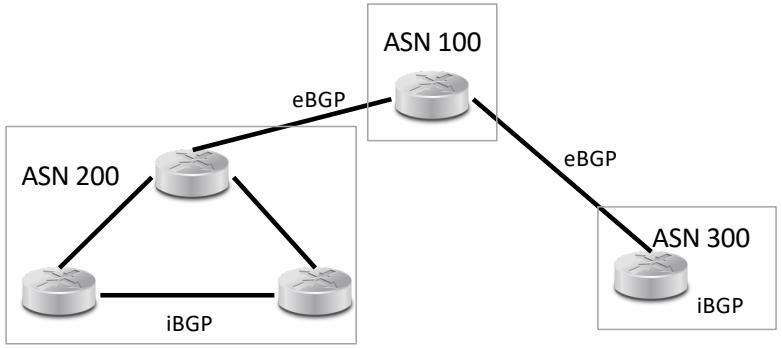
BGP				
Protocolo de Gateway Exterior, descrito en el RFC 1163	Se utiliza para intercambiar información de enrutamiento entre enrutadores de diferentes sistemas autónomos (AS)	Aporta una mayor estabilidad a las redes actuando como protocolo de borde externo y/o borde interno.	Las extensiones del BGP multiprotocolo (MBGP) permiten que el BGP admita IPv6.	Usa TCP como protocolo de transporte y el puerto 179 para establecer conexiones.

BGP: ¿Cuándo se usa BGP?

Se utiliza para el enrutamiento y la gestión del intercambio de datos entre sistemas autónomos y dentro de ellos.

Se utiliza como **eBGP y como iBGP.**

Se garantiza una mayor estabilidad de la red, al tomar decisiones basadas en políticas y reglas definidas por los operadores de red.



BGP: ¿En qué casos se usa BGP?

Dos tipos de interconexiones:

Tránsito:

- Interconexiones entre redes en la cual una provee la capacidad de ingresar a Internet a la otra (ISP)

Peering:

- Es un acuerdo entre dos partes para intercambio de información y ruteo.
- Las redes se conectan para intercambiar trafico que se originan o terminan dentro de sus redes.

• 2 Tipos de Peering:

Publico

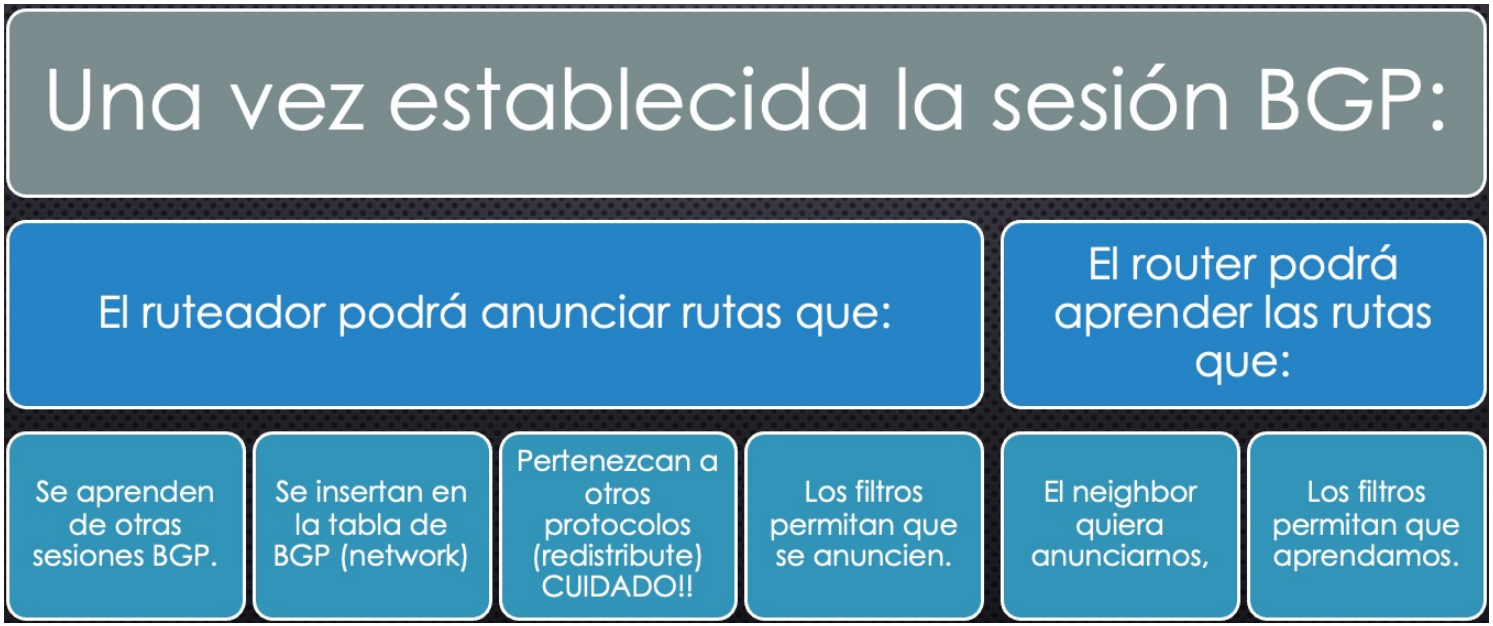
Es realizado a través de Puntos de Intercambio (IXPs), donde una red puede conectarse con varias redes a través de una sola conexión.

Privado

Cuando dos o más redes acuerdan intercambiar su tráfico en una instalación privada.

socium

BGP: ¿Qué sucede luego?



socium

Enrutamiento: ¿Por qué está en riesgo?

Incidentes de Ruteo = Problemas Mundiales Reales

- El ruteo inseguro es uno de los caminos más comunes de amenazas maliciosas.
- Los ataques pueden tardar desde horas hasta días o meses en ser reconocidos.
- Errores inadvertidos pueden sacar de línea a un país entero, mientras que los atacantes pueden robar información personal o tomar la red de una organización como rehén.

Enrutamiento: ¿Por qué está en riesgo?

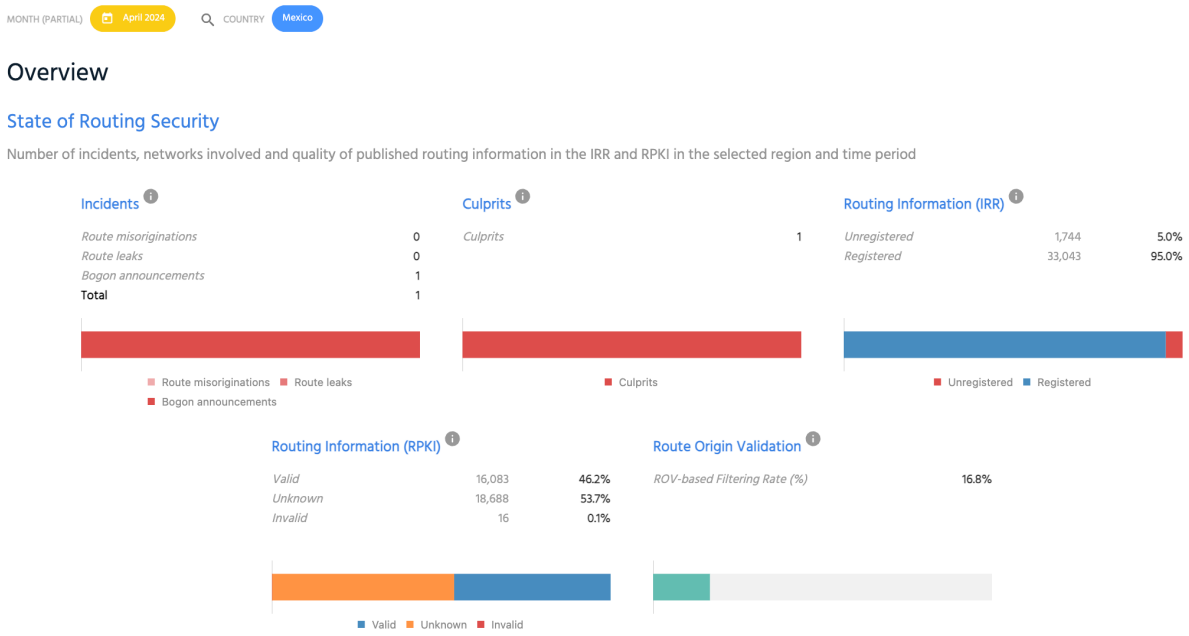
La Solución:

Mutually Agreed Norms for Routing Security (MANRS)

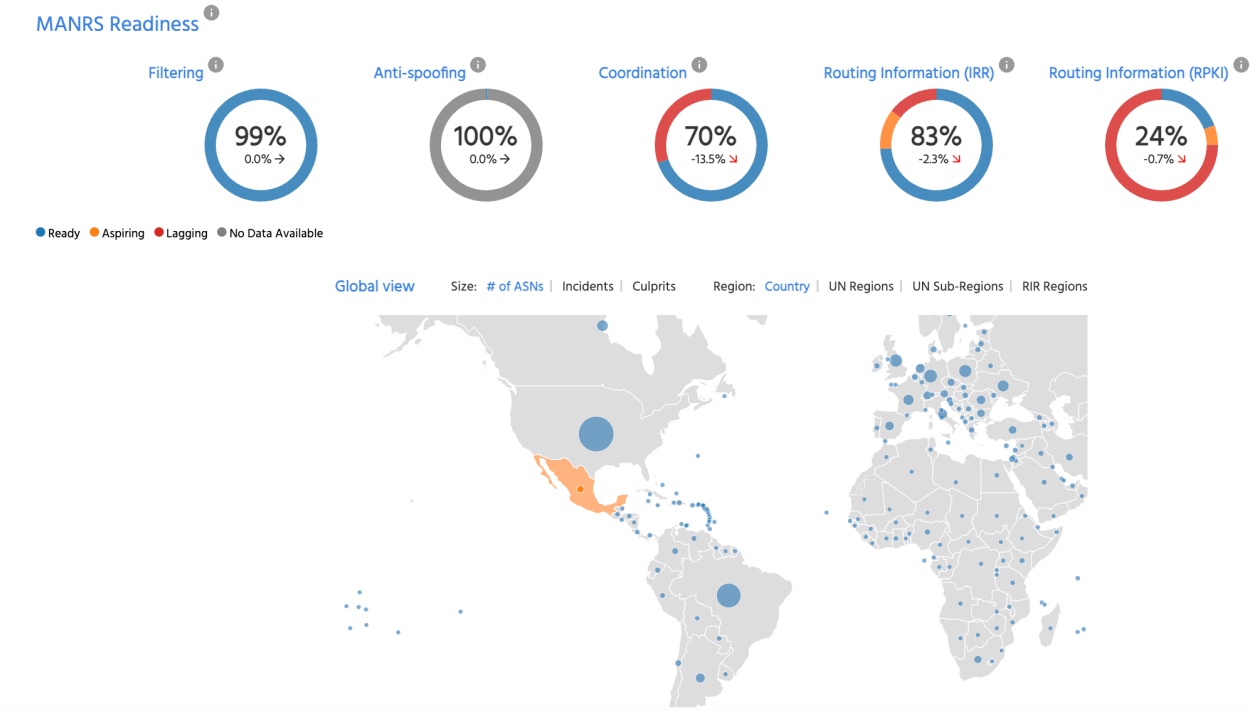
Proporciona soluciones cruciales para reducir las amenazas de enrutamiento más comunes.

socium

MANRS: Estado actual México



MANRS: Estado actual México

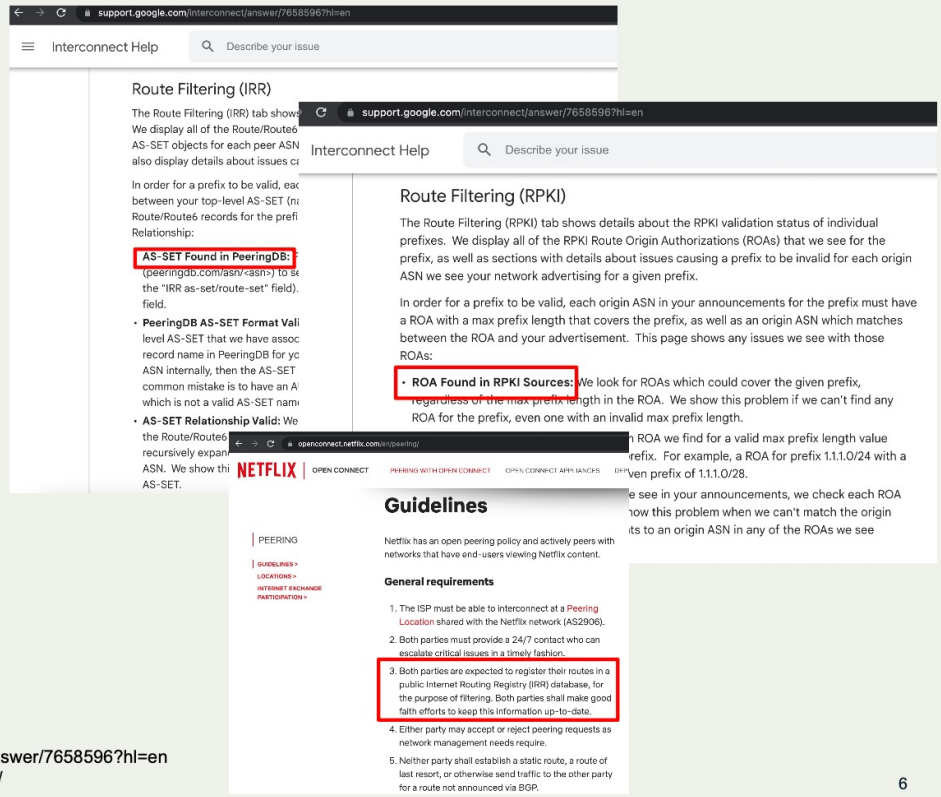


Fuente imagen: facebook.com/casamentormexico

MANRS: Caso Práctico

Caso Práctico

- CDN como Google, Netflix y otras utilizan IRR/RPKI como parte de sus revisiones para entrega de tráfico
- Cada vez el proceso es más automatizado del lado del CDN
- Es escencial no esperar a que se detenga el tráfico para tomar acción



Fuentes: https://support.google.com/interconnect/answer/7658596?hl=en
https://openconnect.netflix.com/en/peering/

Fuente imagen: facebook.com/casamentormexico

MANRS: Acciones a tomar

MANRS Actions for Network Operators

Action 1: Filtering
Prevent propagation of incorrect routing information

Asegure la exactitud de sus propios anuncios y anuncios de sus clientes a redes adyacentes con prefijo y granularidad AS-path.

Action 2: Anti-spoofing
Prevent traffic with spoofed source IP addresses

Habilite la validación de la dirección de origen para al menos una red del cliente que tiene un único punto de entrada y salida, sus propios usuarios finales e infraestructura

Action 3: Coordination
Facilitate global operational communication and coordination between network operators

Mantener la información de contacto actualizada y accesible a nivel mundial en bases de datos de enrutamiento comunes

Action 4: Global Validation
Facilitate validation of routing information on a global scale

Publique sus datos para que otros puedan validar.

IRR/RPKI

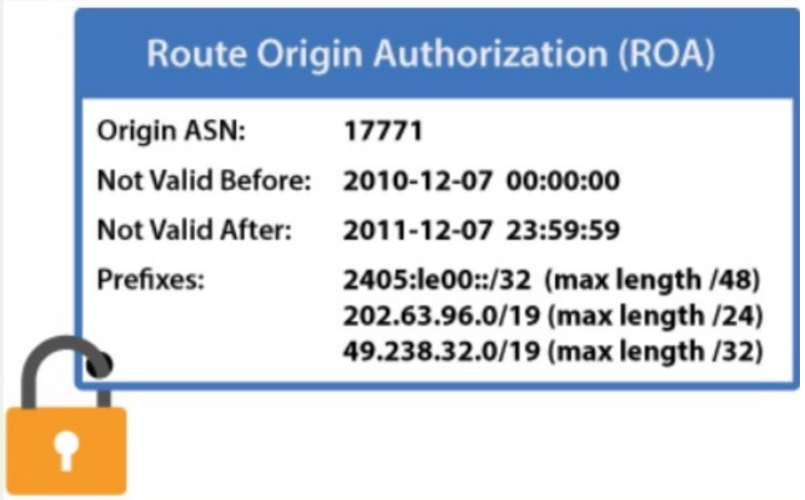
MANRS Implementation Guide https://www.manrs.org/isps/bcop/

MANRS: Creación de ROA

ROA

Adicional a de proporcionar información al sistema IRR, se recomienda que registre las rutas que origina y anime a su cliente a registrar sus rutas en el repositorio RPKI creando allí un objeto de Autorización de Origen de Ruta (ROA).

Los objetos ROA, son objetos firmados criptográficamente que indican los prefijos que un AS está autorizado a originar.



MANRS: Importancia de su implementación

Implementación de Acciones MANRS:

Señala la postura de seguridad avanzada de una organización y puede eliminar las violaciones de SLA que reducen la rentabilidad o el costo de las relaciones con los clientes.

Evita los incidentes de enrutamiento, lo que ayuda a las redes a identificar y abordar fácilmente los problemas con los clientes o peers.

Mejora la eficiencia operativa de una red al establecer vías de comunicación de intercambio de tráfico mejores y más limpias, al mismo tiempo que proporciona información detallada para la resolución de problemas.

Identifica muchas preocupaciones de empresas centradas en la seguridad y otros clientes.

socium

MANRS: ¿Dónde aprender más?

¡Conversemos en nuestro stand!

socium

¡Muchas gracias!

socium


Contacto:
Email: mauricio@socium.cr
Tel: +506 8777-9272
socium
Su aliado seguro