Route Servers – STIX

Los Route Servers (**RS**) facilitan la interconexión multilateral. Una sola sesión BGP con cada RS permite a los participantes ver los prefijos de todos los participantes que también los utilizan.

Los RS conservan el siguiente salto (next-hop) y otros atributos de los prefijos. Los RS nunca enrutan el tráfico, simplemente facilitan el intercambio de prefijos.

Utilización

Ofrecemos 2 RS para resiliencia y pedimos a todos los participantes que establezcan una sesión BGP con ambos. Tener dos servidores también nos permite realizar actualizaciones y mantenimiento seguros sin interrumpir el servicio.

Los miembros de STIX pueden establecer las sesiones BGP con la siguiente información:

RS1 – ASN 64153– IPv4: 45.68.40.1 – IPv6: 2801:19:b800::1
RS2 – ASN 64153– IPv4: 45.68.40.2 – IPv6: 2801:19:b800::2

Para conectarse es necesario que el personal de STIX habilite previamente su sesión BGP.

Filtros de Ingreso

Los servidores de rutas de STIX implementan el filtrado de prefijos utilizando RPKI y datos del Internet Routing Registry de las diversas bases de datos IRR (RIPE, RADB, LACNIC, ARIN, etc.) para permitir a los miembros conectados anunciar solo los prefijos que han registrado públicamente. Si su prefijo tiene un RPKI ROA válido, será aceptado.

Si el resultado de verificación RPKI ROA es no encontrado (aún no ha configurado un ROA), recurriremos a la prueba con IRRDB.

Si un prefijo no tiene un ROA válido (estado inválido) o no está registrado correctamente en el IRRDB, no será aceptado.

Use la pestaña "Filtered Prefixes" y el Looking Glass de los RS en el portal de miembros (https://portal.stix.do) para determinar si se están filtrando los prefijos o si se está acercando al límite máximo de prefijos.

Comunidades BGP

Los participantes RS pueden filtrar sus anuncios de modo que no se envíen a otros participantes. Esto es útil si desea evitar que sus prefijos lleguen a los clientes de tránsito a

través de los RS, o en otras situaciones particulares. La lógica de filtrado se expresa con el uso de comunidades BGP. Las comunidades
grandes (Large Communities LC) también permiten que los prefijos utilicen “prepend” al anunciarse a participantes definidos.

Acción	Standard Community	Large Community
Enviar todos los prefijos a todos los otros participantes del RS (default)	64153:64153	64153:1:0
Enviar un prefijo a un participante del RS con un ASN específico	64153:ASN	64153:1:ASN
No enviar un prefijo a un participante del RS con un ASN específico	0:ASN	64153:0:ASN
No enviar un prefijo a ningún participante del RS	0:64153	64153:0:0
Realizar un prepend a un ASN específico		64153:101:ASN
Realizar un prepend a un ASN específico dos veces		64153:102:ASN
Realizar un prepend a un ASN específico tres veces		64153:103:ASN

Notas sobre las Comunidades

El comportamiento predeterminado si no se especifican comunidades es anunciar todos los prefijos a todos los participantes.

Ejemplo: para anunciar un prefijo solo para AS65001 y AS64500, etiquete el prefijo con las comunidades 0:64153, 64153:65001 y 64153:64500

Ejemplo: para anunciar un prefijo a todos los miembros, excepto AS64500, etiquete el prefijo con la comunidad 0:64500

Las comunidades grandes se evalúan antes que las comunidades BGP estándar.

La mayoría de los miembros querrán enviar sus prefijos a los servidores de ruta y etiquetar a la comunidad 64153:64153 (o 64153:1:0).

Para evitar las limitaciones cuando se utilizan comunidades estándar con ASN de 32 bits, recomendamos utilizar solo comunidades grandes (RFC 8092) si su enrutador lo admite.

La comunidad conocida de RFC 1997 NO_EXPORT (65535: 65281) no es procesada por el RS, sino que se pasa de manera transparente a los participantes. La configuración NO_EXPORT especifica que sus prefijos se anunciarán a los miembros de STIX, pero que ellos no deben anunciarlos a los ASN siguientes u otros ASN externos.

La lógica del uso de comunidades es idéntica para IPv4 e IPv6.

Política de Filtrado

La política de filtrado de los RS de STIX se basa en la configuración de BIRD2 desarrollada por IXP Manager:

- Descartar los prefijos pequeños: mayor que /24 para IPv4 y mayor que /48 para IPv6.
- Descartar todos los "martians" y "bogons" conocidos. (Direcciones privadas y reservadas definidas por RFC 1918, RFC 5735 y RFC 6598).
- Asegurarse de que haya al menos 1 ASN y menos de 64 ASNs en el AS Path.
- Asegurarse de que el ASN del participante sea el mismo que el primer ASN en el AS Path.
- Descartar cualquier prefijo donde la dirección IP del siguiente salto no sea la misma que la dirección IP del participante. Esto evita el secuestro de prefijos.
- Descartar cualquier prefijo con un ASN de una red de tránsito conocida en el AS Path.
- Asegurarse de que el ASN de origen esté en el conjunto de ASN de IRRDB AS-Set del cliente. (Si no se especifica un conjunto, todos los prefijos deben originarse en el ASN del miembro).
- Si el prefijo se evalúa como RPKI válido, aceptarlo.
- Si el prefijo se evalúa como RPKI no válido (inválido), descartarlo.
- Si el prefijo se evalúa como RPKI no encontrado (no existe ROA), vuelva al filtrado del prefijo IRRDB estándar:
    - Todos los ASN de origen deben figurar como miembros: en as-set: (AS Macro) en el IRRDB.
    - Debe haber un objeto route: o route6: con un correcto origin:ASN para que se acepte el prefijo.
- Los RS de STIX aceptan los prefijos IRRDB más específicos, sin embargo, recomendamos un route:object para cada prefijo que pretenda anunciar.
-

Como protección adicional para proteger contra errores de configuración, también se aplica un límite máximo de prefijos. Esto se establece en 50 de forma predeterminada. El RS terminará la sesión BGP si se excede el límite máximo de prefijos. En caso de necesitar aumentar este valor, favor comunicarlo al personal de STIX.