

# Recomendaciones de filtro SA del Protocolo de detección de fuente de multidifusión

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Descripción](#)

[Configuración de la lista de filtro recomendada](#)

[Explicación](#)

[Filtro con grupos de malla del MSDP](#)

[Referencias](#)

[Notas](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento describe cómo configurar un conjunto estándar de reglas de filtrado para los mensajes de Fuente Activa (SA) del Multicast Source Discovery Protocol (MSDP). Cisco recomienda encarecidamente establecer al menos estos filtros al conectar con Internet multicast de IP nativa.

**Nota:** La información de este documento se aplica a todas las versiones actuales del software Cisco IOS® compatibles con MSDP.

## [Prerequisites](#)

## [Requirements](#)

No hay requisitos específicos para este documento.

## [Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

## [Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de](#)

## Descripción

Los mensajes MSDP-SA contienen información (origen, grupo (S,G)) para los puntos de encuentro (RPs) (llamados peers MSDP) en dominios de modo disperso de multidifusión independiente de protocolo (PIM-SM). Este mecanismo les permite a los RP detectar los orígenes de multidifusión en los dominios PIM-SM remotos para que puedan unirse a esos orígenes si existen receptores locales en su propio dominio. También puede utilizar MSDP entre varios RPs en un único dominio PIM-SM para establecer grupos de malla MSDP.

Con una configuración predeterminada, MSDP intercambia mensajes SA sin filtrarlos para un origen o direcciones de grupos en particular.

Generalmente, hay un número de estados (S, G) en el dominio PIM-SM que debería permanecer dentro de ese dominio pero, debido a la filtración predeterminada, pasan en los mensajes SA hacia los pares MSDP. Algunos ejemplos de esto incluyen aplicaciones locales de dominio que utilizan direcciones IP multicast globales y orígenes que utilizan direcciones IP locales (como 10.x.y.z). En el Internet de multidifusión IP nativo, este valor predeterminado hace que se comparta información excesiva (S,G). Para mejorar la escalabilidad de MSDP en el Internet de multidifusión IP nativo y evitar la visibilidad global de la información local de dominio (S,G), recomendamos utilizar la siguiente configuración para reducir la creación, el reenvío y el almacenamiento en caché innecesarios de algunos de estos orígenes locales de dominio conocidos.

## Configuración de la lista de filtro recomendada

Cisco recomienda utilizar el siguiente filtro de configuración para dominios PIM-SM con un solo RP para cada grupo (sin grupo de malla MSDP):

```
!  
    !--- Filter MSDP SA-messages. !--- Replicate the following two rules for every external  
MSDP peer. ! ip msdp sa-filter in <peer_address> list 111 ip msdp sa-filter out <peer_address>  
list 111 ! !--- The redistribution rule is independent of peers. ! ip msdp redistribute list 111  
! !--- ACL to control SA-messages originated, forwarded. ! !--- Domain-local applications.  
access-list 111 deny ip any host 224.0.2.2 ! access-list 111 deny ip any host 224.0.1.3 ! Rwhod  
access-list 111 deny ip any host 224.0.1.24 ! Microsoft-ds access-list 111 deny ip any host  
224.0.1.22 ! SVRLOC access-list 111 deny ip any host 224.0.1.2 ! SGI-Dogfight access-list 111  
deny ip any host 224.0.1.35 ! SVRLOC-DA access-list 111 deny ip any host 224.0.1.60 ! hp-device-  
disc !--- Auto-RP groups. access-list 111 deny ip any host 224.0.1.39 access-list 111 deny ip  
any host 224.0.1.40 !--- Scoped groups. access-list 111 deny ip any 239.0.0.0 0.255.255.255 !---  
Loopback, private addresses (RFC 1918). access-list 111 deny ip 10.0.0.0 0.255.255.255 any  
access-list 111 deny ip 127.0.0.0 0.255.255.255 any access-list 111 deny ip 172.16.0.0  
0.15.255.255 any access-list 111 deny ip 192.168.0.0 0.0.255.255 any !--- Default SSM-range. Do  
not do MSDP in this range. access-list 111 deny ip any 232.0.0.0 0.255.255.255 access-list 111  
permit ip any any ! !
```

## Explicación

En el ejemplo anterior, la lista de acceso 111 (puede utilizar cualquier número) define la información de SA local del dominio. Esto incluye el estado (S,G) para grupos globales utilizado por las aplicaciones locales del dominio, los dos grupos RP automáticos, los grupos de alcance y

el estado (S,G) de las direcciones de IP locales.

Esta lista de filtros se aplica para que el router local no acepte información de SA local de dominio de peers MSDP externos y que los peers MSDP externos nunca obtengan información de SA o información local de dominio del router.

El comando `ip msdp sa-filter en <peer_address> list 111` filtra la información local de los mensajes SA recibidos del peer de MSDP `<peer_address>`. Si configura este comando en cada peer MSDP externo, entonces el propio router no aceptará ninguna información local de dominio desde fuera del dominio.

El comando `ip msdp sa-filter out <peer_address> lista 111` filtra la información local del dominio desde los anuncios SA enviados al peer MSDP `<peer_address>`. Si configura este comando en cada peer MSDP externo, no se anuncia ninguna información local del dominio fuera del dominio.

Incluimos el comando `ip msdp redistribute list 111` para brindar mayor seguridad. Impide que el router origine mensajes SA para el estado local (S,G) del dominio. Esta acción es independiente del filtrado de mensajes SA enviados que causó el comando `ip msdp sa-filter out`.

## Filtro con grupos de malla del MSDP

Si el dominio PIM-SM utiliza un grupo de malla MSDP, entonces hay pares MSDP internos del dominio. Para esta situación, es necesario examinar más a fondo la configuración descrita anteriormente.

Debe aplicar las reglas `ip msdp sa-filter in` e `ip msdp sa-filter out` para pares MSDP externos únicamente. Si los aplica a los peers MSDP internos, toda la información SA filtrada por la lista de acceso 111 no se transmitirá entre peers internos, que interrumpe cualquier aplicación usando las direcciones de origen o de grupo filtradas por la lista de acceso 111 (a menos que, como en el caso de los grupos de RP automático, los grupos utilicen PIM-DM en lugar de PIM-SM).

Cisco recomienda no configurar el comando `ip msdp redistribute list 111` porque evita que el RP origine mensajes SA para el estado local del dominio (S,G). Este comando interrumpe toda aplicación local del dominio que dependa de él. Dado que este comando se incluye para mayor seguridad, eliminarlo no modificará el modo en que los mensajes son filtrados entre los pares MSDP externos.

**Nota:** Debe aplicar consistentemente el filtrado descrito aquí a todos los RP dentro del grupo de malla MSDP.

## Referencias

La [documentación de MSDP sobre CCO](#) describe los comandos MSDP.

Los siguientes comandos filtran los mensajes SA:

- `ip msdp sa-filter en <peer> [list <acl>] [route-map <map>]:` define qué mensajes SA recibidos de los peers MSDP son aceptados. De forma predeterminada, todos los mensajes SA se aceptan si pasan las comprobaciones de Reenvío de Trayectoria Inversa (RPF) de MSDP descritas en este [documento MSDP](#).

- **ip msdp redistribute** [list <acl>] [asn <aspath-acl>] [route-map <map>]: *define para qué información (S,G) el router local origina mensajes SA.* De forma predeterminada, los mensajes SA se originan para todos los orígenes que coinciden con uno de los siguientes criterios: Registro recibido. Conexión directa. Los datos recibidos en la misma interfaz de modo denso y RPF a la que se originará. **Nota:** Cuando se cumple una de estas reglas, se establece un indicador "A" en la entrada (S,G) correspondiente a ese origen en Cisco IOS® Software Release 12.0(6) o posterior.
- **ip msdp sa-filter out** <peer> [list <acl>] [route-map <map>]: *define qué mensajes SA que se han originado localmente o que se han aceptado de peers MSDP se reenvían a otros peers MSDP.* De forma predeterminada, todos los mensajes SA originados localmente y todos los mensajes SA recibidos y aceptados se envían a otros peers MSDP.

## Notas

Para minimizar la necesidad de actualizar continuamente la lista de filtros recomendada anteriormente, las aplicaciones locales de dominio siempre deben utilizar direcciones de grupo con ámbito o direcciones de origen privadas de forma predeterminada. En el límite de dominio, estas direcciones se filtran mediante el filtrado de mensajes SA y por las definiciones de límite multicast para las direcciones multicast alcanzadas.

## Información Relacionada

- [Página de Soporte de IP Routing](#)
- [Soporte Técnico - Cisco Systems](#)