

Recomendações de filtragem do SA do Protocolo de descoberta de origem da multicast

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Descrição](#)

[Configuração recomendada da lista de filtro](#)

[Explicação](#)

[Filtrando com grupos de malha MSDP](#)

[Referências](#)

[Notas](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como configurar um conjunto padrão de regras de filtragem para mensagens ativas na fonte (SA) do protocolo de descoberta de origem multicast (MSDP). A Cisco recomenda enfaticamente estabelecer pelo menos estes três filtros ao conectar com a internet do IP multicast.

Observação: as informações neste documento se aplicam a todas as versões atuais do software Cisco IOS® compatíveis com MSDP.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

[Conventions](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Descrição

As mensagens MSDP-SA contêm informações (origem, grupo (S,G)) para pontos de encontro (RPs) (chamados peers MSDP) em domínios de modo esparsa de envio múltiplo independente de protocolo (PIM-SM). Esse mecanismo permite que os RPs aprendam sobre origens de transmissão múltipla em domínios PIM-SM remotos de modo que eles possam se unir a essas origens se houver receptores locais em seus próprios domínios. Você também pode usar o MSDP entre vários RPs em um único domínio PIM-SM para estabelecer grupos de malha MSDP.

Com uma configuração padrão, o MSDP troca mensagens de SA sem as filtrar quanto a origem específica ou endereços de grupo.

Em geral, existem vários estados (S,G) em um domínio PIM-SM que devem permanecer no domínio PIM-SM, mas, devido à filtragem padrão, eles são transmitidos em mensagens SA aos correspondentes MSDP. Exemplos disso incluem aplicativos locais de domínio que usam endereços IP multicast globais e fontes que usam endereços IP locais (como 10.x.y.z). Na Internet multicast IP nativa, esse padrão leva ao compartilhamento de informações excessivas (S,G). Para melhorar a escalabilidade do MSDP na Internet multicast IP nativa e para evitar a visibilidade global das informações de domínio local (S,G), recomendamos usar a seguinte configuração para reduzir a criação, encaminhamento e cache desnecessários de algumas dessas fontes locais de domínio conhecidas.

Configuração recomendada da lista de filtro

A Cisco recomenda o uso do seguinte filtro de configuração para domínios PIM-SM com um único RP para cada grupo (sem grupo de malha 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 ! !
```

Explicação

No exemplo acima, a lista de acesso 111 (você pode usar qualquer número) define as informações SA locais do domínio. Isso inclui o estado (S,G) para grupos globais usados pelos aplicativos de domínio locais, os dois grupos auto-RP, grupos de escopo e estado (S,G) dos endereços IP locais.

Essa lista de filtros é aplicada de modo que o roteador local não aceite informações SA locais de domínio de peers MSDP externos e que os peers MSDP externos nunca obtenham informações

SA ou informações locais de domínio do roteador.

O comando `ip msdp sa-filter em <peer_address> list 111` filtra as informações locais das mensagens SA recebidas do peer MSDP `<peer_address>`. Se você configurar esse comando em cada peer MSDP externo, o próprio roteador não aceitará nenhuma informação local de domínio de fora do domínio.

O comando `ip msdp sa-filter out <peer_address> list 111` filtra as informações locais do domínio dos anúncios SA enviados ao peer MSDP `<peer_address>`. Se você configurar esse comando em cada peer MSDP externo, nenhuma informação local de domínio será anunciada fora do domínio.

Nós incluímos o comando `ip msdp redistribute list 111` para fornecer mais segurança. Evita que o roteador origine mensagens SA para o estado local do domínio (S,G). Essa ação é independente da filtragem do envio de mensagens SA causadas pelo comando `ip msdp sa-filter out`.

Filtrando com grupos de malha MSDP

Se o domínio PIM-SM usa um grupo de malha MSDP, então há peers MSDP internos do domínio. Para essa situação, a configuração descrita acima precisa ser examinada mais a fundo.

Você deve aplicar as regras `ip msdp sa-filter in` e `ip msdp sa-filter out` somente para peers MSDP externos. Se você aplicá-las aos peers MSDP internos, todas as informações de SA filtradas pela lista de acesso 111 não serão passadas entre peers internos, o que interrompe qualquer aplicativo usando os endereços de origem ou de grupo filtrados pela lista de acesso 111 (a menos que, como no caso dos grupos de RP automático, os grupos usem PIM-DM em vez de PIM-SM).

A Cisco recomenda não configurar o comando `ip msdp redistribute list 111` porque impede que o RP origine mensagens SA para o estado local do domínio (S,G). Esse comando interrompe qualquer aplicativo de domínio local que dependa dele. Como esse comando está incluso para aumentar a segurança, a sua remoção não alterará o modo como as mensagens são filtradas entre correspondentes MSDP externos.

Observação: você deve aplicar consistentemente a filtragem descrita aqui a todos os RPs dentro do grupo de malha MSDP.

Referências

A [documentação do MSDP no CCO](#) descreve os comandos de MSDP.

Os seguintes comandos filtram mensagens SA:

- `ip msdp sa-filter em <peer> [list <acl>] [route-map <map>]` - Define quais mensagens SA recebidas de peers MSDP são aceitas. Por padrão, todas as mensagens de SA são aceitas se passarem pelas verificações de RPF (Reverse Path Forwarding) do MSDP descritas neste [documento do MSDP](#).
- `ip msdp redistribute [list <acl>] [asn <aspath-acl>] [route-map <map>]` - Define para quais informações (S,G) o roteador local origina mensagens SA. Por padrão, as mensagens SA são originadas para todas as fontes que correspondem a um dos seguintes critérios: Registro recebido. Diretamente conectado. Dados recebidos em, e RPF para origem através da mesma interface denso-mode-only. **Observação:** quando uma dessas regras é satisfeita, um

sinalizador "A" é definido na entrada (S,G) correspondente a essa origem no Cisco IOS® Software Release 12.0(6) ou posterior.

- `ip msdp sa-filter out <peer> [list <acl/>] [route-map <map>]` - Define quais mensagens SA originadas localmente ou que foram aceitas de peers MSDP são encaminhadas para outros peers MSDP. Por padrão, todas as mensagens SA originadas localmente e todas as mensagens SA recebidas e aceitas são enviadas para outros peers MSDP.

Notas

Para minimizar a necessidade de atualizar continuamente a lista de filtros recomendada acima, os aplicativos locais de domínio devem sempre usar endereços de grupo com escopo ou endereços de origem privada por padrão. No limite de domínio, esses endereços são filtrados por filtragem de mensagens SA e por definições de limite de multicast para os endereços multicast com escopo.

Informações Relacionadas

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