

# Empfehlungen für den SA-Filter des Multicast Source Discovery Protocol

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Beschreibung](#)

[Empfohlene Filterlistenkonfiguration](#)

[Erläuterung](#)

[Filterung mit MSDP Mesh Groups](#)

[Referenzen](#)

[Hinweise](#)

[Zugehörige Informationen](#)

## [Einführung](#)

In diesem Dokument wird beschrieben, wie ein Standardsatz von Filterregeln für MSDP-Source-Active (SA)-Nachrichten (Multicast Source Discovery Protocol) konfiguriert wird. Cisco empfiehlt dringend, bei der Verbindung mit dem nativen IP-Multicast-Internet mindestens diese Filter einzurichten.

**Hinweis:** Die Informationen in diesem Dokument gelten für alle aktuellen MSDP-fähigen Cisco IOS® Software-Versionen.

## [Voraussetzungen](#)

### [Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

### [Verwendete Komponenten](#)

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

### [Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

## Beschreibung

MSDP-SA-Nachrichten enthalten Informationen (Quelle, Gruppe (S,G)) für Rendezvous Points (RPs) (als MSDP-Peers bezeichnet) in PIM-SM-Domänen (Protocol Independent Multicast Sparse Mode). Dieser Mechanismus ermöglicht es RPs, Informationen über Multicast-Quellen in Remote-PIM-SM-Domänen zu erhalten, sodass sie diese Quellen verbinden können, wenn es lokale Empfänger in ihrer eigenen Domäne gibt. Sie können MSDP auch zwischen mehreren RPs in einer einzigen PIM-SM-Domäne verwenden, um MSDP-Mesh-Gruppen einzurichten.

Bei einer Standardkonfiguration tauscht MSDP SA-Nachrichten aus, ohne sie für bestimmte Quell- oder Gruppenadressen zu filtern.

In der Regel gibt es eine Reihe von (S,G)-Zuständen in einer PIM-SM-Domäne, die innerhalb der PIM-SM-Domäne verbleiben sollten. Aufgrund der Standardfilterung werden sie jedoch in SA-Nachrichten an MSDP-Peers übergeben. Beispiele hierfür sind domänenlokale Anwendungen, die globale IP-Multicast-Adressen verwenden, und Quellen, die lokale IP-Adressen verwenden (z. B. 10.x.y.z). Im nativen IP-Multicast-Internet führt dieser Standardwert dazu, dass übermäßige (S,G)-Informationen freigegeben werden. Um die Skalierbarkeit von MSDP im nativen IP-Multicast-Internet zu verbessern und die globale Transparenz von Domain Local (S,G)-Informationen zu vermeiden, empfehlen wir die Verwendung der folgenden Konfiguration, um die unnötige Erstellung, Weiterleitung und Zwischenspeicherung einiger dieser bekannten lokalen Domänen-Quellen zu reduzieren.

## Empfohlene Filterlistenkonfiguration

Cisco empfiehlt die Verwendung des folgenden Konfigurationsfilters für PIM-SM-Domänen mit einem einzigen RP für jede Gruppe (keine MSDP-Mesh-Gruppe):

```
!  
! --- 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 ! !
```

## Erläuterung

Im obigen Beispiel definiert die Zugriffsliste 111 (Sie können eine beliebige Zahl verwenden) die lokalen SA-Informationen der Domäne. Dies umfasst den (S,G)-Status für globale Gruppen, die von lokalen Domänenanwendungen verwendet werden, die beiden Auto-RP-Gruppen, die Gruppen mit Gültigkeitsbereich und den (S,G)-Status von lokalen IP-Adressen.

Diese Filterliste wird angewendet, sodass der lokale Router domänenlokale SA-Informationen von

externen MSDP-Peers nicht akzeptiert und externe MSDP-Peers niemals SA-Informationen oder lokale Domäneninformationen vom Router erhalten.

Der Befehl **ip msdp sa-filter in der Liste 111** filtert lokale Informationen aus SA-Nachrichten, die vom MSDP-Peer *<peer\_address>* empfangen wurden. Wenn Sie diesen Befehl auf jedem externen MSDP-Peer konfigurieren, akzeptiert der Router selbst keine lokalen Domäneninformationen von außerhalb der Domäne.

Der Befehl **ip msdp sa-filter out <peer\_address>list 111** filtert domänenspezifische Informationen aus SA-Ankündigungen, die an MSDP-Peer *<peer\_address>* gesendet wurden. Wenn Sie diesen Befehl auf jedem externen MSDP-Peer konfigurieren, werden außerhalb der Domäne keine lokalen Domäneninformationen angekündigt.

Zur Erhöhung der Sicherheit wurde der Befehl **ip msdp redistribute list 111** hinzugefügt. Er verhindert, dass der Router SA-Nachrichten für den lokalen (S,G) Domänenstatus ausgibt. Diese Aktion ist unabhängig von der Filterung gesendeter SA-Nachrichten, die durch den Befehl **ip msdp sa-filter out** verursacht werden.

## Filterung mit MSDP Mesh Groups

Wenn die PIM-SM-Domäne eine MSDP-Mesh-Gruppe verwendet, gibt es domäneninterne MSDP-Peers. In diesem Fall muss die oben beschriebene Konfiguration weiter geprüft werden.

Sie sollten die **ip msdp sa-filter in-** und **ip msdp sa-filter out-**Regeln nur auf externe MSDP-Peers anwenden. Wenn Sie sie auf interne MSDP-Peers anwenden, werden alle SA-Informationen, die nach der Zugriffsliste 111 gefiltert werden, nicht zwischen internen Peers weitergegeben. Diese werden dann nicht über die Quell- oder Gruppenadressen getrennt, die durch die Zugriffsliste 111 gefiltert wurden (es sei denn, wie bei Auto-RP-Gruppen werden die Gruppen PIM-DM anstelle von PIM-SM verwendet).

Cisco empfiehlt, den Befehl **ip msdp redistribute list 11** nicht zu konfigurieren, da er verhindert, dass der RP SA-Nachrichten für den lokalen (S,G)-Status generiert. Dieser Befehl unterbricht alle von ihm abhängigen lokalen Domänenanwendungen. Da dieser Befehl zur Erhöhung der Sicherheit enthalten ist, ändert das Entfernen des Befehls nicht, wie Nachrichten zwischen externen MSDP-Peers gefiltert werden.

**Hinweis:** Sie sollten die hier beschriebene Filterung konsistent auf alle RPs innerhalb der MSDP-Mesh-Gruppe anwenden.

## Referenzen

Die [MSDP-Dokumentation zu CCO](#) beschreibt MSDP-Befehle.

Die folgenden Befehle filtern SA-Nachrichten:

- **ip msdp sa-filter in <peer> [list <acl>] [route-map <map>]** - Definiert, welche SA-Nachrichten von MSDP-Peers akzeptiert werden. Standardmäßig werden alle SA-Nachrichten akzeptiert, wenn sie die in diesem [MSDP-Dokument](#) beschriebenen MSDP Reverse Path Forwarding (RPF)-Prüfungen bestehen.
- **ip msdp redistribute [list <acl>] [asn <aspath-acl>] [route-map <map>]** - Definiert, für welche

(S,G)-Informationen der lokale Router SA-Nachrichten generiert. Standardmäßig werden SA-Nachrichten für alle Quellen generiert, die eines der folgenden Kriterien erfüllen: Registrierung erhalten. Direkt verbunden. Daten, die an derselben Nur-Dense-Mode-Schnittstelle empfangen werden, und RPF für die Quelle. **Hinweis:** Wenn eine dieser Regeln erfüllt ist, wird auf dem (S,G)-Eintrag, der dieser Quelle in Cisco IOS® Softwareversion 12.0(6) oder höher entspricht, eine "A"-Markierung festgelegt.

- **ip msdp sa-filter out <peer> [list <acl/>] [route-map <map>]** - Definiert, welche SA-Nachrichten, die lokal generiert wurden oder von MSDP-Peers akzeptiert wurden, an andere MSDP-Peers weitergeleitet werden. Standardmäßig werden alle lokal generierten SA-Nachrichten sowie alle empfangenen und akzeptierten SA-Nachrichten an andere MSDP-Peers gesendet.

## Hinweise

Um die Notwendigkeit einer kontinuierlichen Aktualisierung der oben empfohlenen Filterliste zu minimieren, sollten domänenlokale Anwendungen standardmäßig Gruppen- oder private Quelladressen verwenden. Auf der Domänengrenze werden diese Adressen durch die SA-Nachrichtenfilterung und durch Multicast-Grenzdefinitionen für die betreffenden Multicast-Adressen gefiltert.

## Zugehörige Informationen

- [Support-Seite für IP-Routing](#)
- [Technischer Support - Cisco Systems](#)