Multicast Source Discovery Protocol SA Filter Recommendations

Document ID: 13717

Contents

Introduction

This document describes how to configure a standard set of filtering rules for Multicast Source Discovery Protocol (MSDP) Source−Active (SA) messages. Cisco highly recommends establishing at least these filters when connecting to the native IP multicast Internet.

Note: The information in this document applies to all current MSDP capable Cisco IOS® Software Releases.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Description

MSDP−SA messages contain (source, group (S,G)) information for rendezvous points (RPs) (called MSDP peers) in Protocol Independent Multicast sparse−mode (PIM−SM) domains. This mechanism allows RPs to learn about multicast sources in remote PIM−SM domains so that they can join those sources if there are local receivers in their own domain. You can also use MSDP between multiple RPs in a single PIM−SM domain to establish MSDP mesh−groups.

With a default configuration, MSDP exchanges SA messages without filtering them for specific source or group addresses.

Typically, there are a number of (S,G) states in a PIM−SM domain that should stay within the PIM−SM domain, but, due to default filtering, they get passed in SA messages to MSDP peers. Examples of this include domain local applications that use global IP multicast addresses, and sources that use local IP addresses (such as 10.x.y.z). In the native IP multicast Internet, this default leads to excessive (S,G) information being shared. To improve the scalability of MSDP in the native IP multicast Internet, and to avoid global visibility of domain local (S,G) information, we recommend using the following configuration to reduce unnecessary creation, forwarding, and caching of some of these well−known domain local sources.

Recommended Filter List Configuration

Cisco recommends using the following configuration filter for PIM−SM domains with a single RP for every group (no MSDP mesh−group):

```
!

!--- 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
!
!
```

Explanation

In the example above, access list 111 (you can use any number) defines domain local SA−information. This includes (S,G) state for global groups used by domain local applications, the two auto−RP groups, scoped groups, and (S,G) state from local IP addresses.

This filter list is applied so that the local router does not accept domain−local SA−information from external MSDP peers and that external MSDP peers never get SA−information or domain local information from the router.

The **ip msdp sa−filter in** *<peer_address>* **list 111** command filters local information from SA messages received from MSDP peer *<peer_address>*. If you configure this command on every external MSDP peer, then the router itself will not accept any domain local information from outside the domain.

The **ip msdp sa−filter out** *<peer_address>* **list 111** command filters domain local information from SA announcements sent to MSDP peer *<peer_address>*. If you configure this command on every external MSDP peer, then no domain local information is announced outside the domain.

We included the **ip msdp redistribute list 111** command for added safety. It prevents the router from originating SA messages for domain local (S,G) state. This action is independent of the filtering of sent SA messages caused by the **ip msdp sa−filter out** command.

Filtering with MSDP Mesh−Groups

If the PIM−SM domain uses an MSDP mesh−group, then there are domain internal MSDP peers. For this situation, the configuration described above needs to be examined further.

You should apply the **ip msdp sa−filter in** and **ip msdp sa−filter out** rules to external MSDP peers only. If you apply them to internal MSDP peers, all SA information filtered by access−list 111 will not be passed between internal peers, which breaks any application using the source or group addresses filtered by access−list 111 (unless, as in the case of auto−RP groups, the groups use PIM−DM instead of PIM−SM).

Cisco recommends not configuring the **ip msdp redistribute list 111** command because it prevents the RP from originating SA messages for domain local (S,G) state. This command breaks any domain local application that depends on it. Since this command is included for added safety, removing it will not change how messages are filtered between external MSDP peers.

Note: You should consistently apply the filtering described here to all RPs within the MSDP mesh−group.

References

The MSDP Documentation on CCO describes MSDP commands.

The following commands filter SA messages:

- **ip msdp sa−filter in** *<peer>* **[list** *<acl>*] **[route−map** *<map>*] – Defines which SA messages

received from MSDP peers are accepted. By default, all SA messages are accepted if they pass the MSDP Reverse Path Forwarding (RPF) checks outlined in this MSDP document.

- **ip msdp redistribute [list** *<acl>***] [asn** *<aspath−acl>***] [route−map** *<map>***]** − Defines for which (S,G) information the local router originates SA messages. By default, SA messages are originated for all sources that match one of the following criteria:

  - ♦ Register received.
  - ♦ Directly connected.
  - ♦ Data received on, and RPF to source through, the same dense−mode−only interface.

    Note: When one of these rules is satisfied, an "A" flag is set on the (S,G) entry corresponding to that source in Cisco IOS® Software Release 12.0(6) or later.

- **ip msdp sa−filter out** *<peer>* **[list** *<acl>***] [route−map** *<map>***]** − Defines which SA messages that have originated locally or been accepted from MSDP peers are forwarded to other MSDP peers. By default, all locally−originated SA messages and all received and accepted SA messages are sent to other MSDP peers.

Notes

To minimize the need to continuously update the filter list recommended above, domain local applications should always use scoped group addresses or private source addresses by default. On the domain boundary, these addresses are filtered by SA−message filtering and by multicast boundary definitions for the scoped multicast addresses.

Related Information

- **IP Routing Support Page**
- **Technical Support − Cisco Systems**

Updated: Aug 10, 2005   Document ID: 13717