PIX/ASA 7.x：PIX/ASA平台上外部发送方的组播用配置示例

目录

简介

本文档为运行版本 7.x 的 Cisco 自适应安全设备 (ASA) 和/或 PIX 安全设备上的多播配置提供了一个范例。在本示例中，多播发送方位于安全设备外部，而位于内部的主机尝试接收多播流量。主机向报告组成员发送 IGMP 报告，防火墙使用独立于协议的多播 (PIM) 稀疏模式作为针对上游路由器的动态多播路由协议（数据流的源位于上游路由器之后）。

注意： FWSM/ASA 不支持 232.x.x.x/8 子网作为组编号，因为它是为 ASA SSM 保留的。因此，FWSM/ASA 不允许使用或穿越此子网，并且不会创建多播路由。但是，如果将其封装在 GRE 隧道中，则仍可以通过 ASA/FWSM 传递此多播流量。

先决条件

要求

允许软件版本 7.0、7.1 或 7.2 的 Cisco PIX 或 ASA 安全设备。

使用的组件

本文档中的信息基于运行版本 7.x 的 Cisco PIX 或 Cisco ASA 防火墙。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

PIX/ASA 7.x 为通过防火墙的动态多播路由引入了完全 PIM 稀疏模式和双向支持。不支持 PIM 密集模式。7.x 软件仍支持传统多播的残域模式，其中防火墙只是接口之间的 IGMP 代理（PIX 版本 6.x 支持此模式）。

对于通过防火墙的多播流量，适用以下说明：

- 如果为接收多播流量的接口应用了访问列表，则访问控制列表 (ACL) 必须明确允许该流量。如果接口没有应用访问列表，则并非必须具有允许多播流量的明确 ACL 条目。
- 多播数据包始终要接受防火墙的反向路径转发检查，而不管接口是否配置了 **reverse-path forward check** 命令。因此，如果在接收数据包的接口上没有指向多播数据包源的路由，则会丢弃该数据包。
- 如果接口上没有返回多播数据包源的路由，可以使用 **mroute** 命令指示防火墙不要丢弃该数据包。

配置

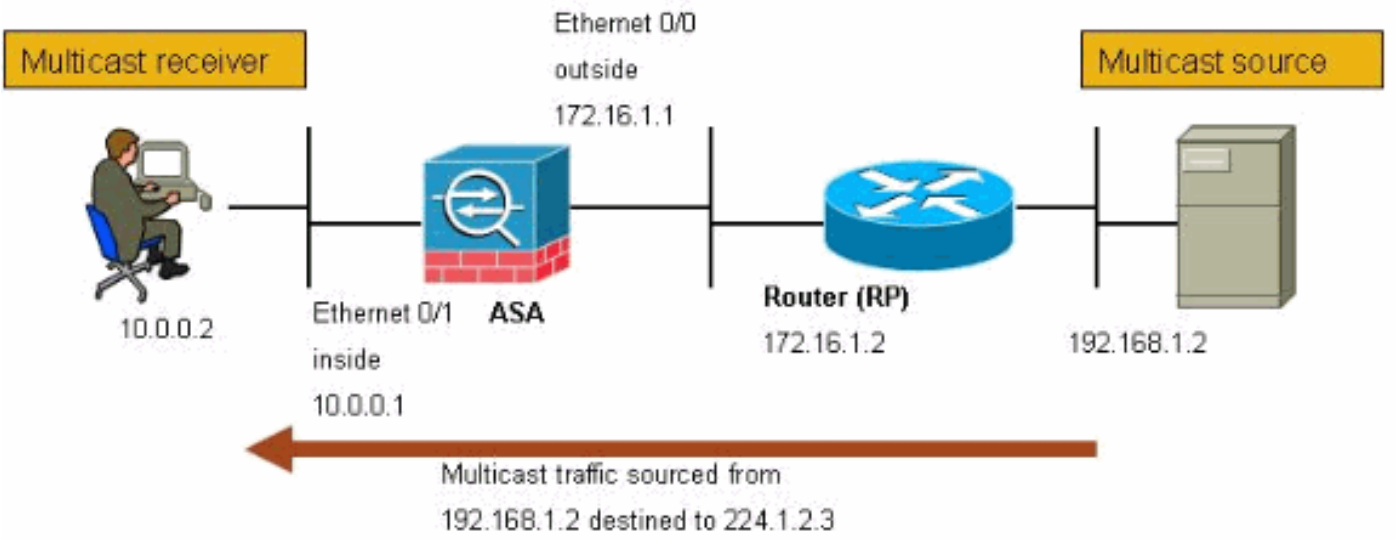
本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用此网络设置。

多播流量源自 192.168.1.2 并在指向组 224.1.2.3 的端口 1234 上使用 UDP 数据包。



配置

本文档使用以下配置：

允许版本 7.x 的 Cisco PIX 或 ASA 防火墙

```
maui-soho-01#show running-config SA Version 7.1(2) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted !--- The multicast-routing command enables
IGMP and PIM !--- on all interfaces of the firewall.
multicast-routing names ! interface Ethernet0/0 nameif
outside security-level 0 ip address 172.16.1.1
255.255.255.0 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 10.0.0.1 255.255.255.0 !
interface Ethernet0/2 no nameif no security-level no ip
address ! interface Ethernet0/3 shutdown no nameif no
security-level no ip address ! interface Management0/0
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted !--- The rendezvous
point address must be defined in the !--- configuration
in order for PIM to function correctly. pim rp-address
172.16.1.2 boot system disk0:/asa712-k8.bin ftp mode
passive !--- It is necessary to permit the multicast
traffic with an !--- access-list entry. access-list
outside_access_inbound extended permit ip any host
224.1.2.3 pager lines 24 logging enable logging buffered
debugging mtu outside 1500 mtu inside 1500 no failover
!--- The access-list that permits the multicast traffic
is applied !--- inbound on the outside interface.
access-group outside_access_inbound in interface outside
!--- This mroute entry specifies that the multicast
sender !--- 192.168.1.2 is off the outside interface. In
this example !--- the mroute entry is necessary since
the firewall has no route to !--- the 192.168.1.2 host
on the outside interface. Otherwise, this !--- entry is
not necessary. mroute 192.168.1.2 255.255.255.255
outside icmp permit any outside asdm image
disk0:/asdm521.bin no asdm history enable arp timeout
14400 timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout
mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout
```

```
uauth 0:05:00 absolute no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart telnet timeout
5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect ftp inspect h323 h225 inspect h323 ras inspect
rsh inspect rtsp inspect esmtp inspect sqlnet inspect
skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp ! service-policy global_policy
global ! end
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show mroute** — 显示 IPv4 多播路由表。`ciscoasa#show mroute Multicast Routing Table Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected, L - Local, I - Received Source Specific Host Report, P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT Timers: Uptime/Expires Interface state: Interface, State` *`!--- Here you see the mroute entry for the shared tree. Notice that the !--- incoming interface specifies outside and that the outgoing interface !--- list specifies inside.`* `(*, 224.1.2.3), 00:00:12/never, RP 172.16.1.2, flags: SCJ Incoming interface: outside RPF nbr: 172.16.1.2 Outgoing interface list: inside, Forward, 00:00:12/never` *`!--- Here is the source specific tree for the mroute entry.`* `(192.168.1.2, 224.1.2.3), 00:00:12/00:03:17, flags: SJ Incoming interface: outside RPF nbr: 0.0.0.0 Immediate Outgoing interface list: Null`
- **show conn** — 显示指定连接类型的连接状态。
  `!--- A connection is built through the firewall for the multicast stream. !--- In this case the stream is sourced from the sender IP and destined !--- to the multicast group.`
  `ciscoasa#show conn 10 in use, 12 most used UDP out 192.168.1.2:51882 in 224.1.2.3:1234 idle 0:00:00 flags - ciscoasa#`
- **show pim neighbor** — 显示 PIM 邻接表中的条目。
  `!--- When you use PIM, the neighbor devices should be seen with the !--- show pim neighbor command.` `ciscoasa#show pim neighbor Neighbor Address Interface Uptime Expires DR pri Bidir 172.16.1.2 outside 04:06:37 00:01:27 1 (DR)`

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除步骤

请按照以下说明排除配置故障。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

1. 如果多播接收方直接连接到防火墙内部，则会发送 IGMP 报告以接收多播流。可以使用 **show igmp traffic** 命令以验证您是否从内部接收 IGMP 报告。`ciscoasa#show igmp traffic IGMP Traffic Counters Elapsed time since counters cleared: 04:11:08 Received Sent Valid IGMP`

Packets 413 244 Queries 128 244 Reports 159 0 Leaves 0 0 Mtrace packets 0 0 DVMRP packets 0 0 PIM packets 126 0 Errors: Malformed Packets 0 Martian source 0 Bad Checksums 0 ciscoasa#

2. 通过使用 **debug igmp** 命令，防火墙可以显示有关 IGMP 数据的更详细信息。在本例中，启用了调试并且主机 10.0.0.2 为组 224.1.2.3 发送 IGMP 报告。

```
!--- Enable IGMP debugging. ciscoasa#debug igmp IGMP debugging is on ciscoasa# IGMP:
Received v2 Report on inside from 10.0.0.2 for 224.1.2.3 IGMP: group_db: add new group
224.1.2.3 on inside IGMP: MRIB updated (*,224.1.2.3) : Success IGMP: Switching to EXCLUDE
mode for 224.1.2.3 on inside IGMP: Updating EXCLUDE group timer for 224.1.2.3 ciscoasa# !--
- Disable IGMP debugging ciscoasa#un all
```

3. 验证防火墙具有有效 PIM 邻居并且防火墙可以发送和接收加入/修剪信息。

```
ciscoasa#show pim neigh Neighbor Address Interface Uptime Expires DR pri Bidir 172.16.1.2 outside 04:26:58
00:01:20 1 (DR) ciscoasa#show pim traffic PIM Traffic Counters Elapsed time since counters
cleared: 04:27:11 Received Sent Valid PIM Packets 543 1144 Hello 543 1079 Join-Prune 0 65
Register 0 0 Register Stop 0 0 Assert 0 0 Bidir DF Election 0 0 Errors: Malformed Packets 0
Bad Checksums 0 Send Errors 0 Packet Sent on Loopback Errors 0 Packets Received on PIM-
disabled Interface 0 Packets Received with Unknown PIM Version 0 Packets Received with
Incorrect Addressing 0 ciscoasa#
```

4. 使用 **capture** 命令以验证外部接口接收组的多播数据包。

```
ciscoasa#configure terminal !---
Create an access-list that is only used !--- to flag the packets to capture.
ciscoasa(config)#access-list captureacl permit ip any host 224.1.2.3 !--- Define the
capture named capout, bind it to the outside interface, and !--- specify to only capture
packets that match the access-list captureacl. ciscoasa(config)#capture capout interface
outside access-list captureacl !--- Repeat for the inside interface.
ciscoasa(config)#capture capin interface inside access-list captureacl !--- View the
contents of the capture on the outside. This verifies that the !--- packets are seen on the
outside interface ciscoasa(config)#show capture capout 138 packets captured 1:
02:38:07.639798 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 2: 02:38:07.696024
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 3: 02:38:07.752295 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 4: 02:38:07.808582 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 5:
02:38:07.864823 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 6: 02:38:07.921110
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 7: 02:38:07.977366 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 8: 02:38:08.033689 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 9:
02:38:08.089961 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 10: 02:38:08.146247
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 11: 02:38:08.202504 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 12: 02:38:08.258760 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316
13: 02:38:08.315047 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 14: 02:38:08.371303
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 15: 02:38:08.427574 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 16: 02:38:08.483846 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316
17: 02:38:08.540117 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 18: 02:38:08.596374
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 19: 02:38:08.652691 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 20: 02:38:08.708932 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316
21: 02:38:08.765188 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 22: 02:38:08.821460
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 23: 02:38:08.877746 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 24: 02:38:08.934018 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316
!--- Here you see the packets forwarded out the inside !--- interface towards the clients.
ciscoasa(config)#show capture capin 89 packets captured 1: 02:38:12.873123
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 2: 02:38:12.929380 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 3: 02:38:12.985621 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 4:
02:38:13.041898 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 5: 02:38:13.098169
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 6: 02:38:13.154471 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 7: 02:38:13.210743 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 8:
02:38:13.266999 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 9: 02:38:13.323255
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 10: 02:38:13.379542 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 11: 02:38:13.435768 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316
12: 02:38:13.492070 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 13: 02:38:13.548342
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 14: 02:38:13.604598 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 15: 02:38:13.660900 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316
16: 02:38:13.717141 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 17: 02:38:13.773489
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 18: 02:38:13.829699 192.168.1.2.52292 >
224.1.2.3.1234: udp 1316 19: 02:38:13.885986 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316
20: 02:38:13.942227 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 21: 02:38:13.998483
192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 22: 02:38:14.054852 192.168.1.2.52292 >
```

```
224.1.2.3.1234: udp 1316 23: 02:38:14.111108 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316
24: 02:38:14.167365 192.168.1.2.52292 > 224.1.2.3.1234: udp 1316 ciscoasa(config)# !---
Remove the capture from the memory of the firewall. ciscoasa(config)#no capture capout
```

已知的 Bug

Cisco bug ID CSCse81633（仅限注册用户）— ASA 4GE-SSM Gig 端口以静默方式丢弃 IGMP 加入信息。

- **症状** — 当将 4GE-SSM 模块安装到 ASA 中并且在接口上配置了多播路由和 IGMP 时，4GE-SSM 模块的接口会丢弃 IGMP 加入信息。
- **情况** — ASA 的内置 Gig 接口未丢弃 IGMP 加入信息。
- **解决办法** — 对于多播路由，使用内置 Gig 接口端口。
- **修正此问题的版本** — 7.0(6)、7.1(2)18、7.2(1)11

相关信息

- Cisco ASA 5500 系列自适应安全设备支持
- Cisco PIX 500 系列安全设备支持
- 技术支持和文档 - Cisco Systems