

PIX/ASA 7.x : 送信者が外部にいる場合の PIX/ASA プラットフォームでのマルチキャスト の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングの手順](#)

[既知のバグ](#)

[関連情報](#)

概要

このドキュメントでは、バージョン 7.x が稼働する Cisco 適応型セキュリティ アプライアンス (ASA) や PIX セキュリティ アプライアンスでのマルチキャストの設定例を紹介します。この例では、マルチキャストの送信者はセキュリティ アプライアンスの外部に存在し、内部のホストではマルチキャストトラフィックを受信しようとしています。ホストがレポートグループのメンバーシップに IGMP レポートを送信し、ファイアウォールはダイナミック マルチキャストルーティングプロトコルとして Protocol Independent Multicast (PIM) スパースモードをストリームの送信元が存在するアップストリーム ルータに使用します。

注 : FWSM/ASAはASA SSM用に予約されているため、グループ番号として232.x.x.x/8サブネットをサポートしません。FWSM/ASAでは、このサブネットの使用や通過を許可せず、mrouteは作成されません。しかし、GREトンネルでカプセル化すると、このマルチキャストトラフィックをASA/FWSMで渡すことができます。

前提条件

要件

ソフトウェアバージョン 7.0、7.1、7.2 のいずれかが稼働する Cisco PIX または ASA セキュリテ

使用するコンポーネント

このドキュメントの情報は、バージョン 7.x が稼働する Cisco PIX または Cisco ASA ファイアウォールに基づきます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

PIX/ASA 7.x では、ファイアウォール経由のダイナミック マルチキャスト ルーティング用に、完全な PIM 希薄モードおよび双方向性がサポートされます。PIM 稠密モードはサポートされません。7.x ソフトウェアではレガシー マルチキャスト「stub-mode」がサポートされ、この場合はファイアウォールが、PIX バージョン 6.x でサポートされていたように、インターフェイス間の単なる IGMP プロキシになります。

ファイアウォール経由のマルチキャストトラフィックには、次のことが当てはまります。

- マルチキャストトラフィックを受信するインターフェイスにアクセスリストを適用する場合は、アクセスコントロールリスト (ACL) でトラフィックを明示的に許可する必要があります。インターフェイスにアクセスリストを適用しない場合、マルチキャストトラフィックを許可する明示的な ACL エントリは必要ありません。
- マルチキャストデータパケットは、**reverse-path forward check** コマンドがインターフェイスで設定されているかどうかに関係なく、常にファイアウォールのリバースパス転送検査を受けます。このため、パケットを受信したインターフェイスからマルチキャストパケットの送信元へのルートがない場合、パケットは廃棄されます。
- マルチキャストパケットの送信元に戻るルートがインターフェイスにない場合は、**mroute** コマンドを使用して、パケットを廃棄しないようにファイアウォールに指示してください。

設定

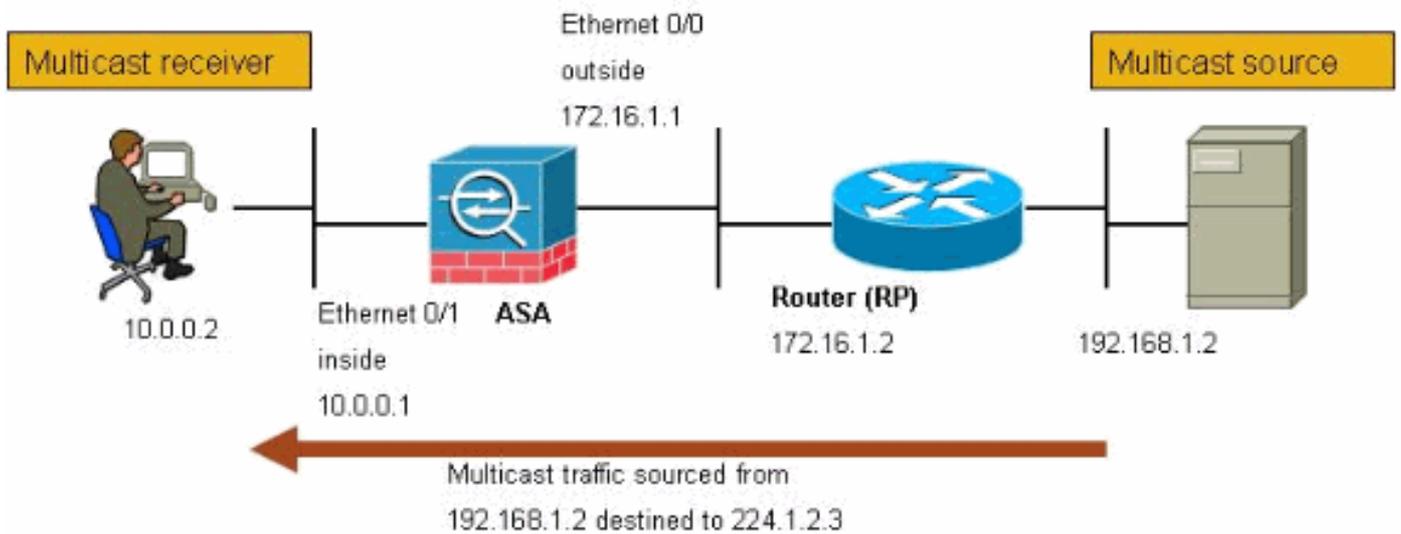
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、**Command Lookup Tool**（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。

マルチキャストトラフィックの送信元は 192.168.1.2 であり、グループ 224.1.2.3 に宛てられたポート 1234 で UDP パケットが使用されています。



コンフィギュレーション

このドキュメントでは、次の設定を使用しています。

バージョン 7.x が稼働する Cisco PIX または ASA ファイアウォール

```
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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show mroute**—IPv4 マルチキャスト ルーティング テーブルが表示されます。

```
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**—指定された接続タイプの接続状態を表示します。

```
!--- 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**—PIM ネイバー テーブルのエントリが表示されます。

!--- 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)
```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングの手順

設定のトラブルシューティングをするには、次の手順を実行します。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の `show` コマンドをサポートします。OIT を使用して、`show` コマンドの出力の分析を表示します。

注 : `debug` コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

1. マルチキャスト受信側は、ファイアウォール内に直接接続している場合、IGMP レポートを送信してマルチキャスト ストリームを受信します。IGMP レポートを内部から受信したことを確認するには、`show igmp traffic` コマンドを使用します。

```
ciscoasa#show igmp traffic
```

```
IGMP Traffic Counters
Elapsed time since counters cleared: 04:11:08

Valid IGMP Packets      Received      Sent
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. `debug igmp` コマンドを使用すると、IGMP データに関する詳細情報をファイアウォールで表示できます。この場合はデバッグが有効であり、ホスト 10.0.0.2 がグループ 224.1.2.3 用に IGMP レポートを送信します。

```
!--- 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. ファイアウォールに有効な PIM ネイバーがあり、ファイアウォールが Join/Prune 情報を受信することを確認します。

```
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. 外部インターフェイスがグループのマルチキャスト パケットを受信することを確認するには、capture コマンドを使用します。

```
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
```

既知のバグ

Cisco Bug ID [CSCse81633](#) ([登録ユーザ専用](#))—ASA 4GE-SSM Gig ポートは IGMP の加入を廃棄して通知しません。

- **症状**—4GE-SSM モジュールを ASA にインストールして、マルチキャスト ルーティングを IGMP とともにインターフェイスで設定すると、IGMP の加入は 4GE-SSM モジュールのインターフェイスで廃棄されます。
- **条件**—IGMP の加入は、ASA のオンボード Gig インターフェイスで廃棄されません。
- **回避策**—マルチキャスト ルーティングの場合は、オンボード ギガビット イーサネット インターフェイス ポートを使用します。
- **修正済みバージョン**—7.0(6)、7.1(2)18、7.2(1)11

関連情報

- [Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンスのサポート](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンスに関するサポート ページ](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)