

firepower脅威対策およびASAマルチキャストPIMのトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[マルチキャストルーティングの基本](#)

[略語/略語](#)

[作業1:PIMスパスモード\(スタティックRP\)](#)

[タスク2:PIMブートストラップルータ\(BSR\)の設定](#)

[トラブルシューティング手法](#)

[PIMトラブルシューティングコマンド\(チートシート\)](#)

[既知の問題](#)

[PIMはvPC Nexusではサポートされない](#)

[宛先ゾーンがサポートされていない](#)

[HSRPが原因でファイアウォールが上流に位置するルータへのPIMメッセージを送信しない](#)

[ファイアウォールがLANセグメントのDRでない場合、LHRと見なされない](#)

[Reverse Path Forwarding\(RPF\)チェックの失敗によりファイアウォールがマルチキャストパケットをドロップする](#)

[ソースツリーへのPIMスイッチオーバー時にファイアウォールがPIM参加を生成しない](#)

[パントレート制限によりファイアウォールが最初の数パケットをドロップする](#)

[ICMPマルチキャストトラフィックのフィルタリング](#)

[既知のPIMマルチキャスト不具合](#)

[関連情報](#)

概要

このドキュメントでは、Firepower脅威対策(FTD)と適応型セキュリティアプライアンス(ASA)がProtocol Independent Multicast(PIM)を実装する方法について説明します。

前提条件

要件

IPルーティングに関する基礎知識

使用するコンポーネント

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、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firepower 4125 Threat Defenseバージョン7.1.0
- Firepower Management Center (FMC) バージョン 7.1.0.
- Cisco 適応型セキュリティアプライアンスソフトウェアバージョン9.17(1)9。

背景説明

マルチキャストルーティングの基本

- ユニキャストはパケットを宛先に転送し、マルチキャストはパケットを送信元から転送しません。
- マルチキャストネットワークデバイス（ファイアウォールやルータなど）は、リバースパス転送(RPF)を介してパケットを転送します。RPFは、特定のタイプの攻撃を防ぐためにユニキャストで使用されるuRPFとは異なることに注意してください。RPFは、マルチキャストパケットを、マルチキャスト受信側に向かうインターフェイスから送信元に転送するメカニズムとして定義できます。その主な役割は、トラフィックループを防止し、正しいトラフィックパスを確保することです。
- PIMのようなマルチキャストプロトコルには、主に3つの機能があります。
 1. アップストリームインターフェイス（送信元に最も近いインターフェイス）を見つけます。
 2. 特定のマルチキャストストリームに関連付けられているダウンストリームインターフェイス（受信側へのインターフェイス）を検出します。
 3. マルチキャストツリーを維持します（ツリー分岐を追加または削除します）。
- マルチキャストツリーは、暗黙的ジョイン（フラッドアンドプルニング）または明示的ジョイン（プルモデル）の2つの方法のいずれかで構築および維持できます。PIMデンスモード(PIM-DM)は暗黙的なjoinを使用し、PIMスパスモード(PIM-SM)は明示的なjoinを使用します。
- マルチキャストツリーは、共有または送信元ベースにすることができます。
 - 共有ツリーはランデブーポイント(RP)の概念を使用し、(*, G)（G = マルチキャストグループIP）で示されます。
 - 送信元ベースのツリーは送信元をルートとし、RPを使用せず、(S, G)として示されます。ここで、Sはマルチキャストの送信元/サーバのIPです。
- マルチキャスト転送モデル：
 - Any-Source Multicast(ASM)配信モードでは、任意の送信元がマルチキャストストリームを送信できる共有ツリー(*, G)を使用します。
 - Source-Specific Multicast(SSM)は、送信元ベースのツリー(S, G)とIP範囲232/8を使

用します。

- 双方向(BiDir)は、コントロールプレーンとデータプレーンの両方のトラフィックが RPを通過する共有ツリー(*、G)のタイプです。
- ランデブーポイントは、次のいずれかの方法で設定または選択できます。
 - スタティック RP
 - Auto-RP
 - ブートストラップルータ(BSR)

PIMモードの概要

PIMモード	RP	共有ツリー	表記法	IGMP	ASA/FTDをサポート
PIM Sparse モード (PIM sparse mode) # PIM Sparse もード #	Yes	Yes	(*、G)および(S、G)	v1/v2/v3	Yes
PIMデンスモード	いいえ	いいえ	(S、G)	v1/v2/v3	いいえ*
PIM双方向モード	Yes	Yes	(*、G)	v1/v2/v3	Yes
PIM Source-Specific-Multicast(SSM)モード	いいえ	いいえ	(S、G)	v3	x **


*Auto-RP =自動RPトラフィックは通過できる

** ASA/FTDをラストホップデバイスにすることはできません

RP設定の概要

ランデブーポイントの設定	ASA/FTD
スタティック RP	Yes
Auto-RP	いいえ。ただし、Auto-RPコントロールプレーントラフィックは通過できます。

BSR	はい。ただし、C-RPはサポートしません。
-----	-----------------------

 注：マルチキャストの問題のトラブルシューティングを開始する前に、マルチキャストトポロジを明確に把握しておくことが非常に重要です。具体的には、少なくとも次のことを把握する必要があります。

- マルチキャストトポロジにおけるファイアウォールの役割は何ですか。
- RPは誰ですか。
- マルチキャストストリームの送信者は誰ですか（送信元IPとマルチキャストグループIP）。
- マルチキャストストリームの受信者はどこですか。
- コントロールプレーン(IGMP/PIM)またはデータプレーン（マルチキャストストリーム）自体に問題がありますか。

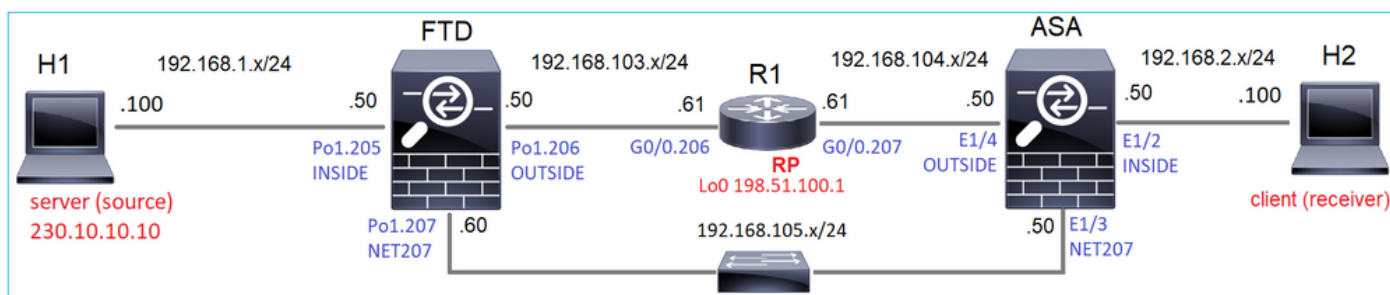
略語/略語

短縮形	説明
FHR	ファーストホップルータ：マルチキャストトラフィックの送信元に直接接続されているホップ。
LHR	ラストホップルータ：マルチキャストトラフィックの受信者に直接接続されているホップ。
RP	ランデブーポイント
DR	指定ルータ
SPT	最短パスツリー
RPT	ランデブーポイント(RP)ツリー、共有ツリー
RPF	リバースパス転送
石油	Outgoing interface list
MRIB	マルチキャストルーティング情報ベース

MFIB	マルチキャスト転送情報ベース
アーキテクチャセー ルスマネ ージャ (ASM)	Any-Sourceマルチキャスト
BSR	ブートストラップルータ
SSM	Source-Specificマルチキャスト
FP	高速パス
SP	遅いパス
CP	コントロールポイント
PPS	パケット/秒レート

作業1:PIMスパースモード (スタティックRP)

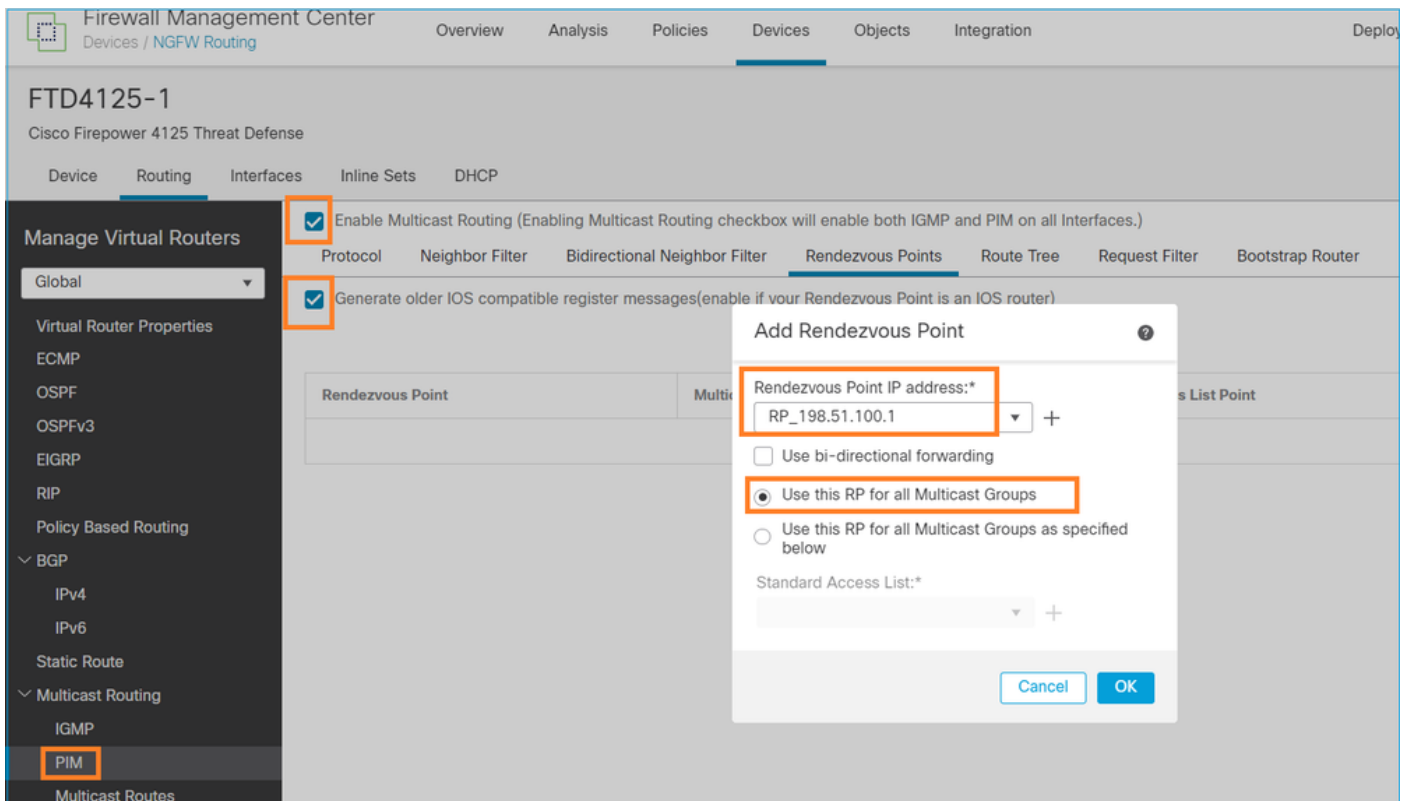
トポロジ



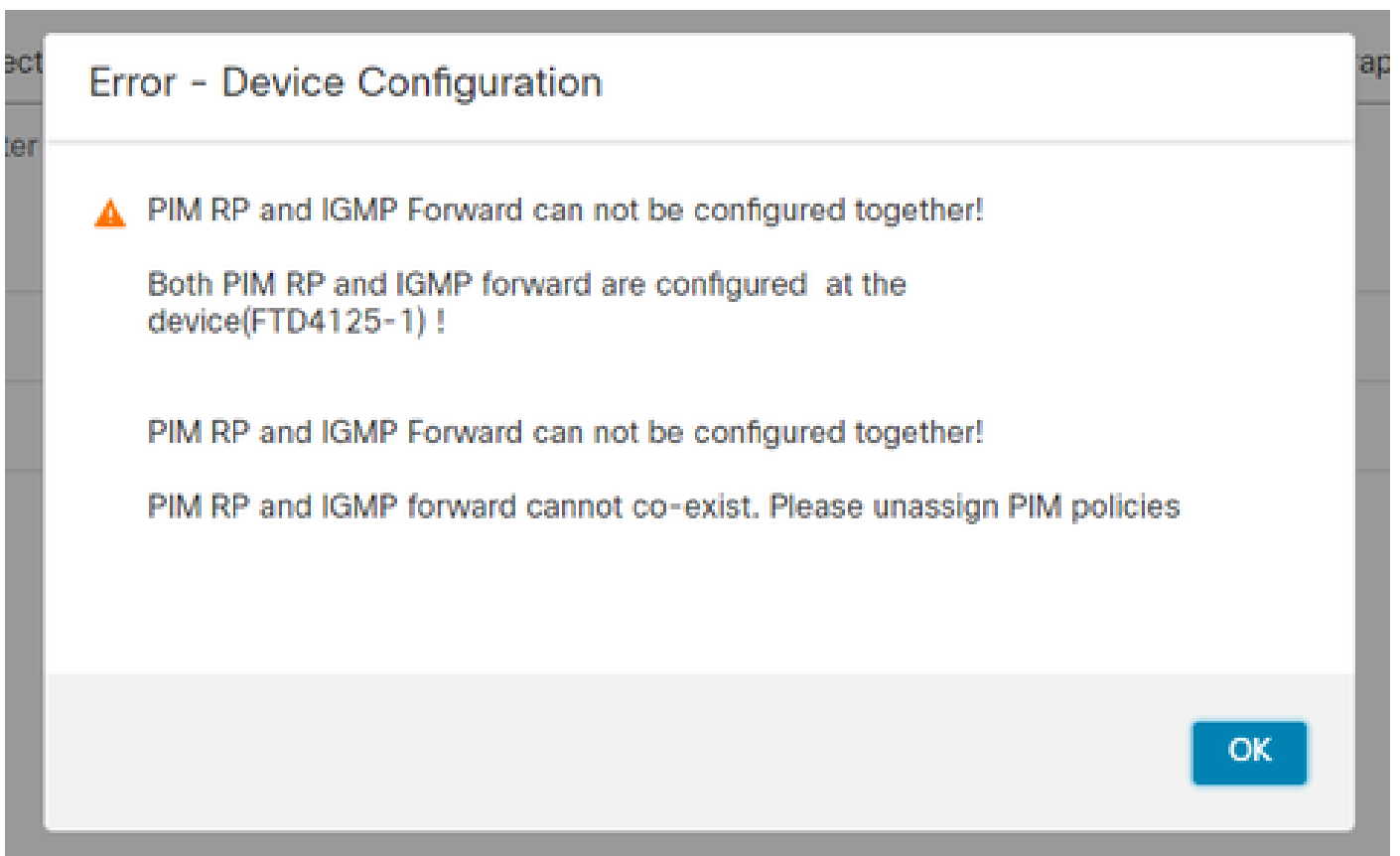
R1(198.51.100.1)をRPとしてトポロジにマルチキャストPIMスパースモードを設定します。

解決方法

FTD設定 :



ASA/FTDは、IGMPスタブルーティングとPIMに対して同時に設定することはできません。



FTDでの結果の設定は次のとおりです。

<#root>

```
firepower#
show running-config multicast-routing

multicast-routing

<-- Multicast routing is enabled globally on the device

firepower#
show running-config pim

pim rp-address 198.51.100.1          <-- Static RP is configured on the firewall

firepower#
ping 198.51.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.1, timeout is 2 seconds:
!!!!!                               <-- The RP is reachable

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ASAファイアウォールでも同様の設定があります。

```
<#root>
asa(config)#
multicast-routing

asa(config)#
pim rp-address 198.51.100.1
```

RP設定 (Ciscoルータ) :

```
<#root>
ip multicast-routing

ip pim rp-address 198.51.100.1          <-- The router is the RP
```

```

!
interface GigabitEthernet0/0.206
 encapsulation dot1Q 206
 ip address 192.168.103.61 255.255.255.0

 ip pim sparse-dense-mode          <-- The interface participates in multicast routing

 ip ospf 1 area 0
!
interface GigabitEthernet0/0.207
 encapsulation dot1Q 207
 ip address 192.168.104.61 255.255.255.0

 ip pim sparse-dense-mode          <-- The interface participates in multicast routing

 ip ospf 1 area 0
!
interface Loopback0

 ip address 198.51.100.1 255.255.255.255

<-- The router is the RP

 ip pim sparse-dense-mode          <-- The interface participates in multicast routing

 ip ospf 1 area 0

```

検証

マルチキャストトラフィック (送信側または受信側) がない場合は、FTDでマルチキャストコントロールプレーンを確認します。

```
<#root>
```

```
firepower#
```

```
show pim interface
```

Address	Interface	PIM	Nbr Count	Hello Intvl	DR Prior	DR	
192.168.105.60	NET207	on	1	30	1	this system	
192.168.1.50	INSIDE	on	0	30	1	this system	<-- PIM enabled on t
0.0.0.0	diagnostic	off	0	30	1	not elected	
192.168.103.50	OUTSIDE	on	1	30	1	192.168.103.61	<-- PIM enabled on t

PIMネイバーを確認します。


```
<#root>
```

```
firepower#
```

```
show pim neighbor
```

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.105.50	NET207	00:05:41	00:01:28	1		B
192.168.103.61	OUTSIDE	00:05:39	00:01:32	1 (DR)		

RPはマルチキャストグループ範囲全体をアドバタイズします。

```
<#root>
```

```
firepower#
```

```
show pim group-map
```

Group Range	Proto	Client	Groups	RP address	Info
224.0.1.39/32*	DM	static	0	0.0.0.0	
224.0.1.40/32*	DM	static	0	0.0.0.0	
224.0.0.0/24*	L-Local	static	1	0.0.0.0	
232.0.0.0/8*	SSM	config	0	0.0.0.0	
224.0.0.0/4*	SM	config	2	198.51.100.1	RPF: OUTSIDE,192.168.103.61 <-- The mult
224.0.0.0/4	SM	static	0	0.0.0.0	RPF: ,0.0.0.0

ファイアウォールのmrouteテーブルには、関連しないエントリがいくつかあります (239.255.255.250は、MAC OSやMicrosoft Windowsなどのベンダーが使用するSimple Service Discovery Protocol(SSDP)です)。

```
<#root>
```

```
firepower#
```

```
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
```

```
(*, 239.255.255.250), 00:17:35/never, RP 198.51.100.1, flags: SCJ
```

```
Incoming interface: OUTSIDE
```

```
RPF nbr: 192.168.103.61
```

```
Immediate Outgoing interface list:
```

```
INSIDE, Forward, 00:17:35/never
```

ファイアウォールとRPの間に構築されたPIMトンネルがあります。

```
<#root>
```

```
firepower#
```

```
show pim tunnel
```

Interface	RP Address	Source Address
Tunnel0	198.51.100.1	192.168.103.50

```
<-- PIM tunnel between the FTD and the RP
```

PIMトンネルは、ファイアウォール接続テーブルでも確認できます。

```
<#root>
```

```
firepower#
```

```
show conn all detail address 198.51.100.1
```

```
...
```

```
PIM OUTSIDE: 198.51.100.1/0 NP Identity Ifc: 192.168.103.50/0,
```

```
<-- PIM tunnel between the FTD and the RP
```

```
, flags , idle 16s, uptime 3m8s, timeout 2m0s, bytes 6350
```

```
Connection lookup keyid: 153426246
```

ASAファイアウォールでの確認：

```
<#root>
```

```
asa#
```

```
show pim neighbor
```

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.105.60	NET207	2d21h	00:01:29	1	(DR)	B
192.168.104.61	OUTSIDE	00:00:18	00:01:37	1	(DR)	

```
<#root>
```

```
asa#
```

```
show pim tunnel
```

Interface	RP Address	Source Address
Tunnel0	198.51.100.1	192.168.104.50

```
<-- PIM tunnel between the ASA and the RP
```

RP (Ciscoルータ) RPの確認。SSDPとAuto-RPには、次のようなマルチキャストグループがあります。


```
<#root>
```

```
Router1#
```

```
show ip pim rp
```

```
Group: 239.255.255.250, RP: 198.51.100.1, next RP-reachable in 00:01:04  
Group: 224.0.1.40, RP: 198.51.100.1, next RP-reachable in 00:00:54
```

受信者がプレゼンスをアナウンスした後の検証

 注：このセクションに示すファイアウォールコマンドは、ASAおよびFTDに完全に適用できません。

ASAはIGMPメンバーシップレポートメッセージを取得し、IGMPとmroute (*, G)エントリを作成します。

```
<#root>
```

```
asa#
```

```
show igmp group 230.10.10.10
```

```
IGMP Connected Group Membership
```

```
Group Address      Interface          Uptime    Expires    Last Reporter
```

```
230.10.10.10      INSIDE            00:01:15  00:03:22  192.168.2.100    <-- Host 192.168.2.100 report
```

ASAファイアウォールは、マルチキャストグループのmrouteを作成します。

```
<#root>
```

```
asa#
```

```
show mroute 230.10.10.10
```

```
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

(* , 230.10.10.10)

, 00:00:17/never,

RP 198.51.100.1

, flags: SCJ

<-- The mroute for group 230.10.10.10

Incoming interface: OUTSIDE

<-- Expected interface for a multicast packet from the source. If the packet is not received on this int

RPF nbr: 192.168.104.61

Immediate Outgoing interface list:
INSIDE, Forward, 00:01:17/never

<-- The OIL points towards the recei

ファイアウォールのもう1つの検証は、PIMトポロジ出力です。

<#root>

asa#


show pim topology 230.10.10.10

...

(* ,230.10.10.10) SM Up: 00:07:15 RP: 198.51.100.1

<-- An entry for multicast group 23

JP: Join(00:00:33) RPF: OUTSIDE,192.168.104.61 Flags: LH
INSIDE 00:03:15 fwd LI LH

 注：ファイアウォールにRPへのルートがない場合、debug pimの出力にはRPFルックアップの失敗が示されます

debug pim出力のRPFルックアップが失敗します。

<#root>

asa#

debug pim

IPv4 PIM: RPF lookup failed for root 198.51.100.1

<-- The RPF look fails because ther

IPv4 PIM: RPF lookup failed for root 198.51.100.1

```
IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.10.10.10) No RPF neighbor to send J/P
```

問題がなければ、ファイアウォールはPIM Join-PruneメッセージをRPに送信します。

```
<#root>
```

```
asa#
```

```
debug pim group 230.10.10.10
```

```
IPv4 PIM group debugging is on
for group 230.10.10.10
```

```
IPv4 PIM: (*,230.10.10.10) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (*,230.10.10.10/32) MRIB modify A NS
IPv4 PIM: [0] (*,230.10.10.10/32) NULLIF-skip MRIB modify !A !NS
IPv4 PIM: [0] (*,230.10.10.10/32) OUTSIDE MRIB modify A NS
IPv4 PIM: (*,230.10.10.10) Processing timers
IPv4 PIM: (*,230.10.10.10) J/P processing
IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs

IPv4 PIM: (*,230.10.10.10) J/P adding Join on OUTSIDE
```

このキャプチャは、PIM Joinメッセージが1分ごとに送信され、PIM Helloが30秒ごとに送信されることを示しています。PIMはIP 224.0.0.13を使用します。

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
7	35.404328	0.000000	192.168.104.50	224.0.0.13	PIMv2	0x1946 (6470)	68	230.10.10.10,230.10.10.10	Join/Prune
19	95.411896	60.007568	192.168.104.50	224.0.0.13	PIMv2	0x4a00 (18944)	68	230.10.10.10,230.10.10.10	Join/Prune
31	155.419479	60.007583	192.168.104.50	224.0.0.13	PIMv2	0x4860 (18528)	68	230.10.10.10,230.10.10.10	Join/Prune

> Frame 7: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.104.50, Dst: 224.0.0.13
v Protocol Independent Multicast
0010 ... = Version: 2
... 0011 = Type: Join/Prune (3)
Reserved byte(s): 00
Checksum: 0x8ebb [correct]
[Checksum Status: Good]
v PIM Options
> Upstream-neighbor: 192.168.104.61 **The upstream neighbor**
Reserved byte(s): 00
Num Groups: 1
Holdtime: 210
v Group 0
> Group 0: 230.10.10.10/32 **A PIM Join for group 230.10.10.10**
v Num Joins: 1
v IP address: 198.51.100.1/32 (SWR) **The RP address**
Address Family: IPv4 (1)
Encoding Type: Native (0)
> Flags: 0x07, Sparse, WildCard, Rendezvous Point Tree
Masklen: 32
Source: 198.51.100.1
Num Prunes: 0

- 🔍 ヒント : Wireshark表示フィルタ : (ip.src==192.168.104.50 && ip.dst==224.0.0.13) &&(pim.group == 230.10.10.10)
- 192.168.104.50は出インターフェイスのファイアウォールIPです (アップストリーム PIMネイバーに向かう)。
 - 224.0.0.13は、PIM Joinおよびプルーニングが送信されるPIMマルチキャストグループです。
 - 230.10.10.10は、PIM Join/Pruneを送信するマルチキャストグループです。

RPは(*, G)のmrouteを作成します。サーバがまだないため、着信インターフェイスはヌルであることを注意してください。

```
<#root>
```

```
Router1#
```

```
show ip mroute 230.10.10.10 | b \(\
```

```
(*, 230.10.10.10), 00:00:27/00:03:02, RP 198.51.100.1, flags: S
```

```
<-- The mroute for the multicas
```

```
Incoming interface: Null
```

```
, RPF nbr 0.0.0.0 <-- No incoming multicast stream
```

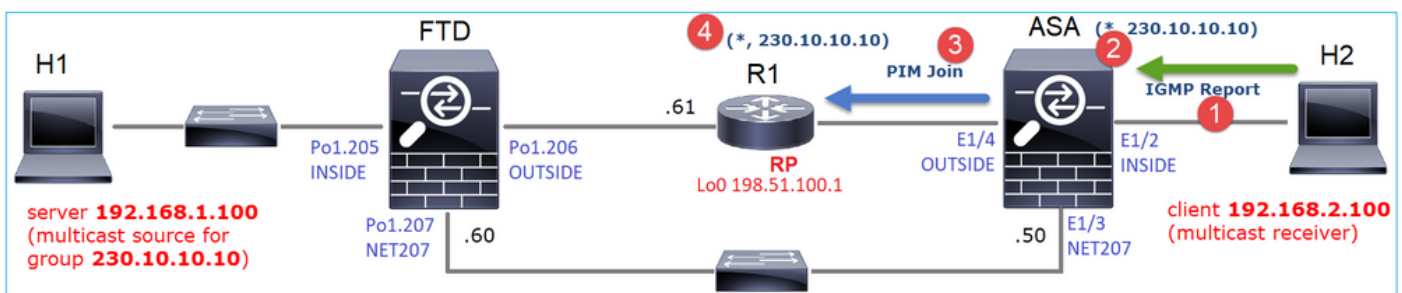
```
Outgoing interface list:
```

```
GigabitEthernet0/0.207
```

```
, Forward/Sparse-Dense, 00:00:27/00:03:02
```

```
<-- There was a PIM Join on this interface
```

それを図で示します。



1. ASAでIGMPレポートが受信されます。
2. (*, G) mrouteが追加されます。
3. ASAがPIM JoinメッセージをRP(198.51.100.1)に送信します。

4. RPはJoinメッセージを受信し、(*, G)mrouteを追加します。

同時に、FTDではIGMPレポートもPIM Joinも受信されなかったため、mrouteは存在しません。

```
<#root>
```

```
firepower#
```

```
show mroute 230.10.10.10
```

```
No mroute entries found.
```

サーバがマルチキャストストリームを送信するときの検証

FTDはH1からマルチキャストストリームを取得し、RPでPIM登録プロセスを開始します。FTDがユニキャストPIM RegisterメッセージをRPに送信します。RPはPIM Joinメッセージをファーストホップルータ(FHR) (この場合はFTD) に送信して、マルチキャストツリーに参加します。次に、Register-Stopメッセージを送信します。

```
<#root>
```

```
firepower#
```

```
debug pim group 230.10.10.10
```

```
IPv4 PIM group debugging is on  
for group 230.10.10.10
```

```
firepower#
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=20,c=20)
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.1.100/INSIDE
```

```
<-- The FTD receives a multicast stream on INSIDE interface for group 230.10.10.10
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Connected status changed from off to on
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !NS
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !DC
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Start registering to 198.51.100.1
```

```
<-- The FTD
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Null to Join
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Prune to Forward
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled in 0.0 secs
```

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify NS
```

```
IPv4 PIM: (192.168.1.100,230.10.10.10) Set SPT bit
```

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !A
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify A !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) Tunnel0 MRIB modify F NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=2,c=20)

IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S

<-- The FT

IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.1.100,230.10.10.10) Processing timers
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P processing
IPv4 PIM: (192.168.1.100,230.10.10.10) Suppress J/P to connected source
IPv4 PIM: (192.168.1.100,230.10.10.10) Suppress J/P to connected source
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 J/P state changed from Null to Join
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 FWD state change from Prune to Forward
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 Raise J/P expiration timer to 210 seconds
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=29,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Send [0/0] Assert on NET207
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: J/P entry: Prune root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Forward to Prune
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !F !NS
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=29,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Send [0/0] Assert on NET207
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE Processing timers

IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop

<-- The RP s

IPv4 PIM: (192.168.1.100,230.10.10.10) Stop registering

IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 FWD state change from Forward to Prune
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) Tunnel0 MRIB modify !F !NS
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Received Register-Stop
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=22,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on INSIDE
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify !SP

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB update (f=2,c=20)

PIM Registerメッセージは、PIMレジスタ情報とともにUDPデータを伝送するPIMメッセージです

。

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
23	15.829623	0.000015	192.168.1.100	230.10.10.10	PIMv2	0x9802 (38914)...	1402		Register
24	15.829623	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9902 (39170)...	1402		Register
25	15.829653	0.000030	192.168.1.100	230.10.10.10	PIMv2	0x9a02 (39426)...	1402		Register
26	15.829653	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9b02 (39682)...	1402		Register
27	15.833224	0.003571	198.51.100.1	192.168.103.50	PIMv2	0x107c (4220)	56	230.10.10.10,230.10.10.10	Register-stop
28	15.833468	0.000244	198.51.100.1	192.168.103.50	PIMv2	0x107d (4221)	56	230.10.10.10,230.10.10.10	Register-stop
29	15.833681	0.000213	198.51.100.1	192.168.103.50	PIMv2	0x107e (4222)	56	230.10.10.10,230.10.10.10	Register-stop
30	15.833910	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x107f (4223)	56	230.10.10.10,230.10.10.10	Register-stop
31	15.834109	0.000199	198.51.100.1	192.168.103.50	PIMv2	0x1080 (4224)	56	230.10.10.10,230.10.10.10	Register-stop
32	15.836092	0.001983	198.51.100.1	192.168.103.50	PIMv2	0x108f (4239)	56	230.10.10.10,230.10.10.10	Register-stop
33	15.836306	0.000214	198.51.100.1	192.168.103.50	PIMv2	0x1090 (4240)	56	230.10.10.10,230.10.10.10	Register-stop
34	15.836535	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x1091 (4241)	56	230.10.10.10,230.10.10.10	Register-stop

> Frame 26: 1402 bytes on wire (11216 bits), 1402 bytes captured (11216 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.168.103.50, Dst: 198.51.100.1
v Protocol Independent Multicast
0010 = Version: 2
... 0001 = Type: Register (1)
Reserved byte(s): 00
> Checksum: 0x966a incorrect, should be 0xdefb
[Checksum Status: Bad]
> PIM Options
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 230.10.10.10
> User Datagram Protocol, Src Port: 64742 (64742), Dst Port: avt-profile-1 (5004)
> Data (1328 bytes)

PIM Register-Stopメッセージ :

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
23	15.829623	0.000015	192.168.1.100	230.10.10.10	PIMv2	0x9802 (38914)...	1402		Register
24	15.829623	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9902 (39170)...	1402		Register
25	15.829653	0.000030	192.168.1.100	230.10.10.10	PIMv2	0x9a02 (39426)...	1402		Register
26	15.829653	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9b02 (39682)...	1402		Register
27	15.833224	0.003571	198.51.100.1	192.168.103.50	PIMv2	0x107c (4220)	56	230.10.10.10,230.10.10.10	Register-stop
28	15.833468	0.000244	198.51.100.1	192.168.103.50	PIMv2	0x107d (4221)	56	230.10.10.10,230.10.10.10	Register-stop
29	15.833681	0.000213	198.51.100.1	192.168.103.50	PIMv2	0x107e (4222)	56	230.10.10.10,230.10.10.10	Register-stop
30	15.833910	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x107f (4223)	56	230.10.10.10,230.10.10.10	Register-stop
31	15.834109	0.000199	198.51.100.1	192.168.103.50	PIMv2	0x1080 (4224)	56	230.10.10.10,230.10.10.10	Register-stop
32	15.836092	0.001983	198.51.100.1	192.168.103.50	PIMv2	0x108f (4239)	56	230.10.10.10,230.10.10.10	Register-stop
33	15.836306	0.000214	198.51.100.1	192.168.103.50	PIMv2	0x1090 (4240)	56	230.10.10.10,230.10.10.10	Register-stop
34	15.836535	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x1091 (4241)	56	230.10.10.10,230.10.10.10	Register-stop

> Frame 27: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_33:44:5d (f4:db:e6:33:44:5d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 198.51.100.1, Dst: 192.168.103.50
v Protocol Independent Multicast
0010 = Version: 2
... 0010 = Type: Register-stop (2)
Reserved byte(s): 00
Checksum: 0x29be [correct]
[Checksum Status: Good]
> PIM Options

🔍 ヒント:WiresharkでPIM登録メッセージとPIM登録停止メッセージのみを表示するには、表示フィルタpim.type in {1 2}を使用します。

ファイアウォール (ラストホップルータ) は、インターフェイスOUTSIDEでマルチキャストストリームを取得し、インターフェイスNET207へのShortest Path Tree(SPT)スイッチオーバーを開始します。

<#root>

asa#

debug pim group 230.10.10.10

IPv4 PIM group debugging is on
for group 230.10.10.10

IPv4 PIM: (*,230.10.10.10) Processing Periodic Join-Prune timer

IPv4 PIM: (*,230.10.10.10) J/P processing

IPv4 PIM: (*,230.10.10.10) Periodic J/P scheduled in 50 secs

IPv4 PIM: (*,230.10.10.10) J/P adding Join on OUTSIDE

<-- A PIM Join message is sent from the interface OUTSIDE

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB update (f=20,c=20)

IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on OUTSIDE

<-- The m

IPv4 PIM: (192.168.1.100,230.10.10.10) Create entry

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify NS

IPv4 PIM: (192.168.1.100,230.10.10.10) RPF changed from 0.0.0.0/- to 192.168.105.60/NET207

<-- The SPT switchover starts from the interface OUTSIDE to the interface NET207

IPv4 PIM: (192.168.1.100,230.10.10.10) Source metric changed from [0/0] to [110/20]

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify DC

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify A NS

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) INSIDE MRIB modify F NS

IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !NS

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !DC

IPv4 PIM: (192.168.1.100,230.10.10.10) Updating J/P status from Null to Join

IPv4 PIM: (192.168.1.100,230.10.10.10) J/P scheduled in 0.0 secs

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify NS

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !SP

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB update (f=2,c=20)

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=28,c=20)

IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207

IPv4 PIM: (192.168.1.100,230.10.10.10)

Set SPT bit

<-- The SPT bit is set

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) MRIB modify !SP

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) OUTSIDE MRIB modify !A

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify A !NS

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Updating J/P status from Null to Prune

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Create entry

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P scheduled in 0.0 secs

IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP

IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=2,c=20)

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Processing timers

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P processing

IPv4 PIM: (192.168.1.100,230.10.10.10)RPT J/P adding Prune on OUTSIDE

<-- A PIM Prune message is sent from the interface OUTSIDE

```
IPv4 PIM: (192.168.1.100,230.10.10.10)RPT Delete entry
IPv4 PIM: (192.168.1.100,230.10.10.10) Processing timers
IPv4 PIM: (192.168.1.100,230.10.10.10) J/P processing
IPv4 PIM: (192.168.1.100,230.10.10.10) Periodic J/P scheduled in 50 secs

IPv4 PIM: (192.168.1.100,230.10.10.10) J/P adding Join on NET207
```

<-- A PIM Join message is sent from the interface NET207

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=22,c=20)
IPv4 PIM: [0] (192.168.1.100,230.10.10.10) Signal presenta on NET207
IPv4 PIM: (192.168.1.100,230.10.10.10) Set alive timer to 210 sec
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify !SP
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=2,c=20)
```

スイッチオーバー発生時のFTDでのPIMデバッグ：

<#root>

```
IPv4 PIM: J/P entry: Join root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 J/P state changed from Null to Join
```

<-- A PIM Join message is sent from the interface NET207

```
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 FWD state change from Prune to Forward
```

<-- The packets are sent from the interface NET207

```
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB modify F NS
IPv4 PIM: (192.168.1.100,230.10.10.10) NET207 Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.1.100,230.10.10.10) Tunnel0 Processing timers
...
IPv4 PIM: [0] (192.168.1.100,230.10.10.10/32) NET207 MRIB update (f=9,c=20)
IPv4 PIM: J/P entry: Prune root: 192.168.1.100 group: 230.10.10.10 flags: S
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE J/P state changed from Join to Null
IPv4 PIM: (192.168.1.100,230.10.10.10) OUTSIDE FWD state change from Forward to Prune
```

<-- A PIM Prune message is sent from the interface OUTSIDE

SPTスイッチオーバー開始後のFTD mroute:

```
<#root>
```

```
firepower#
```

```
show mroute 230.10.10.10
```

```
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
```

```
(192.168.1.100, 230.10.10.10), 00:00:06/00:03:23, flags: SF
```

```
T          <-- SPT-bit is set when the switchover occurs
```

```
  Incoming interface: INSIDE
```

```
  RPF nbr: 192.168.1.100, Registering
```

```
  Immediate Outgoing interface list:
```

```
NET207, Forward, 00:00:06/00:03:23
```

```
<-- Both interfaces are shown in
```

```
OUTSIDE, Forward, 00:00:06/00:03:23
```

```
<-- Both interfaces are shown in
```

```
  Tunnel0, Forward, 00:00:06/never
```

SPTスイッチオーバーの終了時には、NET207インターフェイスだけがFTDのOILに示されます。

```
<#root>
```

```
firepower#
```

```
show mroute 230.10.10.10
```

```
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
```

```
(192.168.1.100, 230.10.10.10), 00:00:28/00:03:01, flags: SFT
```

```
  Incoming interface: INSIDE
```

```
  RPF nbr: 192.168.1.100
```

Immediate Outgoing interface list:

NET207, Forward

, 00:00:28/00:03:01

<-- The interface NET207 forwards the multicast stream after the SPT switchover

ラストホップルータ(ASA)では、SPTビットも設定されます。

<#root>

asa#

show mroute 230.10.10.10

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

(* , 230.10.10.10), 01:43:09/never, RP 198.51.100.1, flags: SCJ

Incoming interface: OUTSIDE

RPF nbr: 192.168.104.61

Immediate Outgoing interface list:

INSIDE, Forward, 01:43:09/never

(192.168.1.100, 230.10.10.10)

, 00:00:03/00:03:27, flags: SJ

T <-- SPT switchover for group 230.10.10.10

Incoming interface:

NET207

<-- The multicast packets arrive on interface NET207

RPF nbr: 192.168.105.60

Inherited Outgoing interface list:

INSIDE, Forward, 01:43:09/never

ASA NET207インターフェイス (スイッチオーバーを実行したファーストホップルータ) からのスイッチオーバー。PIM Joinメッセージがアップストリームデバイス(FTD)に送信されます。

```

(pim.src == 230.10.10.10) && (pim.type == 3) && (ip.src == 192.168.105.50)

```

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
202	61.891684	0.000000	192.168.105.50	224.0.0.13	PIMv2	0x1c71 (7281)	68	230.10.10.10,230.10.10.10	Join/Prune
1073	120.893225	59.001541	192.168.105.50	224.0.0.13	PIMv2	0x68ac (26796)	68	230.10.10.10,230.10.10.10	Join/Prune
1174	180.894766	60.001541	192.168.105.50	224.0.0.13	PIMv2	0x0df8 (3576)	68	230.10.10.10,230.10.10.10	Join/Prune
1276	240.896307	60.001541	192.168.105.50	224.0.0.13	PIMv2	0x6858 (26712)	68	230.10.10.10,230.10.10.10	Join/Prune

```

> Frame 202: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:ae (00:be:75:f6:1d:ae), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.105.50, Dst: 224.0.0.13
v Protocol Independent Multicast
  0010 .... = Version: 2
  ... 0011 = Type: Join/Prune (3)
  Reserved byte(s): 00
  Checksum: 0xf8e4 [correct]
  [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.105.60
    Reserved byte(s): 00
    Num Groups: 1
    Holdtime: 210
  v Group 0
    > Group 0: 230.10.10.10/32
    v Num Joins: 1
      > IP address: 192.168.1.100/32 (S)
    Num Prunes: 0

```

OUTSIDEインターフェイスでは、マルチキャストストリームを停止するために、PIM PruneメッセージがRPに送信されます。

```

(ip.src == 192.168.104.50 && pim.type == 3) && (pim.group == 230.10.10.10) && (pim.numjoins == 0)

```

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
202	61.891668	0.000000	192.168.104.50	224.0.0.13	PIMv2	0x3a56 (14934)	68	230.10.10.10,230.10.10.10	Join/Prune
2818	1137.915409	1076.023741	192.168.104.50	224.0.0.13	PIMv2	0x1acf (6863)	68	230.10.10.10,230.10.10.10	Join/Prune
5124	1257.917103	120.001694	192.168.104.50	224.0.0.13	PIMv2	0x0b52 (2898)	68	230.10.10.10,230.10.10.10	Join/Prune

```

> Frame 202: 68 bytes on wire (544 bits), 68 bytes captured (544 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> Internet Protocol Version 4, Src: 192.168.104.50, Dst: 224.0.0.13
v Protocol Independent Multicast
  0010 .... = Version: 2
  ... 0011 = Type: Join/Prune (3)
  Reserved byte(s): 00
  Checksum: 0xf8e3 [correct]
  [Checksum Status: Good]
  v PIM Options
    > Upstream-neighbor: 192.168.104.61
    Reserved byte(s): 00
    Num Groups: 1
    Holdtime: 210
  v Group 0
    > Group 0: 230.10.10.10/32
    Num Joins: 0
    v Num Prunes: 1
      > IP address: 192.168.1.100/32 (SR)

```

PIMトラフィックの検証：

```
<#root>
```

```
firepower#
```

```
show pim traffic
```

```
PIM Traffic Counters
```

```
Elapsed time since counters cleared: 1w2d
```

	Received	Sent	
Valid PIM Packets	53934	63983	
Hello	36905	77023	
Join-Prune	6495	494	<-- PIM Join/Prune messages
Register	0	2052	<-- PIM Register messages
Register Stop	1501	0	<-- PIM Register Stop messages
Assert	289	362	
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	

低速パスと高速パスとコントロールポイントで処理されたパケットの数を確認するには、次の手順を実行します。

<#root>

firepower#

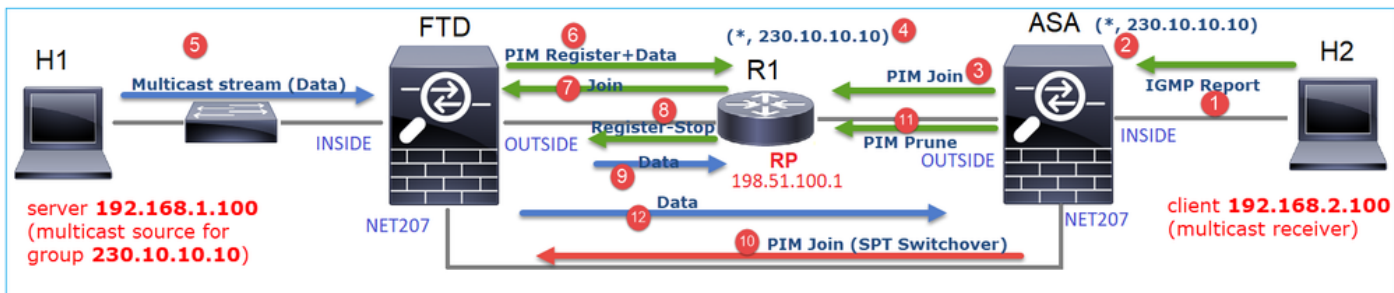
show asp cluster counter

Global dp-counters:

Context specific dp-counters:

MCAST_FP_FROM_PUNT	2712	Number of multicast packets punted from CP to FP
MCAST_FP_FORWARDED	94901	Number of multicast packets forwarded in FP
MCAST_FP_TO_SP	1105138	Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL	1107850	Number of total multicast packets processed in SP
MCAST_SP_FROM_PUNT	2712	Number of multicast packets punted from CP to SP
MCAST_SP_FROM_PUNT_FORWARD	2712	Number of multicast packets coming from CP that are forwarded
MCAST_SP_PKTS	537562	Number of multicast packets that require slow-path attention
MCAST_SP_PKTS_TO_FP_FWD	109	Number of multicast packets that skip over punt rule and are forwarded
MCAST_SP_PKTS_TO_CP	166981	Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE	567576	Number of multicast packets failed with no flow mcast_handle
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC	223847	Number of multicast packets failed with no accept interface
MCAST_FP_CHK_FAIL_NO_SEQ_NO_MATCH	131	Number of multicast packets failed with no matched sequence
MCAST_FP_CHK_FAIL_NO_FP_FWD	313584	Number of multicast packets that cannot be fast-path forwarded
MCAST_FP_UPD_FOR_UNMATCH_IFC	91	Number of times that multicast flow's ifc_out cannot be updated

動作をステップごとに示す図：



1. エンドホスト(H2)は、マルチキャストストリーム230.10.10.10に参加するためにIGMPレポートを送信します。
2. PIM DRであるラストホップルータ(ASA)は(*, 230.10.10.10)エントリを作成します。
3. ASAがグループ230.10.10.10のRPにPIM Joinメッセージを送信します。
4. RPによって(*, 230.10.10.10)エントリが作成されます。
5. サーバはマルチキャストストリームデータを送信します。
6. FTDはPIM登録メッセージにマルチキャストパケットをカプセル化し、それらを(ユニキャスト)RPに送信します。この時点で、RPはアクティブなレシーバがあることを認識し、マルチキャストパケットをカプセル化解除して、レシーバに送信します。
7. RPは、マルチキャストツリーに参加するためにFTDにPIM Joinメッセージを送信します。
8. RPからFTDにPIM Register-Stopメッセージが送信されます。
9. FTDはRPに対してネイティブマルチキャストストリーム(PIMカプセル化なし)を送信します。
10. ラストホップルータ(ASA)は、送信元(192.168.1.100)にNET207インターフェイスからの適切なパスがあることを認識し、スイッチオーバーを開始します。PIM Joinメッセージをアップストリームデバイス(FTD)に送信します。
11. ラストホップルータはRPにPIM Pruneメッセージを送信します。
12. FTDはマルチキャストストリームをNET207インターフェイスに転送します。ASAが共有ツリー(RPツリー)から送信元ツリー(SPT)に移動します。

タスク2:PIMブートストラップルータ(BSR)の設定

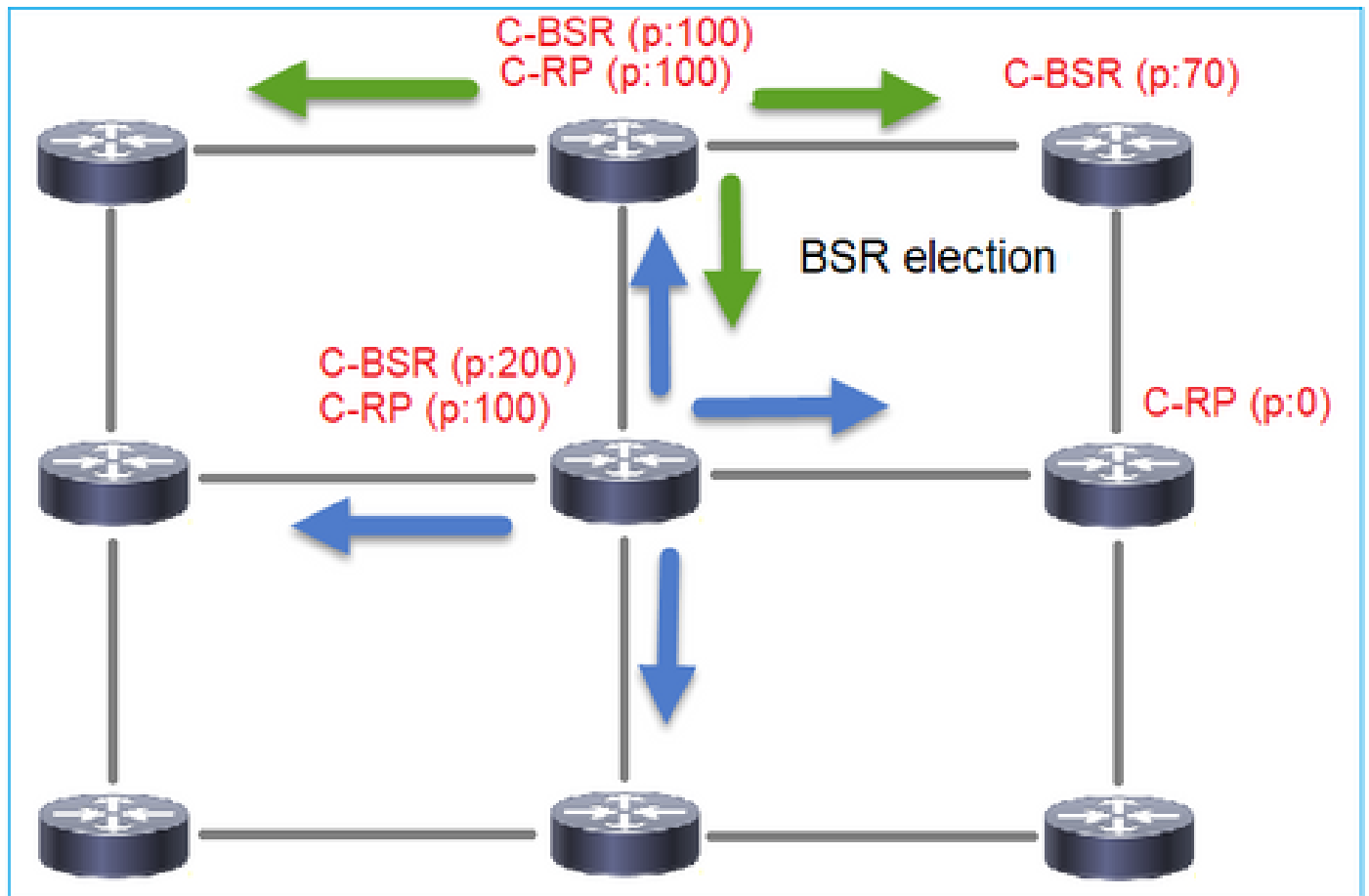
BSRの基本

- BSR(RFC 5059)は、PIMプロトコルを使用するコントロールプレーンマルチキャストメカニズムで、デバイスはRP情報を動的に学習できます。
- BSR定義：
 - 候補RP(C-RP):RPにしたいデバイス。
 - 候補BSR(C-BSR):BSRになり、他のデバイスにRPセットをアドバタイズするデバイス。
 - BSR：多数のC-BSRの中からBSRに選出されるデバイス。最も高いBSRプライオリティが選出されます。
 - RP-set：すべてのC-RPとその優先順位のリスト。
 - RP:RPプライオリティが最も低いデバイスが選出されます。
 - BSR PIMメッセージ(空):BSRの選択に使用されるPIMメッセージ。
 - BSR PIMメッセージ(通常):224.0.0.13 IPに送信されるPIMメッセージで、RPセットとBSR情報が含まれています。

BSRの仕組み

1. BSR選択メカニズム。

各C-BSRは、プライオリティを含むPIM BSR空のメッセージを送信します。最も高いプライオリティ（フォールバックが最も高いIP）を持つデバイスが選出され、BSRになります。残りのデバイスは、空のBSRメッセージを送信しません。



選出プロセスで使用されるBSRメッセージには、C-BSRの優先順位情報だけが含まれます。

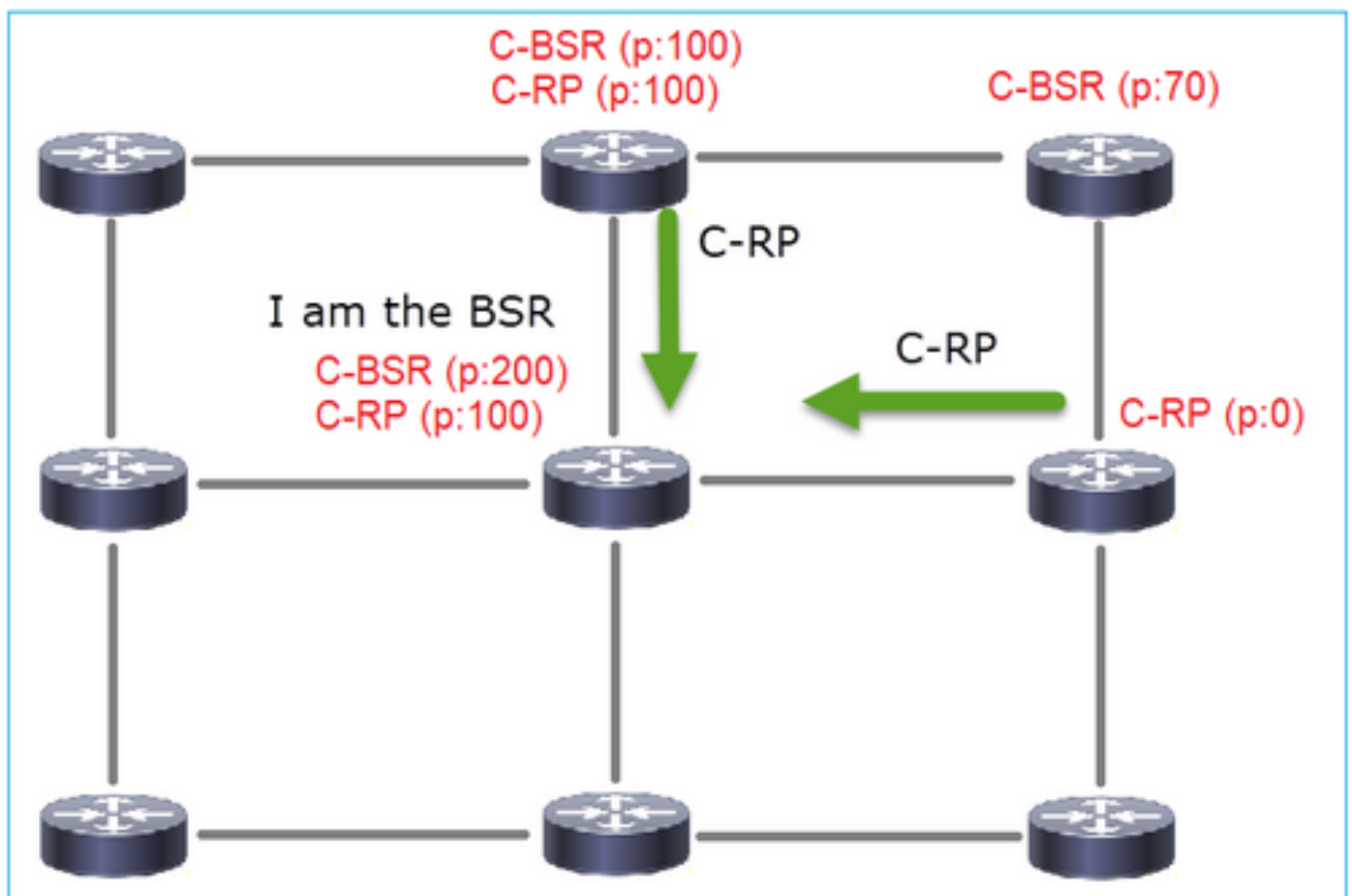
No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
2	6.437401	0.000000	192.168.103.50	224.0.0.13	PIMv2	0x2740 (10048)	52		Bootstrap
8	66.643725	60.206324	192.168.103.50	224.0.0.13	PIMv2	0x1559 (5465)	52		Bootstrap
13	126.850014	60.206289	192.168.103.50	224.0.0.13	PIMv2	0x0d32 (3378)	52		Bootstrap


```

> Frame 2: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.168.103.50, Dst: 224.0.0.13
v Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0100 = Type: Bootstrap (4)
  Reserved byte(s): 00
  Checksum: 0x4aa9 [correct]
  [Checksum Status: Good]
v PIM Options
  Fragment tag: 0x687b
  Hash mask len: 0
  BSR priority: 0
  > BSR: 192.168.103.50

```

WiresharkでBSRメッセージを表示するには、次の表示フィルタを使用します。pim.type == 4
 2. C-RPは、C-RPプライオリティを含むBSRにユニキャスト BSRメッセージを送信します。



候補RPメッセージ :

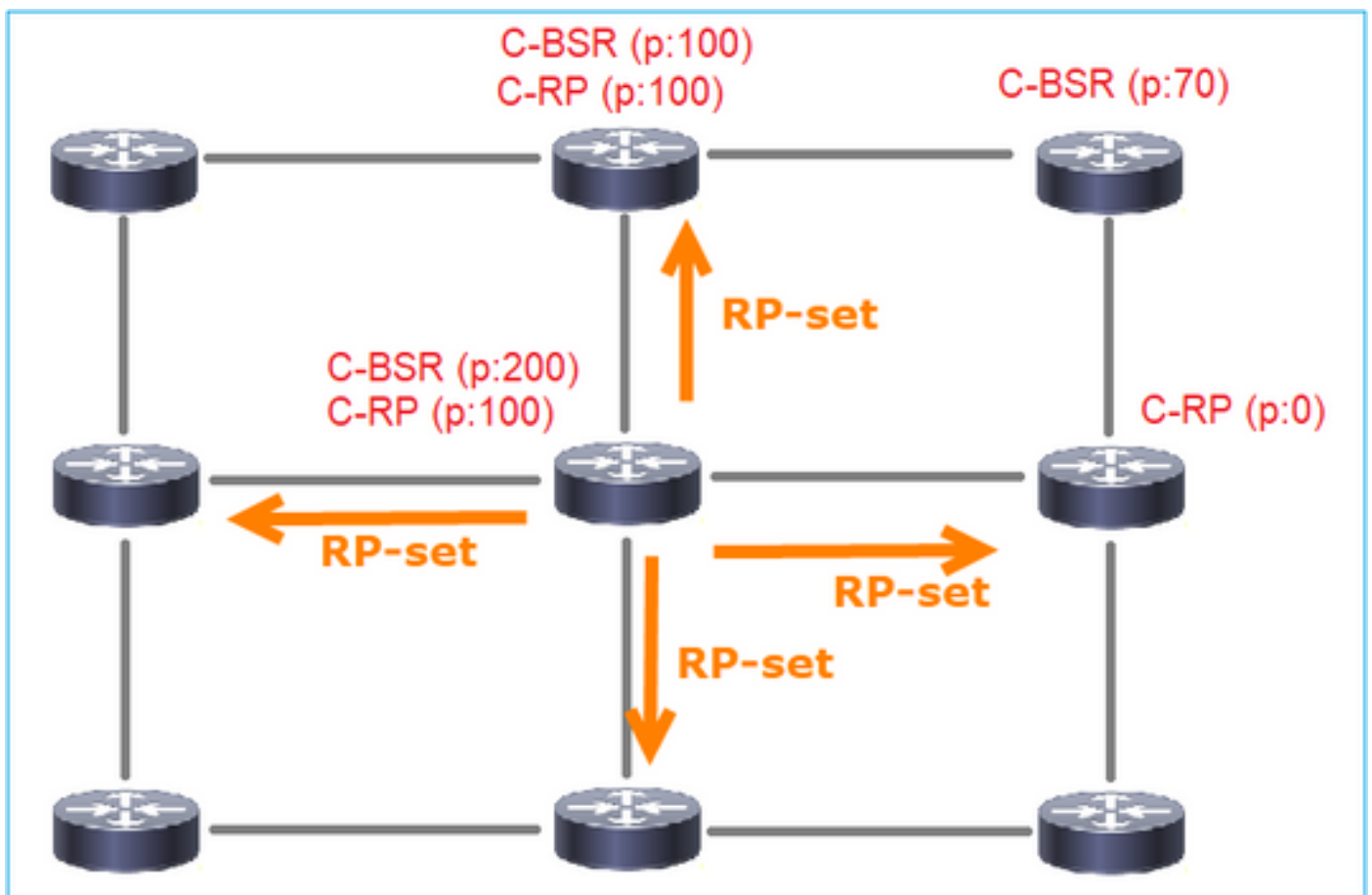
No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
35	383.703125	0.000000	192.0.2.1	192.168.103.50	PIMv2	0x4ca8 (19624)	60	224.0...	Candidate-RP-Advertisement

```

> Frame 35: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_33:44:5d (f4:db:e6:33:44:5d)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 206
> Internet Protocol Version 4, Src: 192.0.2.1, Dst: 192.168.103.50
< Protocol Independent Multicast
  0010 .... = Version: 2
  .... 1000 = Type: Candidate-RP-Advertisement (8)
  Reserved byte(s): 00
  Checksum: 0x3263 [correct]
  [Checksum Status: Good]
  < PIM Options
    Prefix-count: 1
    Priority: 0
    Holdtime: 150
    < RP: 192.0.2.1
      Address Family: IPv4 (1)
      Encoding Type: Native (0)
      Unicast: 192.0.2.1
      < Group 0: 224.0.0.0/4
        Address Family: IPv4 (1)
        Encoding Type: Native (0)
        > Flags: 0x00
        Masklen: 4
        Group: 224.0.0.0
  
```

WiresharkでBSRメッセージを表示するには、次の表示フィルタを使用します。pim.type == 8

3. BSRはRPセットを構成し、すべてのPIMネイバーにアドバタイズします。



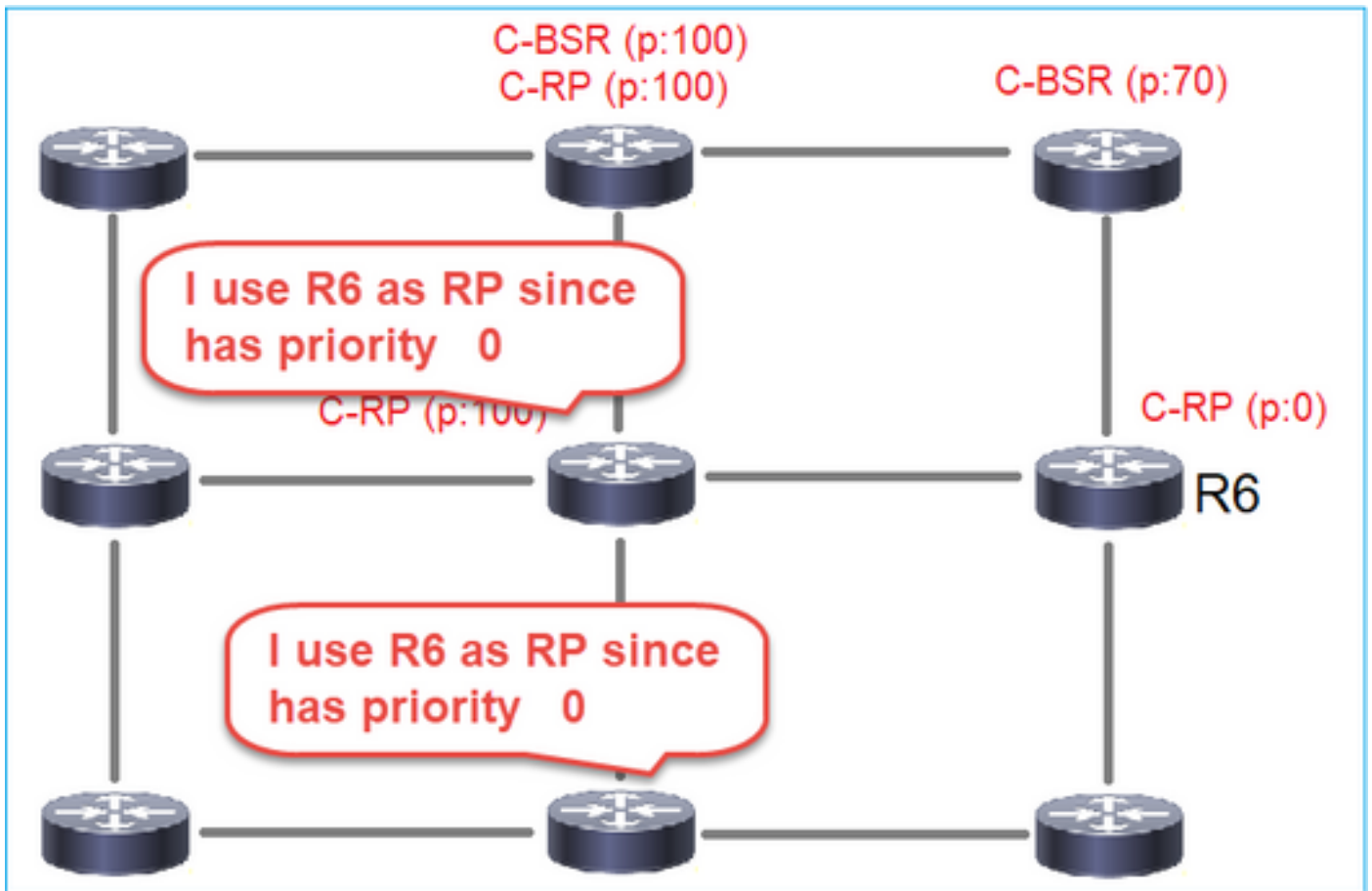
No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
152	747.108256	1.001297	192.168.105.60	224.0.0.13	PIMv2	0x0bec (3052)	84	224.0.0.0,224.0.0.0	Bootstrap

```

> Frame 152: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
> Ethernet II, Src: Cisco_33:44:5d (f4:db:e6:33:44:5d), Dst: IPv4mcast_0d (01:00:5e:00:00:0d)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 207
> Internet Protocol Version 4, Src: 192.168.105.60, Dst: 224.0.0.13
< Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0100 = Type: Bootstrap (4)
  Reserved byte(s): 00
  Checksum: 0x264f [correct]
  [Checksum Status: Good]
  < PIM Options
    Fragment tag: 0x2412
    Hash mask len: 0
    BSR priority: 100
  > BSR: 192.0.2.2
  < Group 0: 224.0.0.0/4
    Address Family: IPv4 (1)
    Encoding Type: Native (0)
  > Flags: 0x00
    Masklen: 4
    Group: 224.0.0.0
    RP count: 2
    FRP count: 2
    Priority: 0
    Priority: 100
  > RP 0: 192.0.2.1
    Holdtime: 150
  > RP 1: 192.0.2.2
    Holdtime: 150
  Reserved byte(s): 00
  Reserved byte(s): 00

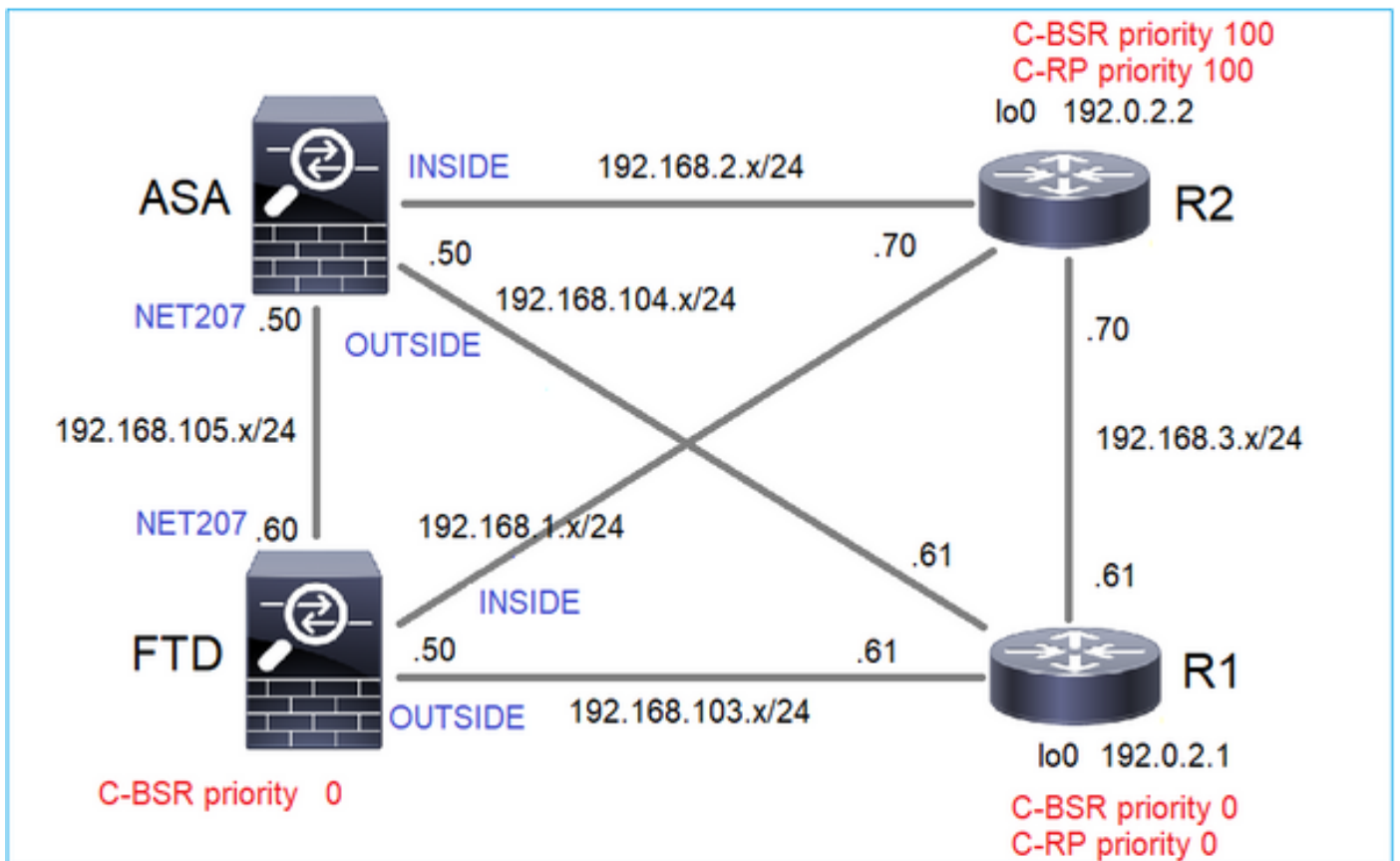
```

4. ルータ/ファイアウォールはRPセットを取得し、最も低いプライオリティに基づいてRPを選択します。



タスクの要件

次のトポロジに従ってC-BSRとC-RPを設定します。



このタスクでは、FTDはBSRプライオリティ0のOUTSIDEインターフェイスでC-BSRとして自分自身をアナウンスする必要があります。

解決方法

FTDのFMC設定：

Firewall Management Center
Devices / NGFW Routing

Overview Analysis Policies **Devices** Objects Integration

FTD4125-1
Cisco Firepower 4125 Threat Defense

Device **Routing** Interfaces Inline Sets DHCP

Manage Virtual Routers
Global

Virtual Router Properties
ECMP
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM

Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all Interfaces.)

Protocol Neighbor Filter Bidirectional Neighbor Filter Rendezvous Points Route Tree Request Filter **Bootstrap Router**

Configure this FTD as a Candidate Bootstrap Router (C-BSR)

Interface:*
OUTSIDE

Hashmask Length:
0 (0-32)

Priority:
0 (0-255)

Configure this FTD as Border Bootstrap Router (BSR) (optional)

Interface	Enable BSR
No records to display	

導入された設定は次のとおりです。

```
multicast-routing
!  
pim bsr-candidate OUTSIDE 0 0
```

他のデバイスの設定：

R1

```
ip multicast-routing  
ip pim bsr-candidate Loopback0 0  
ip pim rp-candidate Loopback0  
!  
interface Loopback0  
ip address 192.0.2.1 255.255.255.255  
ip pim sparse-mode  
!  
! PIM is also enabled on the transit interfaces (e.g. G0/0.203, G0/0.207, G0/0.205)
```

R2では同じですが、C-BSRとC-RPのプライオリティが異なります

```
ip pim bsr-candidate Loopback0 0 100
ip pim rp-candidate Loopback0 priority 100
```

ASAでは、マルチキャストがグローバルに有効になっているだけです。これにより、すべてのインターフェイスでPIMが有効になります。

```
multicast-routing
```

検証

R2は最も高いプライオリティを持つため、選出されたBSRです。

```
<#root>
```

```
firepower#
```

```
show pim bsr-router
```

```
PIMv2 BSR information
```

```
BSR Election Information
```

```
BSR Address: 192.0.2.2          <-- This is the IP of the BSR (R1 lo0)
```

```
    Uptime: 00:03:35, BSR Priority: 100
```

```
,
```

```
Hash mask length: 0
```

```
    RPF: 192.168.1.70,INSIDE
```

```
<-- The interface to the BSR
```

```
    BS Timer: 00:01:34
```

```
    This system is candidate BSR
```

```
    Candidate BSR address: 192.168.103.50, priority: 0, hash mask length: 0
```

R1はプライオリティが最も低いため、RPとして選択されます。

```
<#root>
```

```
firepower#
```

```
show pim group-map
```

Group Range	Proto	Client	Groups	RP address	Info
224.0.1.39/32*	DM	static	0	0.0.0.0	
224.0.1.40/32*	DM	static	0	0.0.0.0	
224.0.0.0/24*	L-Local	static	1	0.0.0.0	
232.0.0.0/8*	SSM	config	0	0.0.0.0	
224.0.0.0/4					

*
SM

BSR

0

192.0.2.1

RPF: OUTSIDE,192.168.103.61

<-- The elected BSR

224.0.0.0/4	SM	BSR	0	192.0.2.2	RPF: INSIDE,192.168.1.70
224.0.0.0/4	SM	static	0	0.0.0.0	RPF: ,0.0.0.0

BSRメッセージはRPFチェックの対象となります。これを確認するには、debug pim bsrを有効にします。

<#root>

IPv4 BSR: Received BSR message from 192.168.105.50 for 192.0.2.2, BSR priority 100 hash mask length 0
IPv4 BSR:

BSR message

from 192.168.105.50/

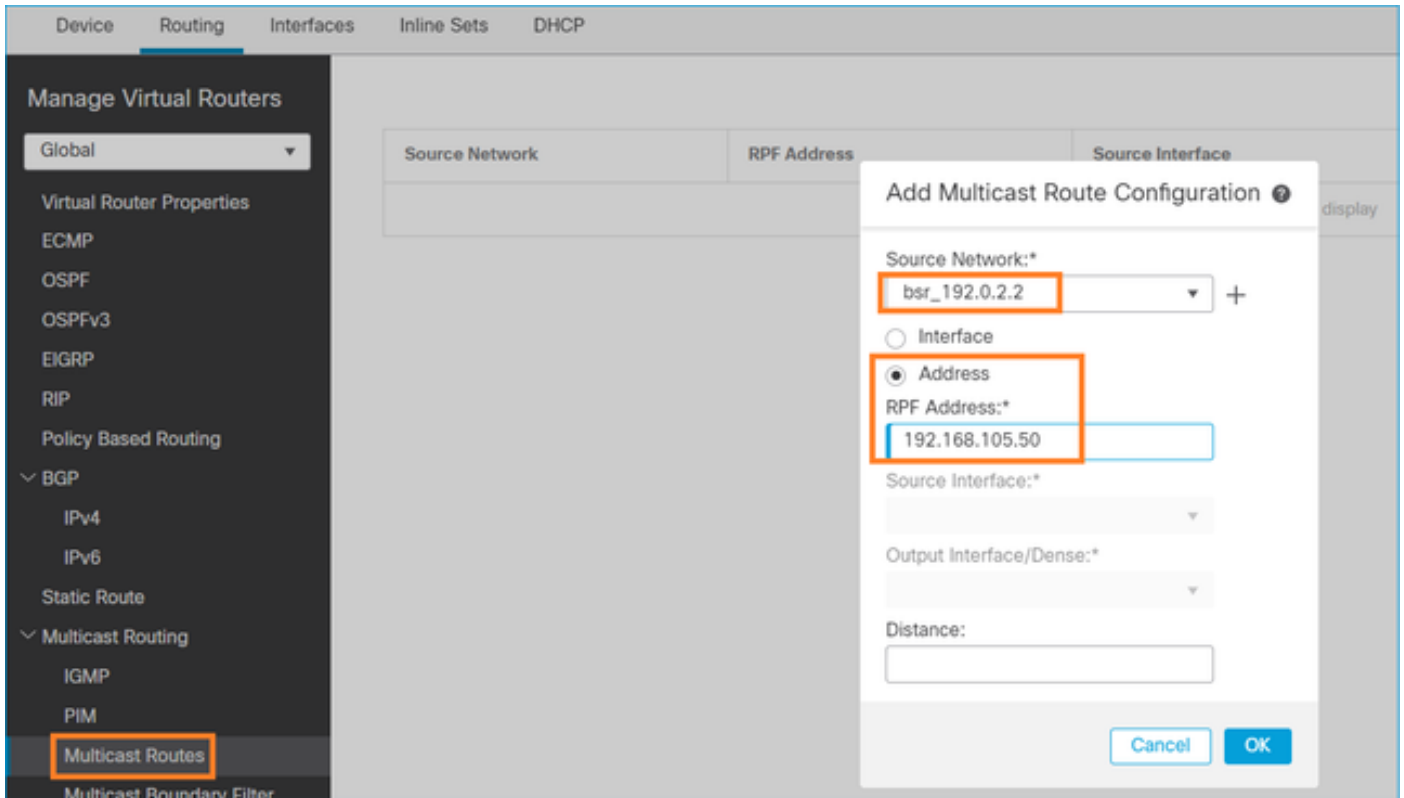
NET207

for 192.0.2.2

RPF failed, dropped

<-- The RPF check for the received BSR message failed

RPFインターフェイスを変更する場合は、スタティックなmrouteを設定できます。この例では、ファイアウォールはIP 192.168.105.50からのBSRメッセージを受け入れます。



```
<#root>
```

```
firepower#
```

```
show run mroute
```

```
mroute 192.0.2.2 255.255.255.255 192.168.105.50
```

```
<#root>
```

```
firepower#
```

```
show pim bsr-router
```

```
PIMv2 BSR information
```

```
BSR Election Information
```

```
BSR Address: 192.0.2.2
```

```
Uptime: 01:21:38, BSR Priority: 100, Hash mask length: 0
```

```
RPF: 192.168.105.50,NET207
```

```
<-- The RPF check points to the static mroute
```

```
BS Timer: 00:01:37
```

```
This system is candidate BSR
```

```
Candidate BSR address: 192.168.103.50, priority: 0, hash mask length: 0
```

ここで、NET207インターフェイスのBSRメッセージは受け入れられますが、INSIDEではドロツ

プされます。

```
<#root>
```

```
IPv4 BSR: Received BSR message from 192.168.1.70 for 192.0.2.2, BSR priority 100 hash mask length 0

IPv4 BSR: BSR message from 192.168.1.70/INSIDE for 192.0.2.2 RPF failed, dropped

...

IPv4 BSR: Received BSR message from 192.168.105.50 for 192.0.2.2, BSR priority 100 hash mask length 0

<-- RPF check is OK
```

ファイアウォールでトレースによるキャプチャを有効にし、BSRメッセージの処理方法を確認します。

```
<#root>
```

```
firepower#
show capture

capture CAPI type raw-data trace interface INSIDE [Capturing - 276 bytes]
  match pim any any
capture CAPO type raw-data trace interface OUTSIDE [Capturing - 176 bytes]
  match pim any any
```

PIM接続はファイアウォールで終端されるため、トレースで有用な情報を表示するには、ボックスへの接続をクリアする必要があります。

```
<#root>
```

```
firepower#
show conn all | i PIM

firepower# show conn all | include PIM
PIM OUTSIDE 192.168.103.61 NP Identity Ifc 224.0.0.13, idle 0:00:23, bytes 116802, flags
PIM NET207 192.168.104.50 NP Identity Ifc 224.0.0.13, idle 0:00:17, bytes 307296, flags
PIM NET207 192.168.104.61 NP Identity Ifc 224.0.0.13, idle 0:00:01, bytes 184544, flags
PIM NET207 192.168.105.50 NP Identity Ifc 224.0.0.13, idle 0:00:18, bytes 120248, flags
PIM INSIDE 192.168.1.70 NP Identity Ifc 224.0.0.13, idle 0:00:27, bytes 15334, flags
PIM OUTSIDE 224.0.0.13 NP Identity Ifc 192.168.103.50, idle 0:00:21, bytes 460834, flags
PIM INSIDE 224.0.0.13 NP Identity Ifc 192.168.1.50, idle 0:00:00, bytes 441106, flags
PIM NET207 224.0.0.13 NP Identity Ifc 192.168.105.60, idle 0:00:09, bytes 458462, flags

firepower#
clear conn all addr 224.0.0.13
```

8 connection(s) deleted.

firepower#

clear cap /all

<#root>

firepower#

show capture CAPI packet-number 2 trace

6 packets captured

2: 11:31:44.390421 802.1Q vlan#205 P6

192.168.1.70 > 224.0.0.13

ip-proto-103, length 38

<-- Ingress PIM packet

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Elapsed time: 4880 ns

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 4880 ns

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: No ECMP load balancing

Result: ALLOW

Elapsed time: 9760 ns

Config:

Additional Information:

Destination is locally connected. No ECMP load balancing.

Found next-hop 192.168.1.70 using egress ifc INSIDE(vrfid:0)

Phase: 4

Type: CLUSTER-DROP-ON-SLAVE

Subtype: cluster-drop-on-slave

Result: ALLOW

Elapsed time: 4392 ns

Config:

Additional Information:

Phase: 5

Type: ACCESS-LIST

Subtype:
Result: ALLOW
Elapsed time: 4392 ns
Config:
Implicit Rule
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 4392 ns
Config:
Additional Information:

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Elapsed time: 18056 ns
Config:
Additional Information:

Phase: 9
Type: MULTICAST <-- The multicast process

Subtype: pim

Result: ALLOW
Elapsed time: 976 ns
Config:
Additional Information:

Phase: 10
Type: MULTICAST
Subtype:
Result: ALLOW
Elapsed time: 488 ns
Config:
Additional Information:

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 20008 ns
Config:
Additional Information:
New flow created with id 25630, packet dispatched to next module

Result:

```
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up
output-line-status: up
```

Action: allow

Time Taken: 76616 ns

RPF障害が原因でPIMパケットがドロップされた場合、トレースには次のように表示されます。

```
<#root>
```

```
firepower#
```

```
show capture NET207 packet-number 4 trace
```

```
85 packets captured
```

```
4: 11:31:42.385951 802.1Q vlan#207 P6
```

```
192.168.104.61 > 224.0.0.13 ip-proto-103
```

```
, length 38
```

```
<-- Ingress PIM packet
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 5368 ns
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 5368 ns
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: INPUT-ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Elapsed time: 11224 ns
```

```
Config:
```

```
Additional Information:
```

```
Found next-hop 192.168.103.61 using egress ifc OUTSIDE(vrfid:0)
```

```
Phase: 4
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 3416 ns
Config:
Additional Information:
Found next-hop 192.168.103.61 using egress ifc OUTSIDE(vrfid:0)
```

```
Result:
input-interface: NET207(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Time Taken: 25376 ns
```

```
Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000558f240d6e15 flow (NA
```

```
<-- the packet is dropped due to RPF check failure
```

ASPテーブルのドロップとキャプチャは、RPFに失敗したパケットを示しています。

```
<#root>
```

```
firepower#
```

```
show asp drop
```

```
Frame drop:
```

```
Reverse-path verify failed (rpf-violated) 122
<-- Multicast RPF drops
Flow is denied by configured rule (acl-drop) 256
FP L2 rule drop (l2_acl) 768
```

RPF障害が原因で廃棄されたパケットをキャプチャするには、次のコマンドを実行します。

```
<#root>
```

```
firepower#
```

```
capture ASP type asp-drop rpf-violated
```

```
<#root>
```

```
firepower#
```

```
show capture ASP | include 224.0.0.13
```

```
2: 11:36:20.445960 802.1Q vlan#207 P6 192.168.104.50 > 224.0.0.13 ip-proto-103, length 38
10: 11:36:38.787846 802.1Q vlan#207 P6 192.168.104.61 > 224.0.0.13 ip-proto-103, length 38
15: 11:36:48.299743 802.1Q vlan#207 P6 192.168.104.50 > 224.0.0.13 ip-proto-103, length 46
16: 11:36:48.300063 802.1Q vlan#207 P6 192.168.104.61 > 224.0.0.13 ip-proto-103, length 46
```

トラブルシューティング手法

ファイアウォールのトラブルシューティング方法は、主にマルチキャストトポロジでのファイアウォールの役割によって異なります。次に、トラブルシューティングの推奨手順を示します。

1. 問題の説明と症状の詳細を明確にする。範囲をコントロールプレーン(IGMP/PIM)またはデータプレーン (マルチキャストストリーム) の問題に絞り込んでください。
2. ファイアウォールでマルチキャストの問題をトラブルシューティングするための必須の前提条件は、マルチキャストトポロジを明確にすることです。少なくとも、次のものを特定する必要があります。
 - マルチキャストトポロジでのファイアウォールの役割 (FHR、LHR、RP、またはその他の仲介役割)。
 - ファイアウォールで想定されるマルチキャスト入出カインターフェイス。
 - RP.
 - 送信元の送信元IPアドレス
 - マルチキャストは、IPアドレスと宛先ポートをグループ化します。
 - マルチキャストストリームのレシーバです。

3.マルチキャストルーティングのタイプ(スタブまたはPIMマルチキャストルーティング)を特定します。

- スタブマルチキャストルーティング：ダイナミックホスト登録を提供し、マルチキャストルーティングを容易にします。スタブマルチキャストルーティング用に設定されている場合、ASAはIGMPプロキシエージェントとして動作します。ASAは、マルチキャストルーティングに全面的に参加する代わりに、IGMPメッセージをアップストリームマルチキャストルータに転送します。これにより、マルチキャストデータの配信がセットアップされます。スタブモードルーティングを特定するには、show igmp interfaceコマンドを使用して、IGMP転送設定を確認します。

```
<#root>
```

```
firepower#
```

```
show igmp interface
```

```
inside is up, line protocol is up
  Internet address is 192.168.2.2/24
  IGMP is disabled on interface
outside is up, line protocol is up
  Internet address is 192.168.3.1/24
  IGMP is enabled on interface
```

```
Current IGMP version is 2
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Inbound IGMP access group is:
IGMP limit is 500, currently active joins: 0
Cumulative IGMP activity: 0 joins, 0 leaves
```

```
IGMP forwarding on interface inside
```

```
IGMP querying router is 192.168.3.1 (this system)
```

インターフェイスでPIMが有効になっているが、ネイバーシップが確立されていない。

```
<#root>
```

```
firepower#
```

```
show pim interface
```

Address	Interface	PIM	Nbr Count	Hello Intvl	DR Prior	DR
192.168.2.2	inside	on	0	30	1	this system
192.168.3.1	outside	on	0	30	1	this system

```
firepower# show pim neighbor
```

```
No neighbors found.
```

PIM-SM/BidirとIGMPフォワーディングは同時にはサポートされません。

RPアドレスなどのオプションは設定できません。

```
<#root>
```

```
%Error: PIM-SM/Bidir and IGMP forwarding are not supported concurrently
```

- PIMマルチキャストルーティング:PIMマルチキャストルーティングは最も一般的な導入です。ファイアウォールは、PIM-SMと双方向PIMの両方をサポートします。PIM-SMは、基盤となるユニキャストルーティング情報ベースまたは個別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャストルーティングプロトコルです。マルチキャストグループごとに1つのランデブーポイント(RP)をルートとする単方向共有ツリーを構築し、オプションでマルチキャストソースごとに最短パスツリーを作成します。この導入モードでは、スタブモードとは異なり、ユーザは通常、RPアドレスの設定を行い、ファイアウォールはピアとのPIM隣接関係を確立します。


```
<#root>
```

```
firepower#
```

```
show run pim
```

```
pim rp-address 10.10.10.1
```

```
firepower#
```

```
show pim group-map
```

Group Range	Proto	Client	Groups	RP address	Info
224.0.1.39/32*	DM	static	0	0.0.0.0	
224.0.1.40/32*	DM	static	0	0.0.0.0	
224.0.0.0/24*	L-Local	static	1	0.0.0.0	
232.0.0.0/8*	SSM	config	0	0.0.0.0	
224.0.0.0/4*	SM	config	1	10.10.10.1	RPF: inside,192.168.2.1 <--- RP address is 10.10.10.1
224.0.0.0/4	SM	static	0	0.0.0.0	RPF: ,0.0.0.0

```
firepower#
```

```
show pim neighbor
```

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.2.1	inside	00:02:52	00:01:19	1		
192.168.3.100	outside	00:03:03	00:01:39	1 (DR)		

4. RPのIPアドレスが設定されていて、到達可能性が高いことを確認します。

```
<#root>
```

```
firepower#
```

```
show run pim
```

```
pim rp-address 10.10.10.1
```

```
firepower#
```

```
show pim group-map
```

Group Range	Proto	Client	Groups	RP address	Info
224.0.1.39/32*	DM	static	0	0.0.0.0	
224.0.1.40/32*	DM	static	0	0.0.0.0	
224.0.0.0/24*	L-Local	static	1	0.0.0.0	
232.0.0.0/8*	SSM	config	0	0.0.0.0	
224.0.0.0/4*	SM	config	1	10.10.10.1	RPF: inside,192.168.2.1 <--- RP is 10.10.10.1
224.0.0.0/4	SM	static	0	0.0.0.0	RPF: ,0.0.0.0

```
<#root>
```

```
firepower#
```

```
show pim group-map
```

Group Range	Proto	Client	Groups	RP address	Info
224.0.1.39/32*	DM	static	0	0.0.0.0	
224.0.1.40/32*	DM	static	0	0.0.0.0	
224.0.0.0/24*	L-Local	static	1	0.0.0.0	
232.0.0.0/8*	SSM	config	0	0.0.0.0	
224.0.0.0/4*	SM	config	1	192.168.2.2	RPF: Tunnel0,192.168.2.2 (us) <--- "us" mean
224.0.0.0/4	SM	static	0	0.0.0.0	RPF: ,0.0.0.0

 警告：ファイアウォールをRPとFHRの両方に同時に設定することはできません。

5.マルチキャストトポロジでのファイアウォールの役割と問題の症状に応じて、追加の出力を確認します。

FHR

- インターフェイスTunnel0のステータスをチェックします。このインターフェイスは、PIMペイロード内のrawマルチキャストトラフィックをカプセル化し、PIMレジスタビットが設定されたRPにユニキャストパケットを送信するために使用されます。

```
<#root>
```

```
firepower#
```

```
show interface detail | b Interface Tunnel0
```

```
Interface Tunnel0 "", is up, line protocol is up
```

```
Hardware is Available but not configured via nameif
  MAC address 0000.0000.0000, MTU not set
  IP address unassigned
Control Point Interface States:
  Interface number is un-assigned
  Interface config status is active
  Interface state is active
```

```
firepower#
```

```
show pim tunnel
```

Interface	RP Address	Source Address
Tunnel0	10.10.10.1	192.168.2.2

- mroutesをチェックします。

```
<#root>
```

```
firepower#
```

```
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
```

```
(192.168.2.1, 230.1.1.1), 00:00:07/00:03:22, flags: SFT
```

```
  Incoming interface: inside
```

```
  RPF nbr: 192.168.2.1, Registering <--- Registering state
```

```
  Immediate Outgoing interface list:
```

```
    outside, Forward, 00:00:07/00:03:26
```

```
    Tunnel0, Forward, 00:00:07/never <--- Tunnel0 is in OIL, that indicates raw traffic is encapsulated.
```

ファイアウォールがRegister-Stopビットを含むPIMパケットを受信すると、OILからTunnel0が削除されます。その後、ファイアウォールはカプセル化を停止し、出カインターフェイス経由でrawマルチキャストトラフィックを送信します。

```
<#root>
```

```
firepower#
```

```
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
```

```
(192.168.2.1, 230.1.1.1), 00:07:26/00:02:59, flags: SFT
```

```
  Incoming interface: inside
```

```
  RPF nbr: 192.168.2.1
```

```
  Immediate Outgoing interface list:
```

```
    outside, Forward, 00:07:26/00:02:59
```

- PIMレジスタカウンタを確認します。

```
<#root>
```

```
firepower#
```

```
show pim traffic
```

```
PIM Traffic Counters
```

```
Elapsed time since counters cleared: 00:13:13
```

	Received	Sent	
Valid PIM Packets	42	58	
Hello	27	53	
Join-Prune	9	0	
Register	0	8	<--- Sent to the RP
Register Stop	6	0	<--- Received from the RP
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	

- ファイアウォールとRPの間のユニキャストPIMパケットキャプチャを確認します。

```
<#root>
```

```
firepower#
```

```
capture capo interface outside match pim any host 10.10.10.1 <--- RP IP
```

```
firepower#
```

```
show capture capi
```

```
4 packets captured
```

```
1: 09:53:28.097559      192.168.3.1 > 10.10.10.1 ip-proto-103, length 50      <--- Unicast to RP
2: 09:53:32.089167      192.168.3.1 > 10.10.10.1 ip-proto-103, length 50
```

```
3: 09:53:37.092890      192.168.3.1 > 10.10.10.1  ip-proto-103, length 50
4: 09:53:37.095850      10.10.10.1 > 192.168.3.1  ip-proto-103, length 18    <--- Unicast from RP
```

- 追加の出力を収集します (x.x.x.xはマルチキャストグループ、y.y.y.yはRP IP)。出力を数回収集することをお勧めします。

<#root>

```
show conn all protocol udp address x.x.x.x
```

```
show local-host x.x.x.x
```

```
show asp event dp-cp
```

```
show asp drop
```

```
show asp cluster counter
```

```
show asp table routing y.y.y.y
```

```
show route y.y.y.y
```

```
show mroute
```

```
show pim interface
```

```
show pim neighbor
show pim traffic
```

```
show igmp interface
```

```
show mfib count
```

- 生のマルチキャストインターフェイスパケットとASPドロップキャプチャを収集します。

<#root>

```
capture capi interface
```

```
buffer 32000000 match udp host X host Z <--- (ingress capture for multicast UDP traffic from host X)
```

```
capture capo interface
```

```
buffer 32000000 match udp host X host Z <--- (egress capture for multicast UDP traffic from host X)
```

```
capture asp type asp-drop buffer 32000000 match udp host X host Z <--- (ASP drop capture for multicast traffic)
```

- Syslogメッセージ：一般的なIDは、302015、302016、および710005です。

RP

- インターフェイスTunnel0のステータスをチェックします。このインターフェイスは、PIMペイロード内のrawマルチキャストトラフィックをカプセル化し、PIM-stopビットが設定されたユニキャストパケットをFHRに送信するために使用されます。

```
<#root>
```

```
firepower#
```

```
show interface detail | b Interface Tunnel0
```

```
Interface Tunnel0 "", is up, line protocol is up
```

```
Hardware is Available but not configured via nameif
MAC address 0000.0000.0000, MTU not set
IP address unassigned
```

```
Control Point Interface States:
  Interface number is un-assigned
  Interface config status is active
  Interface state is active
```

```
firepower#
```

```
show pim tunnel
```

Interface	RP Address	Source Address
Tunnel0	192.168.2.2	192.168.2.2
Tunnel0	192.168.2.2	-

- mroutesをチェックします。

```
<#root>
```

```
firepower#
```

```
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
```

```
(* , 230.1.1.1), 01:04:30/00:02:50, RP 192.168.2.2, flags: S <--- *,G entry
```

```
Incoming interface: Tunnel0
```

```
RPF nbr: 192.168.2.2
```

```
Immediate Outgoing interface list:
```

```
outside
```

```
, Forward, 01:04:30/00:02:50
```

```
(192.168.1.100, 230.1.1.1), 00:00:04/00:03:28, flags: ST S <--- S,G entry
```

```
Incoming interface:
```

```
inside
```

RPF nbr: 192.168.2.1
Immediate Outgoing interface list:

outside, Forward, 00:00:03/00:03:25

- PIMカウンタを確認します。

<#root>

firepower #

show pim traffic

PIM Traffic Counters

Elapsed time since counters cleared: 02:24:37

	Received	Sent
Valid PIM Packets	948	755
Hello	467	584
Join-Prune	125	32
Register	344	16
Register Stop	12	129
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

- 追加の出力を収集します (x.x.x.xはマルチキャストグループ、y.y.y.yはRP IP)。出力を数回収集することをお勧めします。

<#root>

show conn all protocol udp address x.x.x.x


```
show conn all | i PIM
```

```
show local-host x.x.x.x
```

```
show asp event dp-cp
```

```
show asp drop
```

```
show asp cluster counter
```

```
show asp table routing y.y.y.y
```

```
show route y.y.y.y
```

```
show mroute
```

```
show pim interface
```

```
show pim neighbor
```

```
show igmp interface
```

```
show mfib count
```

- rawマルチキャストインターフェイスパケットとASPドロップキャプチャを収集します。

```
<#root>
```

```
capture capi interface
```

```
buffer 32000000 match udp host X host Z <--- (ingress capture for multicast UDP traffic from host
```

```
capture capo interface
```

```
buffer 32000000 match udp host X host Z <--- (egress capture for multicast UDP traffic from host X)
```

```
capture asp type asp-drop buffer 32000000 match udp host X host Z <--- (ASP drop capture for multicast U
```

- Syslog : 一般的なIDは、302015、302016、および710005です。

LHR

RPと次の追加チェックのセクションで説明した手順を検討します。

- Mroutes:

```
<#root>
```

```
firepower#
```

```
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

```
(* , 230.1.1.1), 00:23:30/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver
```

Incoming interface:

```
inside
```

RPF nbr: 192.168.2.1

Immediate Outgoing interface list:

outside

, Forward, 00:23:30/never

(192.168.1.100, 230.1.1.1), 00:00:36/00:03:04, flags: SJT <--- J flag indicates switchover to SPT, T fla

Incoming interface:

inside

RPF nbr: 192.168.2.1

Inherited Outgoing interface list:

outside

, Forward, 00:23:30/never

(* , 230.1.1.2), 00:01:50/never, RP 10.10.10.1, flags: SCJ <--- C flag means connected receiver

Incoming interface:

inside

RPF nbr: 192.168.2.1

Immediate Outgoing interface list:

outside

, Forward, 00:01:50/never

(192.168.1.100, 230.1.1.2), 00:00:10/00:03:29, flags: SJT <--- <--- J flag indicates switchover to SPT,

Incoming interface:

inside

RPF nbr: 192.168.2.1

Inherited Outgoing interface list:

outside

, Forward, 00:01:50/never

- IGMPグループ :

<#root>

firepower#

show igmp groups detail <--- The list of IGMP groups

```
Interface:    outside
Group:        230.1.1.1

Uptime:       00:21:42
Router mode:  EXCLUDE (Expires: 00:03:17)
Host mode:    INCLUDE

Last reporter: 192.168.3.100 <--- Host joined group 230.1.1.1
```

```
Source list is empty
Interface:    outside
```

```
Group:        230.1.1.2
```

```
Uptime:       00:00:02
Router mode:  EXCLUDE (Expires: 00:04:17)
Host mode:    INCLUDE

Last reporter: 192.168.3.101 <--- Host joined group 230.1.1.2
```

```
Source list is empty
```

- IGMPトラフィック統計情報 :

```
<#root>
```

```
firepower#
```

```
show igmp traffic
```

```
IGMP Traffic Counters
```

```
Elapsed time since counters cleared: 1d04h
```

	Received	Sent
Valid IGMP Packets	2468	856
Queries	2448	856
Reports	20	0
Leaves	0	0
Mtrace packets	0	0
DVMRP packets	0	0
PIM packets	0	0

```
Errors:
```

Malformed Packets	0
Martian source	0
Bad Checksums	0

PIMトラブルシューティングコマンド (チートシート)

コマンド	説明
show running-config multicast-routingを使用します。	マルチキャストルーティングがファイアウォールで有効になっているかどうかを確認するには
show run mroute	ファイアウォールに設定されたスタティックmrouteを表示するには
show running-config pimを実行します。	ファイアウォールのPIM設定を表示するには
show pim interfaceコマンド	どのファイアウォールインターフェイスでPIMが有効になっており、PIMネイバーが存在するかを確認します。
show pim neighborコマンド	PIMネイバーを表示するには
show pim group-map (PIMのグループマップを表示)	RPにマッピングされたマルチキャストグループを表示するには
show mroute	完全なマルチキャストルーティングテーブルを表示するには
show mroute 230.10.10.10	特定のマルチキャストグループのマルチキャストテーブルを表示するには
show pim tunnel (PIMトンネルの表示)	ファイアウォールとRPの間にPIMトンネルが構築されているかどうかを確認する
show conn all detail address RP_IP_ADDRESS (すべての詳細アドレスのRP_IP_ADDRESS)	ファイアウォールとRPの間で接続 (PIMトンネル) が確立されているかどうかを確認する
show pim topology	ファイアウォールPIMトポロジ出力を表示するには
PIMのデバッグ	このデバッグでは、ファイアウォールとの間で送受信されるすべてのPIMメッセージが表示されます

debug pim group 230.10.10.10	このデバッグでは、特定のマルチキャストグループに関するファイアウォールとの間のすべてのPIMメッセージが表示されます
show pim traffic	送受信されたPIMメッセージに関する統計情報を表示する
show asp clusterカウンタ	低速パスと高速パスとコントロールポイントで処理されたパケットの数を確認する
show asp drop	ファイアウォール上のすべてのソフトウェアレベルのドロップを表示する
capture CAP interface INSIDE trace match pim any any	ファイアウォール上の入力PIMマルチキャストパケットをキャプチャしてトレースするため
cap interface INSIDEトレースのキャプチャ : udp host 224.1.2.3 any	入力マルチキャストストリームをキャプチャしてトレースする
show pim bsr-router	選出されたBSRルータを確認する
show conn allアドレス224.1.2.3	親マルチキャスト接続を表示する
show local-host 224.1.2.3 (ローカルホストの表示)	子/スタブマルチキャスト接続を表示する

ファイアウォールキャプチャの詳細については、「[Firepower脅威対策キャプチャとPacket Tracerを使用する](#)」を参照してください。

既知の問題

Firepowerマルチキャストの制限：

- IPv6をサポートしない
- PIM/IGMPマルチキャストは、トラフィックゾーン(EMCP)内のインターフェイスではサポートされません。
- ファイアウォールをRPとFHRに同時に設定することはできません。
- show conn allコマンドでは、IDマルチキャスト接続だけが表示されます。スタブ/セカンダ

リマルチキャスト接続を表示するには、show local-host <group IP> コマンドを使用します。

PIMはvPC Nexusではサポートされない

Nexus vPCとファイアウォールの間にPIMアジャセンシー関係を展開しようとする、次に示すNexusの制限があります。

[Nexusプラットフォームにおける仮想ポートチャンネルを介したルーティングでサポートされるトポロジ](#)

NGFWの観点からは、次のドロップをトレースしてキャプチャを確認できます。

```
<#root>
```

```
Result:
```

```
input-interface: NET102
```

```
input-status: up
```

```
input-line-status: up
```

```
output-interface: NET102
```

```
output-status: up
```

```
output-line-status: up
```

```
Action: drop
```

```
Drop-reason: (no-mcast-intrf) FP no mcast output intrf      <-- The ingress multicast packet is dropped
```

ファイアウォールがRP登録を完了できません：

```
<#root>
```

```
firepower#
```

```
show mroute 224.1.2.3
```

```
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
```

```
(*, 224.1.2.3), 01:05:21/never, RP 10.1.0.209, flags: SCJ
```

```
  Incoming interface: OUTSIDE
```

```
  RPF nbr: 10.1.104.10
```

```
  Immediate Outgoing interface list:
```

```
    Server_102, Forward, 01:05:21/never
```

```
(10.1.1.48, 224.1.2.3), 00:39:15/00:00:04, flags: SFJT
```

```
  Incoming interface: NET102
```

```
  RPF nbr: 10.1.1.48, Registering      <-- The RP Registration is stuck
```

```
  Immediate Outgoing interface list:
```

宛先ゾーンがサポートされていない

マルチキャストトラフィックに一致するアクセスコントロールポリシールールには、宛先セキュリティゾーンを指定できません。

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action
1	allow_multicast	INSIDE_ZONE	OUTSIDE_ZONE	Any	224.1.2.3	Any	Any	Any	Any	Any	Any	Any	Any	Allow

これは、FMCユーザガイドにも記載されています。

Internet multicast routing from address range 224.0.0/24 is not supported; IGMP group is not created when enabling multicast routing for the reserved addresses.

Clustering

In clustering, for IGMP and PIM, this feature is only supported on the primary unit.

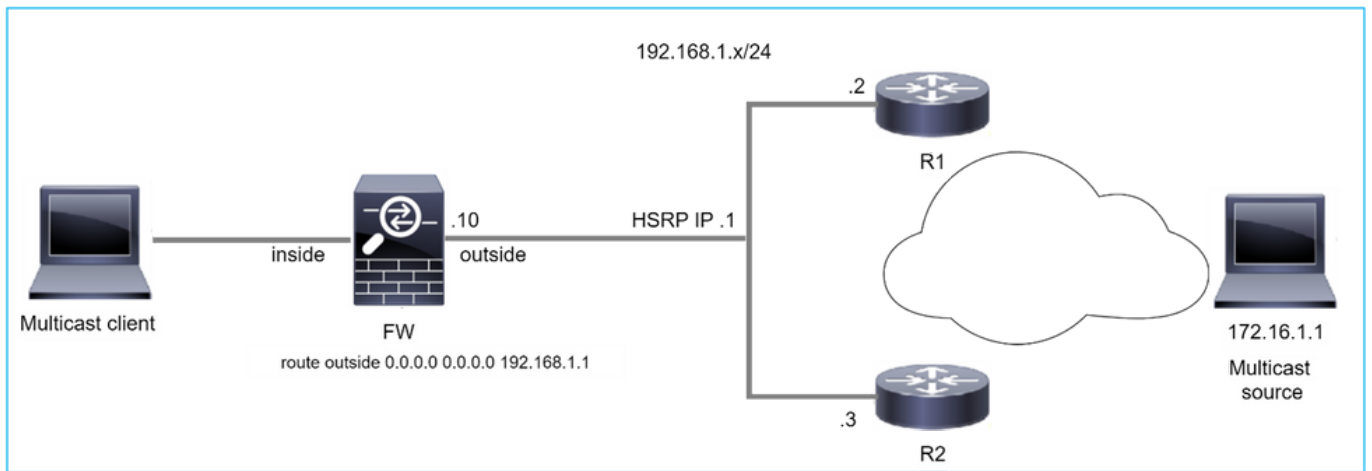
Additional Guidelines

- You must configure an access control or prefilter rule on the inbound security zone to allow traffic to the multicast host, such as 224.1.2.3. However, you cannot specify a destination security zone for the rule, or it cannot be applied to multicast connections during initial connection validation.
- You cannot disable an interface with PIM configured on it. If you have configured PIM on the interface (see [Configure PIM Protocol](#)), disabling the multicast routing and PIM does not remove the PIM configuration. You must remove (delete) the PIM configuration to disable the interface.
- PIM/IGMP Multicast routing is not supported on interfaces in a traffic zone.
- Do not configure FTD to simultaneously be a Rendezvous Point (RP) and a First Hop Router.

Configure IGMP Features

IP hosts use IGMP to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP

HSRPが原因でファイアウォールが上流に位置するルータへのPIMメッセージを送信しない



この場合、ファイアウォールには、ホットスタンバイ冗長プロトコル(HSRP)IP 192.168.1.1およびルータR1とR2とのPIMネイバースhipを経由するデフォルトルートがあります。

```
<#root>
```

```
firepower#
```

```
show run route
```

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

ファイアウォールは、R1とR2の外部インターフェイスIPと物理インターフェイスIPの間にPIM隣接関係を確立します。

```
<#root>
```

```
firepower#
```

```
show pim neighbor
```

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.1.1	outside	01:18:27	00:01:25	1		
192.168.1.2	outside	01:18:03	00:01:29	1	(DR)	

ファイアウォールはアップストリームネットワークにPIM Joinメッセージを送信しません。PIM debugコマンドのdebug pimは次の出力を示します。

```
<#root>
```

```
firepower#
```

```
debug pim
```

```
...
```

IPv4 PIM: Sending J/P to an invalid neighbor: outside 192.168.1.1

[RFC 2362](#) には「ルータは、(S,G)、(*,G)、および(*,*,RP)の各エントリに関連付けられた明確なRPF ネイバーに対して、定期的にJoin/Prune メッセージを送信する。Join/Prune メッセージは、RPF ネイバーがPIM ネイバーである場合にのみ送信される」と定義されています。」

この問題を軽減するために、ユーザはスタティックなmrouteエントリをファイアウォールに追加できます。ルータは、2つのルータインターフェイスIPアドレスの1つ、192.168.1.2または192.168.1.3 (通常はHSRPアクティブルータIP) をポイントしている必要があります。

以下に例を挙げます。

```
<#root>
```


```
firepower#
```

```
show run mroute
```

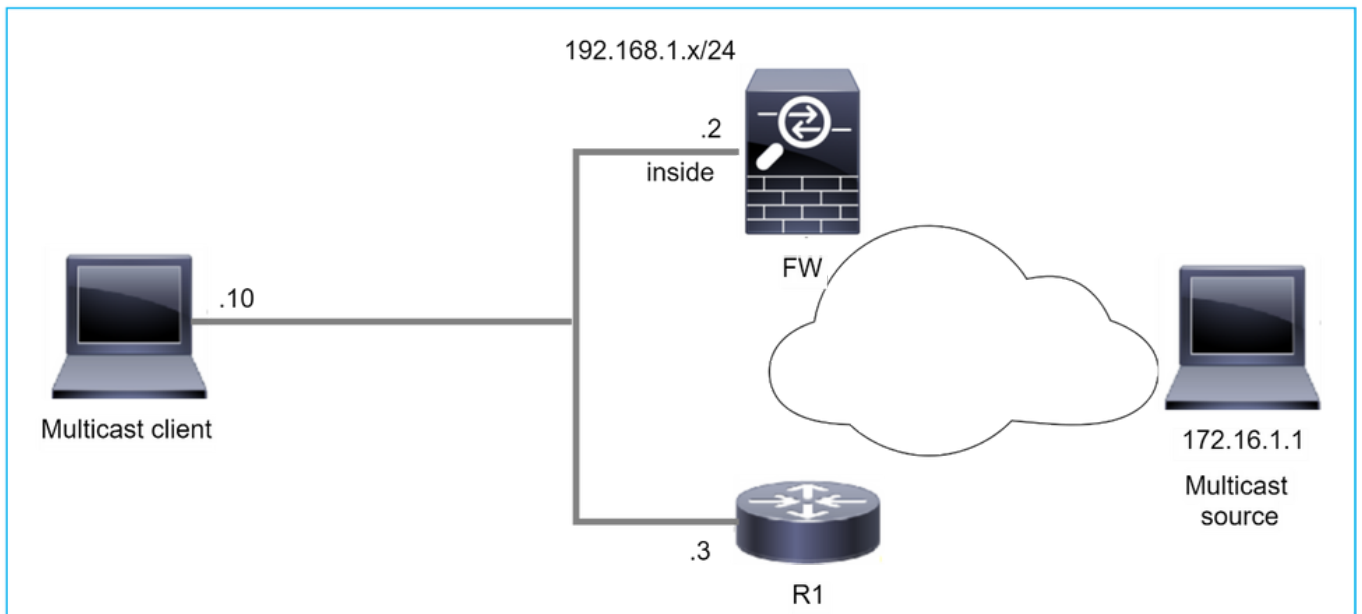
```
firepower#
```

```
mroute 172.16.1.1 255.255.255.255 192.168.1.2
```

スタティックなmrouteの設定が完了すると、RPFルックアップのために、ファイアウォールはASAのユニキャストルーティングテーブルではなくマルチキャストルーティングテーブルを優先し、PIMメッセージをネイバー192.168.1.2に直接送信します。

 注：スタティックなmrouteは、mrouteがアドレスまたはネットマスクごとに1つのネクストホップしか受け入れないため、HSRP冗長性の有用性を損なうものです。mrouteコマンドで指定されたネクストホップに障害が発生したり、到達不能になった場合、ファイアウォールは他のルータにフォールバックしません。

ファイアウォールがLANセグメントのDRでない場合、LHRと見なされない



ファイアウォールには、LANセグメントのPIMネイバーとしてR1があります。R1はPIM DRです。

<#root>

firepower#

show pim neighbor

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.1.3	inside	00:12:50	00:01:38	1	(DR)	

クライアントからのIGMP参加要求を受信した場合、ファイアウォールはLHRになりません。

mrouteはOILとして追加のNullを示し、Prunedフラグを持っています。

<#root>

firepower#

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

(* , 230.1.1.1), 00:06:30/never, RP 0.0.0.0,

```
flags
: S
P
C
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Immediate Outgoing interface list:

inside, Null, 00:06:30/never <--- OIL has inside and Null
```

ファイアウォールをLHRにするため、インターフェイスのDRプライオリティを上げることができません。

```
<#root>
firepower#
interface GigabitEthernet0/0

firepower#
pim dr-priority 2

firepower#
show pim neighbor

Neighbor Address  Interface          Uptime    Expires DR pri Bidir
192.168.1.3       inside             17:05:28  00:01:41 1
```

PIM debugコマンドのdebug pimは次の出力を示します。

```
<#root>
firepower#
debug pim
firepower#

IPv4 PIM: (*,230.1.1.1) inside Start being last hop <--- Firewall considers itself as the lasp hop

IPv4 PIM: (*,230.1.1.1) Start being last hop
```

```
IPv4 PIM: (*,230.1.1.1) Start signaling sources
IPv4 PIM: [0] (*,230.1.1.1/32) NULLIF-skip MRIB modify NS
IPv4 PIM: (*,230.1.1.1) inside FWD state change from Prune to Forward
IPv4 PIM: [0] (*,230.1.1.1/32) inside MRIB modify F NS
IPv4 PIM: (*,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (*,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: (*,230.1.1.1) Processing timers
IPv4 PIM: (*,230.1.1.1) J/P processing
IPv4 PIM: (*,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (*,230.1.1.1) No RPF interface to send J/P
```

PrunedフラグとNullはmrouteから削除されます。

```
<#root>
```

```
firepower#
```

```
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
```

```
(*, 230.1.1.1), 16:48:23/never, RP 0.0.0.0, flags:
```

```
SCJ
```

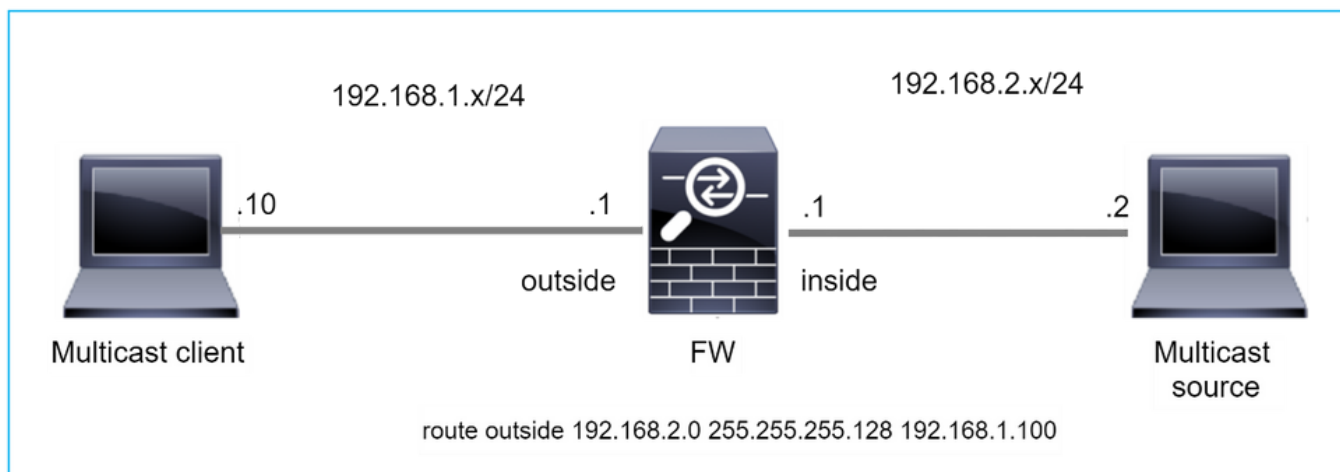
```
  Incoming interface: Null
```

```
  RPF nbr: 0.0.0.0
```

```
  Immediate Outgoing interface list:
```

```
    inside, Forward, 16:48:23/never
```

Reverse Path Forwarding(RPF)チェックの失敗によりファイアウォールがマルチキャストパケットをドロップする



この場合、ファイアウォールには外部インターフェイスを経由するマスクが255.255.255.128のより詳細なルートがあるため、マルチキャストUDPパケットはRPF障害のためにドロップされます。

```
<#root>
```

```
firepower#
```

```
capture capi type raw-data trace interface inside match udp any any
```

```
firepower#
```

```
show capture capi packet-number 1 trace
```

```
106 packets captured
```

```
1: 08:57:18.867234 192.168.2.2.12345 > 230.1.1.1.12354: udp 500
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 2684 ns
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Elapsed time: 2684 ns
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 3
```

```
Type: INPUT-ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

Elapsed time: 13664 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc outside

Phase: 4
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 8296 ns
Config:
Additional Information:
Found next-hop 192.168.1.100 using egress ifc outside

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Time Taken: 27328 ns

Drop-reason: (rpf-violated) Reverse-path verify failed, Drop-location: frame 0x0000556bcb1069dd flow

(NA)/NA

firepower#

show route static

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

S 192.168.2.0 255.255.255.128 [1/0] via 192.168.1.100, outside

ASPドロップキャプチャは、rpf-violatedドロップの理由を示します。

<#root>

firepower#

show capture asp

Target: OTHER
Hardware: ASAV
Cisco Adaptive Security Appliance Software Version 9.19(1)
ASLR enabled, text region 556bc9390000-556bcd0603dd

21 packets captured

```
1: 09:00:53.608290      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Reverse
2: 09:00:53.708032      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
3: 09:00:53.812152      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
4: 09:00:53.908613      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) R
```

MFIB出力のRPF失敗カウンタが増加します。

<#root>

firepower#

```
show mfib 230.1.1.1 count
```

IP Multicast Statistics

7 routes, 4 groups, 0.00 average sources per group

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 230.1.1.1

RP-tree:

Forwarding: 0/0/0/0, Other: 6788/6788/0

...

firepower#

```
show mfib 230.1.1.1 count
```

IP Multicast Statistics

7 routes, 4 groups, 0.00 average sources per group

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 230.1.1.1

RP-tree:

Forwarding: 0/0/0/0, Other: 6812/6812/0 <--- RPF failed counter increased

解決策は、RPFチェックの障害を修正することです。1つのオプションは、スタティックルートを削除することです。

RPFチェックの失敗がこれ以上ない場合、パケットは転送され、MFIB出力のForwardingカウンタが増加します。

<#root>

firepower#

show mfib 230.1.1.1 count

IP Multicast Statistics

8 routes, 4 groups, 0.25 average sources per group

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 230.1.1.1

RP-tree:

Forwarding: 0/0/0/0, Other: 9342/9342/0

Source: 192.168.2.2,

Forwarding: 1033/9/528/39

, Other: 0/0/0

Tot. shown: Source count: 1, pkt count: 0

...

firepower#

show mfib 230.1.1.1 count

IP Multicast Statistics

8 routes, 4 groups, 0.25 average sources per group

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 230.1.1.1

RP-tree:

Forwarding: 0/0/0/0, Other: 9342/9342/0

Source: 192.168.2.2,

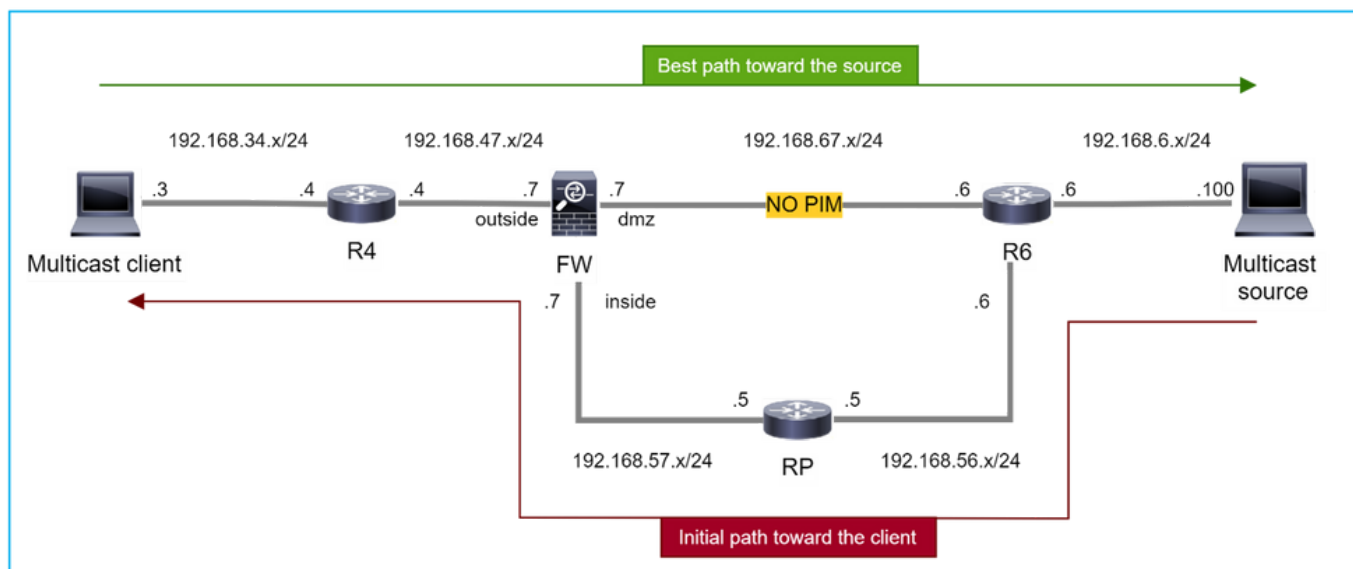
Forwarding: 1044/10/528/41

, Other: 0/0/0

<--- Forward counter increased

Tot. shown: Source count: 1, pkt count: 0

ソースツリーへのPIMスイッチオーバー時にファイアウォールがPIM参加を生成しない



この場合、ファイアウォールはdmzインターフェイスR4 > FW > R6を介してマルチキャスト送信元へのパスを学習しますが、送信元からクライアントへの最初のトラフィックパスはR6 > RP > DW > R4です。

<#root>

firepower#

show route 192.168.6.100

```
Routing entry for 192.168.6.0 255.255.255.0
  Known via "ospf 1", distance 110, metric 11, type intra area
```

Last update from 192.168.67.6 on dmz, 0:36:22 ago

Routing Descriptor Blocks:

* 192.168.67.6, from 192.168.67.6, 0:36:22 ago, via dmz

Route metric is 11, traffic share count is 1

R4はSPTスイッチオーバーを開始し、SPTスイッチオーバーのしきい値に達すると、送信元固有のPIM joinメッセージを送信します。ファイアウォールではSPTスイッチオーバーは行われず、(S,G)mrouteにはTフラグがありません。

<#root>

firepower#

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

(* , 230.1.1.1), 00:00:05/00:03:24, RP 10.5.5.5, flags: S

Incoming interface: inside

RPF nbr: 192.168.57.5

Immediate Outgoing interface list:

outside, Forward, 00:00:05/00:03:24

(192.168.6.100, 230.1.1.1), 00:00:05/00:03:24, flags: S

Incoming interface: dmz

RPF nbr: 192.168.67.6

Immediate Outgoing interface list:

outside, Forward, 00:00:05/00:03:2

PIM debugコマンドdebug pimは、ピアR4から2つの受信PIM Join要求(S、G)および(S、G)を示します。ファイアウォールが(*,G)アップストリームに対するPIM Join要求を送信しましたが、ネイバー192.168.67.6が無効なため、送信元固有の要求を送信できませんでした。

```
<#root>
```

```
firepower#
```

```
debug pim
```

```
IPv4 PIM: Received J/P on outside from 192.168.47.4 target: 192.168.47.7 (to us) <--- 1st PIM join to th
```

```
IPv4 PIM: J/P entry: Join root: 10.5.5.5 group: 230.1.1.1 flags: RPT WC S <--- 1st PIM join with root a
```

```
IPv4 PIM: (*,230.1.1.1) Create entry
```

```
IPv4 PIM: [0] (*,230.1.1.1/32) MRIB modify DC
```

```
IPv4 PIM: [0] (*,230.1.1.1/32) inside MRIB modify A
```

```
IPv4 PIM: (*,230.1.1.1) outside J/P state changed from Null to Join
```

```
IPv4 PIM: (*,230.1.1.1) outside Raise J/P expiration timer to 210 seconds
```

```
IPv4 PIM: (*,230.1.1.1) outside FWD state change from Prune to Forward
```

```
IPv4 PIM: [0] (*,230.1.1.1/32) outside MRIB modify F NS
```

```
IPv4 PIM: (*,230.1.1.1) Updating J/P status from Null to Join
```

```
IPv4 PIM: (*,230.1.1.1) J/P scheduled in 0.0 secs
```

```
IPv4 PIM: (*,230.1.1.1) Processing timers
```

```
IPv4 PIM: (*,230.1.1.1) J/P processing
```

```
IPv4 PIM: (*,230.1.1.1) Periodic J/P scheduled in 50 secs
```

```
IPv4 PIM: (*,230.1.1.1) J/P adding Join on inside
```

```
IPv4 PIM: Sending J/P message for neighbor 192.168.57.5 on inside for 1 groups <--- PIM Join sent from
```

IPv4 PIM: Received J/P on outside from 192.168.47.4 target: 192.168.47.7 (to us) <--- 1st PIM join to th

IPv4 PIM: J/P entry: Join root: 192.168.6.100 group: 230.1.1.1 flags: S <--- 1st PIM join with

```
IPv4 PIM: (192.168.6.100,230.1.1.1) Create entry
IPv4 PIM: Adding monitor for 192.168.6.100
IPv4 PIM: RPF lookup for root 192.168.6.100: nbr 192.168.67.6, dmz via the rib
IPv4 PIM: (192.168.6.100,230.1.1.1) RPF changed from 0.0.0.0/- to 192.168.67.6/dmz
IPv4 PIM: (192.168.6.100,230.1.1.1) Source metric changed from [0/0] to [110/11]
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) MRIB modify DC
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) inside MRIB modify A
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) outside MRIB modify F NS
IPv4 PIM: (192.168.6.100,230.1.1.1) outside J/P state changed from Null to Join
IPv4 PIM: (192.168.6.100,230.1.1.1) outside Imm FWD state change from Prune to Forward
IPv4 PIM: (192.168.6.100,230.1.1.1) Updating J/P status from Null to Join
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P scheduled in 0.0 secs
IPv4 PIM: [0] (192.168.6.100,230.1.1.1/32) dmz MRIB modify NS
IPv4 PIM: (192.168.6.100,230.1.1.1) outside Raise J/P expiration timer to 210 seconds
IPv4 PIM: (192.168.6.100,230.1.1.1) Processing timers
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P processing
IPv4 PIM: (192.168.6.100,230.1.1.1) Periodic J/P scheduled in 50 secs
IPv4 PIM: (192.168.6.100,230.1.1.1) J/P adding Join on dmz

IPv4 PIM: Sending J/P to an invalid neighbor: dmz 192.168.67.6
```

<--- Invalid neighbor

show pim neighbourコマンドの出力にR6がありません。

<#root>

firepower#

show pim neighbor

Neighbor Address	Interface	Uptime	Expires	DR	pri	Bidir
192.168.47.4	outside	00:21:12	00:01:44	1		
192.168.57.5	inside	02:43:43	00:01:15	1		

ファイアウォールインターフェイスdmzでPIMが有効になっている。

<#root>

firepower#

show pim interface

Address	Interface	PIM	Nbr	Hello	DR	DR
			Count	Intvl	Prior	

```
192.168.47.7    outside    on 1    30    1    this system
192.168.67.7    dmz        on 0    30    1    this system
192.168.57.7    inside     on 1    30    1    this system
```

R6インターフェイスでPIMが無効になっている。

```
<#root>
```

```
R6#
```

```
show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.6.1	YES	manual	up	up
GigabitEthernet0/1	192.168.56.6	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	192.168.67.6	YES	manual	up	up
Tunnel0	192.168.56.6	YES	unset	up	up

```
R6#
```

```
show ip pim interface GigabitEthernet0/3 detail
```

```
GigabitEthernet0/3 is up, line protocol is up
 Internet address is 192.168.67.6/24
 Multicast switching: fast
 Multicast packets in/out: 0/123628
 Multicast TTL threshold: 0
```

```
PIM: disabled <--- PIM is disabled
```

```
 Multicast Tagswitching: disabled
```

解決策は、R6のインターフェイスGigabitEthernet0/3でPIMを有効にすることです。

```
<#root>
```

```
R6(config-if)#
```

```
interface GigabitEthernet0/3
```

```
R6(config-if)#
```

```
ip pim sparse-mode
```

```
R6(config-if)#
```

```
*Apr 21 13:17:14.575: %PIM-5-NBRCHG: neighbor 192.168.67.7 UP on interface GigabitEthernet0/3
```

```
*Apr 21 13:17:14.577: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to 192.168.67.7 on interface GigabitEthernet0/3
```

ファイアウォールは、SPTスイッチオーバーを示すTフラグをインストールします：を入力します。

```
<#root>
```

```
firepower#
```

```
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
```

```
(* , 230.1.1.1), 00:26:30/00:02:50, RP 10.5.5.5, flags: S
```

```
Incoming interface: inside
```

```
RPF nbr: 192.168.57.5
```

```
Immediate Outgoing interface list:
```

```
outside, Forward, 00:26:30/00:02:50
```

```
(192.168.6.100, 230.1.1.1), 00:26:30/00:03:29, flags: ST
```

```
Incoming interface: dmz
```

```
RPF nbr: 192.168.67.6
```

```
Immediate Outgoing interface list:
```

```
outside, Forward, 00:26:30/00:02:39
```

パントレート制限によりファイアウォールが最初の数パケットをドロップする

ファイアウォールがFPで新しいマルチキャストストリームの最初のパケットを受信する場合、CPによる追加処理が必要になる場合があります。この場合、FPは追加操作のためにSP(FP > SP > CP)を介してパケットをCPにパントします。

- 入インターフェイスとIDインターフェイス間のFPでの親接続の作成。
- RPF検証、PIMカプセル化 (ファイアウォールがFHRの場合)、OILチェックなど、その他のマルチキャスト固有のチェック。
- mrouteテーブルの着信インターフェイスと発信インターフェイスを使用した(S,G)エントリの作成。
- 着信インターフェイスと発信インターフェイス間のFPでの子/スタブ接続の作成。

コントロールプレーン保護の一部として、ファイアウォールはCPにパントされるパケットのレー

トを内部で制限します。

レートを超えるパケットは、punt-rate-limitドロップの理由でドロップされます。

```
<#root>
```

```
firepower#
```

```
show asp drop
```

Frame drop:

```
Punt rate limit exceeded (punt-rate-limit) 2062
```

SPからCPにパントされたマルチキャストパケットの数を確認するには、show asp cluster counterコマンドを使用します。

```
<#root>
```

```
firepower#
```

```
show asp cluster counter
```

Global dp-counters:

Context specific dp-counters:

MCAST_FP_FROM_PUNT	30	Number of multicast packets punted from CP to FP
MCAST_FP_TO_SP	2680	Number of multicast packets punted from FP to SP
MCAST_SP_TOTAL	2710	Number of total multicast packets processed in SP
MCAST_SP_FROM_PUNT	30	Number of multicast packets punted from CP to SP <--- Number of
MCAST_SP_FROM_PUNT_FORWARD	30	Number of multicast packets coming from CP that are forwarded
MCAST_SP_PKTS	30	Number of multicast packets that require slow-path attention
MCAST_SP_PKTS_TO_CP	30	Number of multicast packets punted to CP from SP
MCAST_FP_CHK_FAIL_NO_HANDLE	2650	Number of multicast packets failed with no flow mcast_handle
MCAST_FP_CHK_FAIL_NO_FP_FWD	30	Number of multicast packets that cannot be fast-path forwarded

show asp event dp-cp puntコマンドを使用して、FP > CPキューのパケット数と15秒のレートを確認します。

```
<#root>
```

```
firepower#
```

```
show asp event dp-cp punt | begin EVENT-TYPE
```

```
EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
```

```

punt                24452         0        24452         0        10852        1402

multicast
    23800         0
23800
    0         10200
1402

pim                 652         0         652         0         652         0

```

mrouteが設定され、FPで親子接続が確立されると、パケットは既存の接続の一部としてFPに転送されます。この場合、FPはパケットをCPにパントしません。

ファイアウォールは新しいマルチキャストストリームの最初のパケットをどのように処理しますか。

ファイアウォールがデータパス内の新しいマルチキャストストリームの最初のパケットを受信すると、ファイアウォールは次のアクションを実行します。

1. セキュリティポリシーでパケットが許可されているかどうかを確認します。
2. パスFPを介してパケットをCPにパントします。
3. 入インターフェイスとIDインターフェイスの間に親接続を作成します。

<#root>

```
firepower#
```

```
show capture capi packet-number 1 trace
```

```
10 packets captured
```

```
1: 08:54:15.007003      192.168.1.100.12345 > 230.1.1.1.12345:  udp 400
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
MAC Access list
```


Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.2.1 using egress ifc inside

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: QOS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9

Type: MULTICAST

Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10

Type: FLOW-CREATION

Subtype:
Result: ALLOW

Config:

Additional Information:

New flow created with id 19, packet dispatched to next module <--- New flow

Result:

input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up

Action: allow

Syslog:

<#root>

firepower# Apr 24 2023 08:54:15: %ASA-7-609001: Built local-host inside:192.168.1.100

Apr 24 2023 08:54:15: %FTD-7-609001: Built local-host identity:230.1.1.1

Apr 24 2023 08:54:15: %FTD-6-302015: Built inbound UDP connection 19 for inside:192.168.1.100/12345 (192.168.1.100)

この接続は、show conn allコマンドの出力に表示されます。

<#root>

firepower#

show conn all protocol udp

13 in use, 17 most used

UDP inside 192.168.1.100:12345 NP Identity Ifc 230.1.1.1:12345, idle 0:00:02, bytes 0, flags -

4. CPは、RPF検証、PIMカプセル化 (ファイアウォールがFHRの場合)、OILチェックなど、追加のマルチキャスト固有のチェックのためにマルチキャストプロセスを実行します。
5. CPは、mrouteに着信インターフェイスと発信インターフェイスを持つ(S,G)エントリを作成します。

<#root>

firepower#

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

(* , 230.1.1.1), 00:19:28/00:03:13, RP 192.168.192.168, flags: S

Incoming interface: inside

RPF nbr: 192.168.2.1

Immediate Outgoing interface list:

outside, Forward, 00:19:28/00:03:13

(192.168.1.100, 230.1.1.1), 00:08:50/00:03:09, flags: ST

Incoming interface: inside

RPF nbr: 192.168.2.1

Immediate Outgoing interface list:

outside, Forward, 00:00:32/00:02:57

6. CPは、着信インターフェイスと発信インターフェイスの間に子/スタブ接続を作成するように、CP > SP > FPパス経由でFPに指示します。

この接続は、show local-hostコマンドの出力にのみ表示されます。

<#root>

firepower#

show local-host

Interface outside: 5 active, 5 maximum active

local host: <224.0.0.13> ,

local host: <192.168.3.100> ,

local host: <230.1.1.1> ,

Conn:

UDP outside 230.1.1.1:12345 inside 192.168.1.100:12345, idle

0:00:04, bytes 4000, flags -

local host: <224.0.0.5> ,

local host: <224.0.0.1> ,

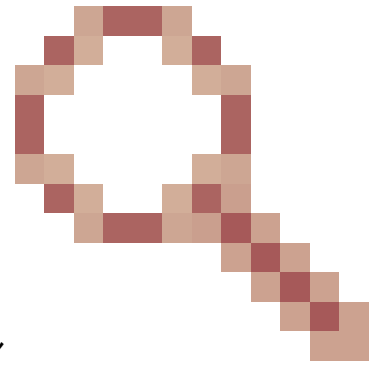
Interface inside: 4 active, 5 maximum active

local host: <192.168.1.100> ,

Conn:

```
UDP outside 230.1.1.1:12345 inside 192.168.1.100:12345, idle
```

```
0:00:04, bytes 4000, flags -  
local host: <224.0.0.13>,  
local host: <192.168.2.1>,  
local host: <224.0.0.5>,  
Interface nlp_int_tap: 0 active, 2 maximum active  
Interface any: 0 active, 0 maximum active
```



Cisco Bug ID [CSCwe21280](#)の修正が適用されたソフトウェアバージョンの場合、子/スタブ接続のsyslogメッセージ302015も生成されます。

```
<#root>
```

```
Apr 24 2023 08:54:15: %FTD-6-302015:
```

```
Built outbound UDP connection 20 for outside:230.1.1.1/12345 (230.1.1.1/12345) to inside:192.168.1.100/1
```

親と子/スタブの両方の接続が確立されると、入力パケットは既存の接続と一致し、FPで転送されます。

```
<#root>
```

```
firepower#
```

```
show capture capi trace packet-number 2
```

```
10 packets captured
```

```
2: 08:54:15.020567 192.168.1.100.12345 > 230.1.1.1.12345: udp 400
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
MAC Access list
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

Implicit Rule
Additional Information:
MAC Access list

Phase: 3

Type: FLOW-LOOKUP

Subtype:
Result: ALLOW
Config:
Additional Information:

Found flow with id 19, using existing flow <--- Existing flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow

ICMPマルチキャストトラフィックのフィルタリング

ACLを使用してICMPマルチキャストトラフィックをフィルタリングすることはできません。コントロールプレーンポリシー(ICMP)を使用する必要があります。

Cisco Bug ID [CSCsl26860](#) ASAがマルチキャストICMPパケットをフィルタリングしない

既知のPIMマルチキャスト不具合

既知の不具合については、Bug Search Tool(<https://bst.cloudapps.cisco.com/bugsearch>)を使用できます。

ほとんどのASAおよびFTD不具合は、「Cisco適応型セキュリティアプライアンス(ASA)ソフトウェア」製品の下にリストされています。

Bug Search Tool

Search For 1

Product 2 Select from List

Release

The results

94 Results | Sorted by Severity Sort By: Show All

<p>Filters Clear Filters</p> <p>Severity <input type="text" value="Show All"/></p> <p>Status <input type="text" value="Show All"/></p>	<p>CSCsy08778 no pim on one subif disables eigrp on same physical of 4 ge module Symptom: eigrp stops working on one subinterface, if "no pim" is issued on another subinterface which belongs to the same physical interface. Conditions: The physical interface belongs to the 4-GE module. If using the main-board Severity: 2 Status: Fixed Updated: Nov 09, 2016 Cases:3 ★★☆☆☆ (0)</p> <p>CSCtg52478 PIM nbr jp_buffer can be corrupted under stress Symptom: memory corruption of pim nbr structure Conditions: multicast w/ PIM-SM and heavy traffic and CLI</p>
---	--

関連情報

- [ASA マルチキャスト トラブルシューティングと一般的な問題](#)
- [Firepower Management Center マルチキャスト](#)
- [firepower マルチキャスト フラグの要約](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。