

Fehlerbehebung bei Firepower Threat Defense und ASA Multicast PIM

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Grundlagen des Multicast-Routings](#)

[Abkürzungen/Akronyme](#)

[Aufgabe 1: PIM Sparse Mode \(statischer RP\)](#)

[Aufgabe 2: Konfigurieren des PIM-Bootstrap-Routers \(BSR\)](#)

[Methodik der Fehlerbehebung](#)

[Befehle zur PIM-Fehlerbehebung \(Kurzreferenz\)](#)

[Bekanntes Probleme](#)

[PIM wird auf einem vPC-Nexus nicht unterstützt](#)

[Zielzonen werden nicht unterstützt](#)

[Firewall sendet aufgrund von HSRP keine PIM-Nachrichten an Upstream-Router](#)

[Die Firewall wird nicht als LHR betrachtet, wenn sie nicht der DR im LAN-Segment ist.](#)

[Die Firewall lässt Multicast-Pakete aufgrund eines Fehlers bei der Überprüfung der Umkehrpfad-Weiterleitung verloren](#)

[Firewall generiert beim PIM-Switchover zum Source-Tree keinen PIM-Join](#)

[Firewall verwirft die ersten paar Pakete aufgrund von Punt-Rate Limit](#)

[ICMP-Multicast-Datenverkehr filtern](#)

[Bekanntes PIM-Multicast-Fehler](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Firepower Threat Defense (FTD) und Adaptive Security Appliance (ASA) Protocol Independent Multicast (PIM) implementieren.

Voraussetzungen

Anforderungen

Grundlegende Kenntnisse zu IP-Routing

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FirePOWER 4125 Threat Defence Version 7.1.0
- FirePOWER Management Center (FMC) Version 7.1.0
- Cisco Adaptive Security Appliance-Software Version 9.17(1)9.

Hintergrundinformationen

Grundlagen des Multicast-Routings

- Unicast leitet Pakete an das Ziel weiter, während **Multicast Pakete von der Quelle weg weiterleitet**.
- Multicast-Netzwerkgeräte (Firewalls/Router usw.) leiten die Pakete über **Reverse Path Forwarding (RPF) weiter**. Beachten Sie, dass RPF nicht mit uRPF identisch ist, das in Unicast verwendet wird, um bestimmte Angriffstypen zu verhindern. RPF kann als Mechanismus definiert werden, der Multicast-Pakete von der Quelle weg an Schnittstellen weiterleitet, die zu Multicast-Empfängern führen. Seine primäre Rolle besteht darin, Datenverkehrsschleifen zu verhindern und korrekte Datenverkehrspfade sicherzustellen.
- Ein Multicast-Protokoll wie PIM hat drei Hauptfunktionen:

1. Suchen Sie die **Upstream-Schnittstelle** (Schnittstelle, die der Quelle am nächsten liegt).

2. Suchen Sie die **Downstream-Schnittstellen**, die einem bestimmten Multicast-Stream zugeordnet sind (Schnittstellen zu den Empfängern).

3. Beibehalten des Multicast Tree (Hinzufügen oder Entfernen der Verzweigungen des Tree)

- Ein Multicast-Tree kann mit einer der beiden Methoden erstellt und verwaltet werden: **implizite Joins (Flood-and-Prune)** oder **explizite Joins (Pull-Modell)**. Der PIM Dense Mode (PIM-DM) verwendet implizite Joins, während der PIM Sparse Mode (PIM-SM) explizite Joins verwendet.
- Eine Multicast-Struktur kann entweder **gemeinsam genutzt** oder **quellenbasiert sein**:
 - Gemeinsam genutzte Trees verwenden das Konzept des **Rendezvous Point (RP)** und werden als **(* ,G)** gekennzeichnet, wobei G = Multicast-Gruppen-IP ist.
 - Source-basierte Trees basieren auf der Quelle, verwenden keinen RP und werden als **(S, G)** gekennzeichnet, wobei S für die IP der Multicast-Quelle bzw. des Multicast-Servers steht.
- Multicast-Weiterleitungsmodelle:
 - **Der Any-Source Multicast (ASM)-Bereitstellungsmodus** verwendet Shared Trees (*, G), über die jede Quelle den Multicast-Stream senden kann.
 - **Source-Specific Multicast (SSM)** verwendet Source-basierte Trees (S, G) und den IP-Bereich 232/8.
 - **Bidirektionaler (BiDir)** ist ein Shared Tree (*,G), in dem sowohl der Steuerungs- als auch der Datenverkehr über den RP läuft.
- Ein Rendezvous Point kann mit einer der folgenden Methoden konfiguriert oder ausgewählt werden:
 - Statische RP
 - Auto-RP
 - Bootstrap-Router (BSR)

Zusammenfassung der PIM-Modi

PIM-Modus	RP	Gemeinsam genutzte Struktur	Anmerkung	IGMP	Unterstützung von ASA/FTD

PIM Sparse Mode	Ja	Ja	(* , G) und (S, G)	v1/v2/v3	Ja
PIM Dense Mode	Nein	Nein	(S, G)	v1/v2/v3	Nein*
Bidirektionaler PIM-Modus	Ja	Ja	(* ,G)	v1/v2/v3	Ja
PIM Source-Specific-Multicast (SSM)-Modus	Nein	Nein	(S, G)	V3	Nein* *

* Auto-RP = Auto-RP-Verkehr kann passieren

** ASA/FTD kann kein Last-Hop-Gerät sein

RP-Konfigurationsübersicht

Rendezvous-Point-Konfiguration	ASA/FTD
Statische RP	Ja
Auto-RP	Nein, aber der Auto-RP-Verkehr auf der Steuerungsebene kann passieren.
BSR	Ja, aber keine C-RP-Unterstützung

Hinweis: Bevor Sie mit der Fehlerbehebung für Probleme mit Multicast beginnen, ist es sehr wichtig, eine klare Sicht auf die Multicast-Topologie zu haben. Sie müssen mindestens Folgendes wissen:

- Welche Rolle spielt die Firewall in der Multicast-Topologie?
- Wer ist der RP?
- Wer ist der Absender des Multicast-Streams (Quell-IP und Multicast-Gruppen-IP)?
- Wer ist der Empfänger des Multicast-Streams?
- Bestehen Probleme mit der Kontrollebene (IGMP/PIM) oder der Datenebene (Multicast-Stream)?

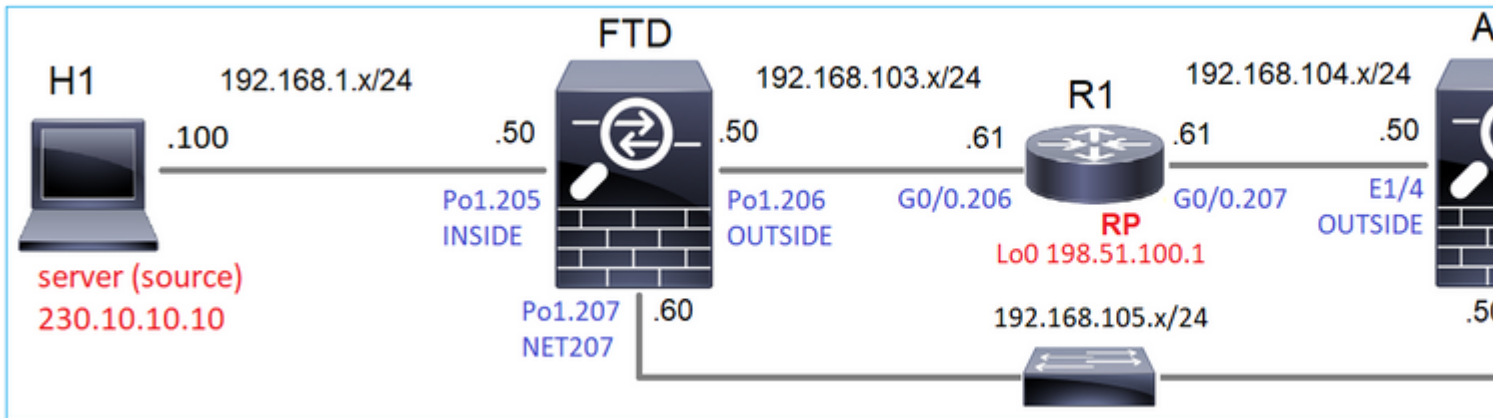
Abkürzungen/Akronyme

Abkürzungen	Erläuterung
FHR	First-Hop-Router - ein Hop, der direkt mit der Quelle des Multicast-

	Verkehrs verbunden ist.
LHR	Last-Hop-Router - ein Hop, der direkt mit den Empfängern des Multicast-Verkehrs verbunden ist.
RP	Rendezvous-Point
DR	Designierter Router
SPT	Baum mit dem kürzesten Pfad
RPT	Rendezvous-Point (RP)-Struktur, Shared-Tree
RP	Umgekehrte Pfadweiterleitung
ÖL	Liste der ausgehenden Schnittstellen
MRIB	Multicast Routing Information Base
MFIB	Multicast Forwarding Information Base
ASM	Quellenunabhängiges Multicast
BSR	Bootstrap-Router
SSM	Source-Specific Multicast
FP	Schneller Pfad
SP	Langsamer Pfad
CP	Kontrollpunkt
PPS	Paketrate pro Sekunde

Aufgabe 1: PIM Sparse Mode (statischer RP)

Topologie



Konfigurieren Sie den Multicast-PIM Sparse-Mode in der Topologie mit R1 (198.51.100.1) als RP.

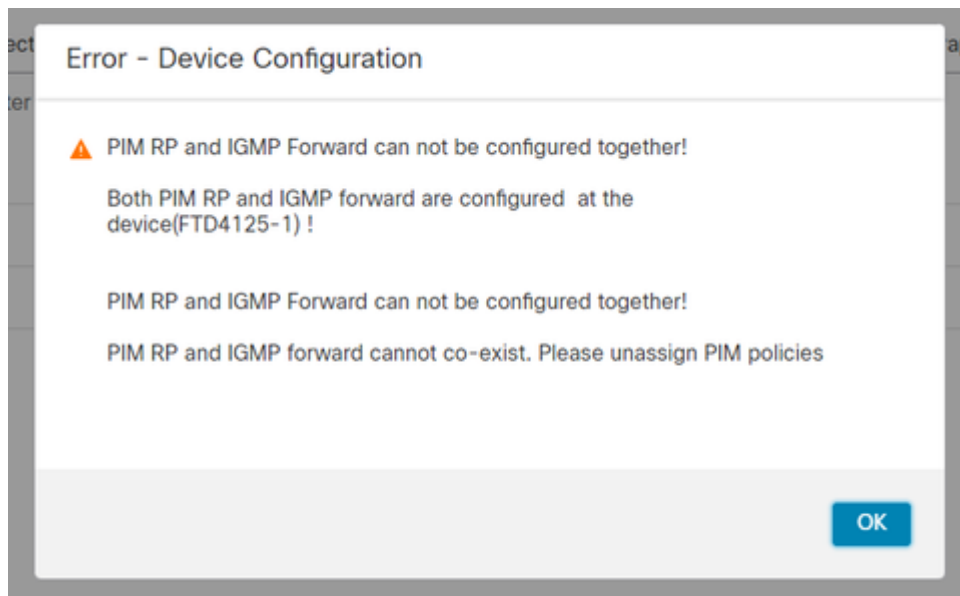
Lösung

FTD-Konfiguration:

The screenshot shows the configuration interface for FTD4125-1 in the Firewall Management Center. The 'Routing' tab is active, and the 'Multicast Routing' section is expanded to show 'PIM' configuration.

- Manage Virtual Routers:** The 'PIM' option is selected in the left sidebar.
- Global Settings:** Two checkboxes are checked and highlighted with orange boxes:
 - Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on a...
 - Generate older IOS compatible register messages(enable if your Rendezvous Point is an IOS router)
- Add Rendezvous Point Dialog:** A dialog box is open with the following settings:
 - Rendezvous Point IP address:*** RP_198.51.100.1 (highlighted with an orange box)
 - Use bi-directional forwarding
 - Use this RP for all Multicast Groups (highlighted with an orange box)
 - Use this RP for all Multicast Groups and below
 - Standard Access List:*** (empty)

ASA/FTD kann nicht gleichzeitig für IGMP-Stub-Routing und PIM konfiguriert werden:



Die resultierende Konfiguration auf FTD:

```
<#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
```

Auf der ASA-Firewall gibt es eine ähnliche Konfiguration:

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

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

RP-Konfiguration (Cisco Router):

```
<#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
```

Verifizierung

Überprüfen Sie die Multicast-Kontrollebene auf FTD, wenn kein Multicast-Verkehr vorhanden ist (Sender oder Empfänger):

```
<#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

```
<-- PIM enabled on the interface. There is 1 PIM neighbor
```

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

Überprüfen Sie die PIM-Nachbarn:

```
<#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)	

Der RP kündigt den gesamten Multicast-Gruppenbereich an:

```
<#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

Die Firewall-Routing-Tabelle enthält einige nicht relevante Einträge (239.255.255.250 ist das Simple Service Discovery Protocol (SSDP), das von Anbietern wie MAC OS und Microsoft Windows verwendet wird):

```
<#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
```

Zwischen den Firewalls und dem RP ist ein PIM-Tunnel aufgebaut:

```
<#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
```

Der PIM-Tunnel ist auch in der Firewall-Verbindungstabelle zu sehen:

```
<#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
```

Verifizierung auf der ASA-Firewall:

```
<#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-Verifizierung (Cisco Router). Es gibt einige Multicast-Gruppen für SSDP und Auto-RP:

```
<#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
```

Überprüfung, sobald ein Empfänger seine Anwesenheit bekannt gibt

Hinweis: Die in diesem Abschnitt aufgeführten Firewall-Befehle gelten uneingeschränkt für ASA und FTD.

Die ASA erhält die IGMP-Mitgliedschaftsbericht-Meldung und erstellt die IGMP- und mroute-Einträge (*,G):

```
<#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 repor

Die ASA-Firewall erstellt eine Route für die Multicast-Gruppe:

```
<#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
```

Eine weitere Firewall-Verifizierung ist die Ausgabe der PIM-Topologie:

```
<#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
```

Hinweis: Wenn die Firewall keine Route zum RP hat, zeigt die **debug-pim**-Ausgabe einen Fehler bei der RPF-Suche an.

Fehler bei der RPF-Suche in der **Debug-PIM**-Ausgabe:

```
<#root>
```

```
asa#
```

```
debug pim
```

```
IPv4 PIM: RPF lookup failed for root 198.51.100.1
```

```
<-- The RPF look fails because the
```

```
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
```

Wenn alles in Ordnung ist, sendet die Firewall eine PIM Join-Prune-Nachricht an den RP:

```
<#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
```

Die Erfassung zeigt, dass die PIM Join-Nachrichten alle 1 Minute und PIM Hellos alle 30 Sekunden gesendet werden. PIM verwendet IP 224.0.0.13:

(ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)

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

> 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

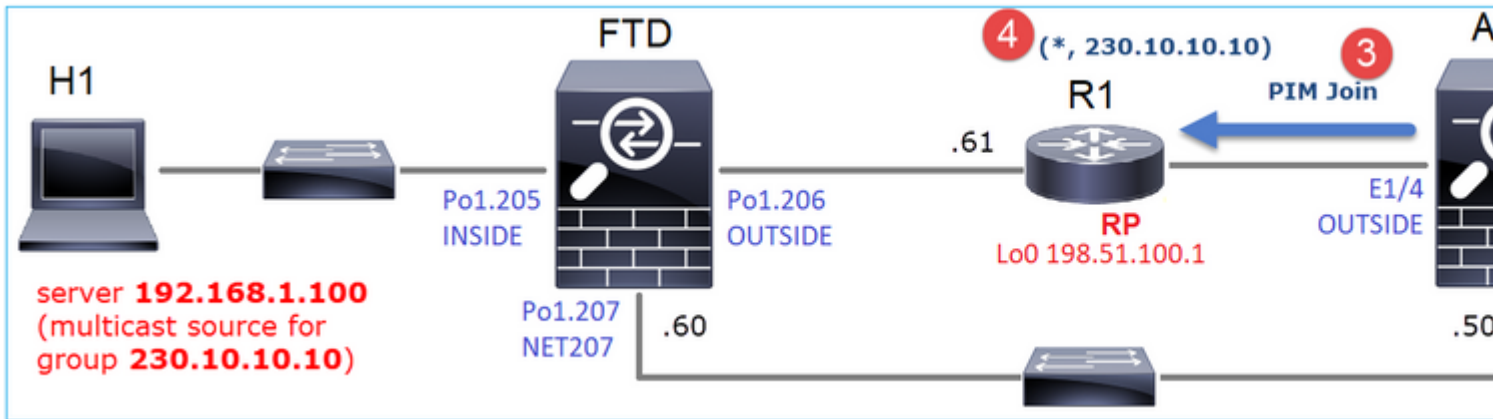
- Tip:** Wireshark display filter: (ip.src==192.168.104.50 && ip.dst==224.0.0.13) && (pim.group == 230.10.10.10)
- 192.168.104.50 ist die Firewall-IP der Ausgangsschnittstelle (zum Upstream-PIM-Nachbarn).
 - 224.0.0.13 ist die PIM-Multicast-Gruppe, an die PIM Joins und Prunes gesendet werden.
 - 230.10.10.10 ist die Multicast-Gruppe, für die wir PIM Join/Prune senden.

Der RP erstellt eine (*,G)-Route. Da noch keine Server vorhanden sind, ist die Eingangsschnittstelle Null:

```
<#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
```

Dies kann wie folgt visualisiert werden:



1. Der IGMP-Bericht wird auf der ASA empfangen.
2. Eine (*,G)-Route wird hinzugefügt.
3. Die ASA sendet eine PIM Join-Nachricht an den RP (198.51.100.1).
4. Der RP empfängt die Join-Nachricht und fügt eine (*,G)-Route hinzu.

Gleichzeitig gibt es auf FTD keine Routen, da es weder einen IGMP-Bericht noch eine PIM-Teilnahme gab:

```
<#root>
firepower#
show mroute 230.10.10.10
No mroute entries found.
```

Überprüfen, wenn der Server einen Multicast-Stream sendet

Der FTD erhält den Multicast-Stream von H1 und startet den **PIM-Registrierungsprozess** mit dem RP. Der FTD sendet eine **Unicast-PIM-Registernachricht** an den RP. Der RP sendet eine **PIM-Join-Nachricht** an den First-Hop-Router (FHR), in diesem Fall den FTD, um dem Multicast-Tree beizutreten. Dann wird eine **Register-Stopp-Nachricht** gesendet.

```
<#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 FTD

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)
```

Die PIM Register-Nachricht ist eine PIM-Nachricht, die UDP-Daten zusammen mit den PIM Register-Informationen enthält:

Filter: pim.type in {1 2}

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group
23	15.829623	0.000015	192.168.1.100	230.10.10.10	PIMv2	0x9802 (38914)...	1402	
24	15.829623	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9902 (39170)...	1402	
25	15.829653	0.000030	192.168.1.100	230.10.10.10	PIMv2	0x9a02 (39426)...	1402	
26	15.829653	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9b02 (39682)...	1402	
27	15.833224	0.003571	198.51.100.1	192.168.103.50	PIMv2	0x107c (4220)	56	230.10.10
28	15.833468	0.000244	198.51.100.1	192.168.103.50	PIMv2	0x107d (4221)	56	230.10.10
29	15.833681	0.000213	198.51.100.1	192.168.103.50	PIMv2	0x107e (4222)	56	230.10.10
30	15.833910	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x107f (4223)	56	230.10.10
31	15.834109	0.000199	198.51.100.1	192.168.103.50	PIMv2	0x1080 (4224)	56	230.10.10
32	15.836092	0.001983	198.51.100.1	192.168.103.50	PIMv2	0x108f (4239)	56	230.10.10
33	15.836306	0.000214	198.51.100.1	192.168.103.50	PIMv2	0x1090 (4240)	56	230.10.10
34	15.836535	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x1091 (4241)	56	230.10.10

> 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
 > Protocol Independent Multicast
 0010 = Version: 2
 ... 0001 = Type: Register (1)
 Reserved byte(s): 00
 > Checksum: 0x966a incorrect, should be 0xdefeff
 [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)

Die PIM Register-Stopp-Meldung:

Filter: pim.type in {1 2}

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group
23	15.829623	0.000015	192.168.1.100	230.10.10.10	PIMv2	0x9802 (38914)...	1402	
24	15.829623	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9902 (39170)...	1402	
25	15.829653	0.000030	192.168.1.100	230.10.10.10	PIMv2	0x9a02 (39426)...	1402	
26	15.829653	0.000000	192.168.1.100	230.10.10.10	PIMv2	0x9b02 (39682)...	1402	
27	15.833224	0.003571	198.51.100.1	192.168.103.50	PIMv2	0x107c (4220)	56	230.10.10
28	15.833468	0.000244	198.51.100.1	192.168.103.50	PIMv2	0x107d (4221)	56	230.10.10
29	15.833681	0.000213	198.51.100.1	192.168.103.50	PIMv2	0x107e (4222)	56	230.10.10
30	15.833910	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x107f (4223)	56	230.10.10
31	15.834109	0.000199	198.51.100.1	192.168.103.50	PIMv2	0x1080 (4224)	56	230.10.10
32	15.836092	0.001983	198.51.100.1	192.168.103.50	PIMv2	0x108f (4239)	56	230.10.10
33	15.836306	0.000214	198.51.100.1	192.168.103.50	PIMv2	0x1090 (4240)	56	230.10.10
34	15.836535	0.000229	198.51.100.1	192.168.103.50	PIMv2	0x1091 (4241)	56	230.10.10

> 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
 > Protocol Independent Multicast
 0010 = Version: 2
 ... 0010 = Type: Register-stop (2)
 Reserved byte(s): 00
 Checksum: 0x29be [correct]
 [Checksum Status: Good]
 > PIM Options

Tipp: Um nur PIM-Register- und PIM-Register-Stopp-Nachrichten in Wireshark anzuzeigen, können Sie den Anzeigefilter pim.type in {1 2} verwenden.

Die Firewall (Last-Hop-Router) empfängt den Multicast-Stream an der Schnittstelle OUTSIDE und initiiert den SPT-Switchover (Shortest Path Tree) zur Schnittstelle NET207:

```
<#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)
```

PIM-Debugging auf dem FTD bei Switchover:

```
<#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
```

FTD-Route nach dem Start des SPT-Switchovers:

```
<#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
```

Am Ende des SPT-Switchovers wird nur die NET207-Schnittstelle im OIL von FTD angezeigt:

```
<#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
```

Auf dem Last-Hop-Router (ASA) ist das SPT-Bit ebenfalls festgelegt:

```
<#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
```

Der Switchover über die ASA NET207-Schnittstelle (der First-Hop-Router, der den Switchover durchgeführt hat) Eine PIM-Join-Nachricht wird an das Upstream-Gerät (FTD) gesendet:

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

No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group
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
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
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
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

> 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

Protocol Independent Multicast

- 0010 = Version: 2
- 0011 = Type: Join/Prune (3)
- Reserved byte(s): 00
- Checksum: 0xf8e4 [correct]
- [Checksum Status: Good]
- > PIM Options
 - > Upstream-neighbor: 192.168.105.60
 - Reserved byte(s): 00
 - Num Groups: 1
 - Holdtime: 210
 - Group 0
 - > Group 0: 230.10.10.10/32
 - Num Joins: 1
 - > IP address: 192.168.1.100/32 (S)
 - Num Prunes: 0

Auf der OUTSIDE-Schnittstelle wird eine PIM Prune-Nachricht an den RP gesendet, um den Multicast-Stream zu stoppen:

(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
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
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
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

> 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

Protocol Independent Multicast

- 0010 = Version: 2
- 0011 = Type: Join/Prune (3)
- Reserved byte(s): 00
- Checksum: 0xf8e3 [correct]
- [Checksum Status: Good]
- > PIM Options
 - > Upstream-neighbor: 192.168.104.61
 - Reserved byte(s): 00
 - Num Groups: 1
 - Holdtime: 210
 - Group 0
 - > Group 0: 230.10.10.10/32
 - Num Joins: 0
 - Num Prunes: 1
 - > IP address: 192.168.1.100/32 (SR)

Verifizierung des PIM-Verkehrs:

<#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	

So überprüfen Sie die Anzahl der Pakete, die unter Slow Path vs Fast Path vs Control Point verarbeitet werden:

<#root>

firepower#

show asp cluster counter

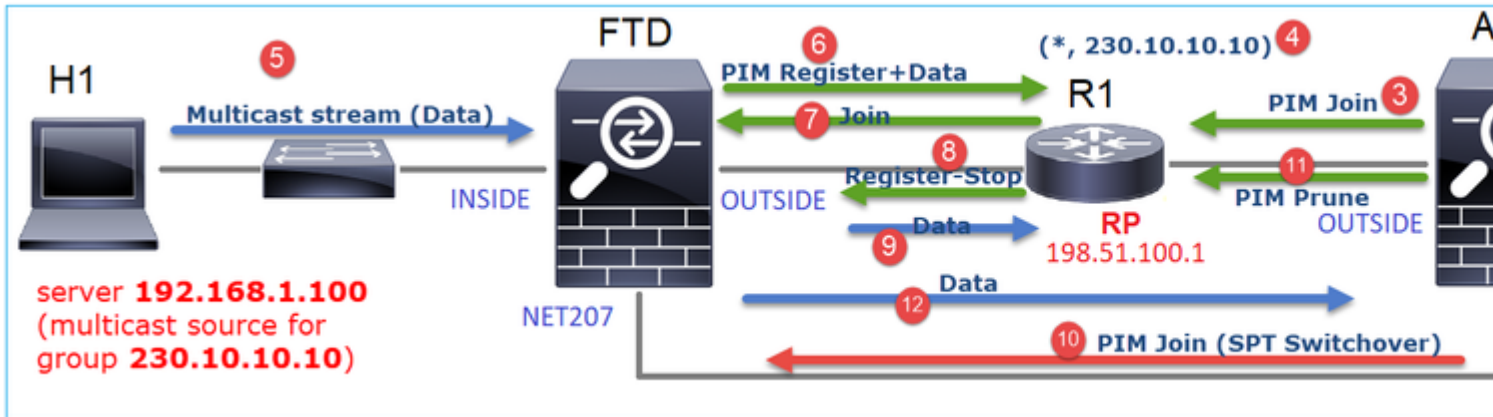
Global dp-counters:

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 inter
MCAST_FP_CHK_FAIL_NO_SEQ_NO_MATCH	131	Number of multicast packets failed with no matched sequ
MCAST_FP_CHK_FAIL_NO_FP_FWD	313584	Number of multicast packets that cannot be fast-path fo
MCAST_FP_UPD_FOR_UNMATCH_IFC	91	Number of times that multicast flow's ifc_out cannot be

Ein Diagramm, das Schritt für Schritt zeigt, was passiert:



1. Der End-Host (H2) sendet einen IGMP-Bericht, um dem Multicast-Stream 230.10.10.10 beizutreten.
2. Der Last-Hop-Router (ASA), also der PIM DR, erstellt einen (*, 230.10.10.10)-Eintrag.
3. Die ASA sendet eine PIM Join-Nachricht an den RP für die Gruppe 230.10.10.10.
4. Der RP erstellt den (*, 230.10.10.10)-Eintrag.
5. Der Server sendet die Multicast-Stream-Daten.
6. Die FTD kapselt die Multicast-Pakete in PIM-Registernachrichten und sendet sie (Unicast) an den RP. An diesem Punkt erkennt der RP, dass er über einen aktiven Empfänger verfügt, entkapselt die Multicast-Pakete und sendet sie an den Empfänger.
7. Der RP sendet eine PIM-Join-Nachricht an den FTD, um dem Multicast-Tree beizutreten.
8. Der RP sendet eine PIM Register-Stopp-Nachricht an den FTD.
9. Die FTD sendet einen nativen Multicast-Stream (keine PIM-Kapselung) an den RP.
10. Der Last-Hop-Router (ASA) stellt fest, dass die Quelle (192.168.1.100) einen besseren Pfad von der NET207-Schnittstelle aufweist, und startet einen Switchover. Es sendet eine PIM Join-Nachricht an das Upstream-Gerät (FTD).
11. Der Last-Hop-Router sendet eine PIM Prune-Nachricht an den RP.
12. Der FTD leitet den Multicast-Stream an die NET207-Schnittstelle weiter. Die ASA wird vom Shared Tree (RP-Tree) zum Source Tree (SPT) verschoben.

Aufgabe 2: Konfigurieren des PIM-Bootstrap-Routers (BSR)

BSR-Grundlagen

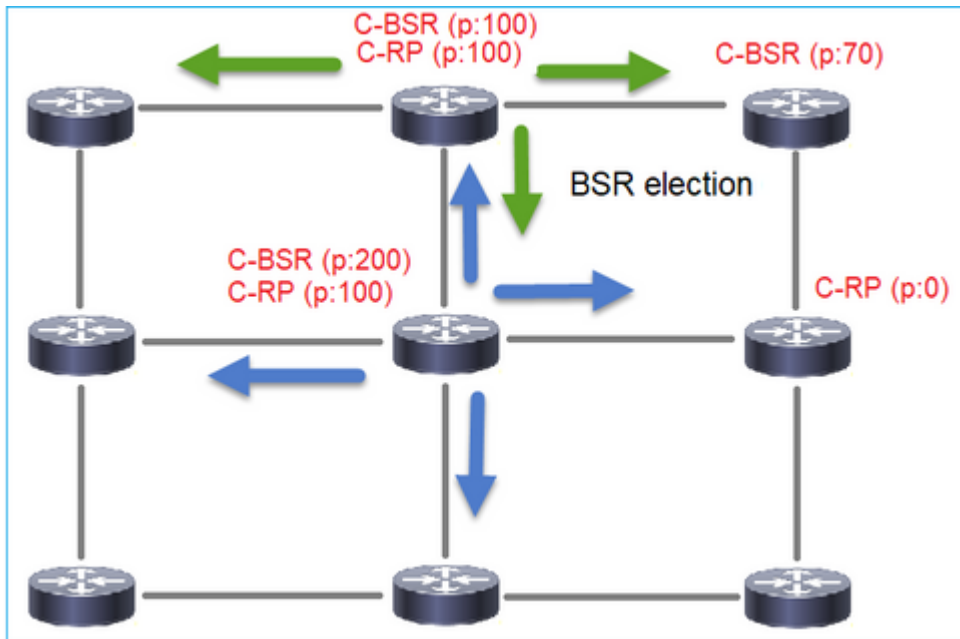
- BSR (RFC 5059) ist ein Multicast-Mechanismus auf Kontrollebene, der das PIM-Protokoll verwendet und es Geräten ermöglicht, die RP-Informationen dynamisch abzurufen.
- BSR-Definitionen:
 - Candidate RP (C-RP) (RP für Kandidaten): Ein Gerät, das ein RP sein möchte.
 - BSR-Kandidat (C-BSR): Ein Gerät, das ein BSR sein will und anderen Geräten RP-Sets ankündigt.
 - BSR: Ein Gerät, das von vielen C-BSRs als BSR gewählt wird. Die **höchste BSR-Priorität gewinnt** die Wahl.
 - RP-Set: Eine Liste aller C-RPs und ihrer Prioritäten.
 - RP: Das Gerät mit der **niedrigsten RP-Priorität gewinnt** die Wahl.
 - BSR-PIM-Nachricht (leer): Eine PIM-Nachricht, die bei der BSR-Wahl verwendet wird.

- BSR-PIM-Nachricht (normal): Eine PIM-Nachricht, die an 224.0.0.13 IP gesendet wird und einen RP-Satz und BSR-Informationen enthält.

Wie BSR funktioniert

1. Wahlmechanismus der BSR.

Jeder C-BSR sendet leere PIM BSR-Nachrichten mit einer Priorität. Das Gerät mit der höchsten Priorität (Fallback ist die höchste IP-Adresse) gewinnt die Wahl und wird zum BSR. Die übrigen Geräte senden keine leeren BSR-Nachrichten mehr.



Eine BSR-Nachricht, die im Wahlprozess verwendet wird, enthält nur C-BSR-Prioritätsinformationen:

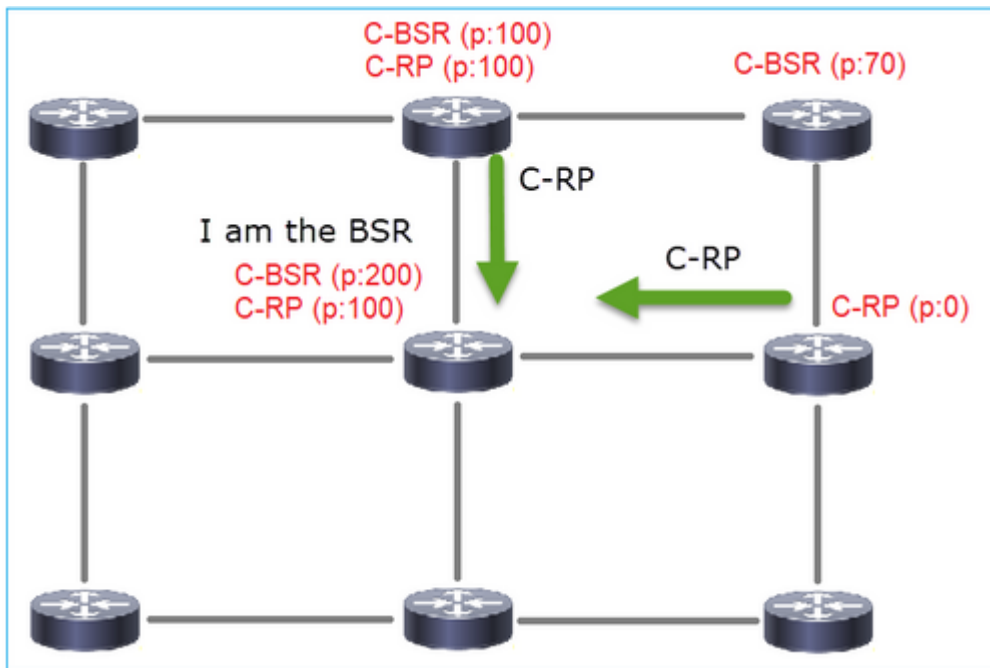
No.	Time	Delta	Source	Destination	Protocol	Identification	Length	Group	Info
2	6.437401	0.000000	192.168.103.50	224.0.0.13	PIMv2	0x2740 (10048)	52		Bootstrap
8	66.643725	60.206324	192.168.103.50	224.0.0.13	PIMv2	0x1559 (5465)	52		Bootstrap
13	126.850014	60.206289	192.168.103.50	224.0.0.13	PIMv2	0x0d32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

Um BSR-Nachrichten in Wireshark anzuzeigen, verwenden Sie diesen Anzeigefilter: pim.type == 4

2. Die C-RPs senden **Unicast**-BSR-Nachrichten an den BSR, die ihre C-RP-Priorität enthalten:



Eine RP-Kandidatennachricht:

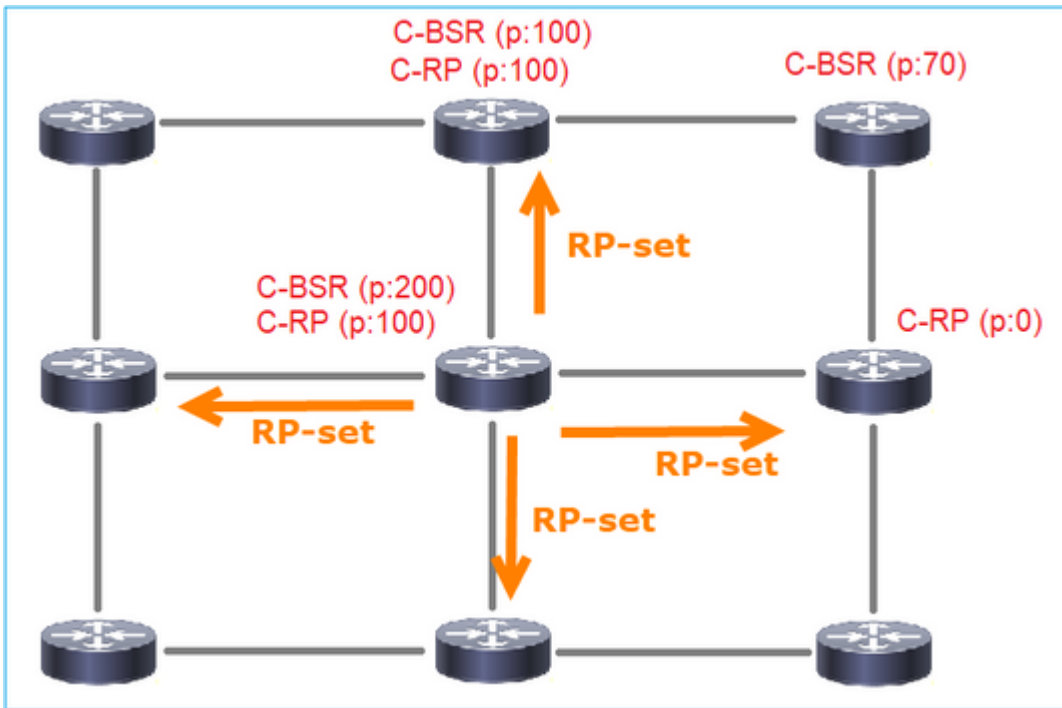
```

pim.type == 8
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: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
v Protocol Independent Multicast
  0010 .... = Version: 2
  ... 1000 = Type: Candidate-RP-Advertisement (8)
  Reserved byte(s): 00
  Checksum: 0x3263 [correct]
  [Checksum Status: Good]
  v PIM Options
    Prefix-count: 1
    Priority: 0
    Holdtime: 150
    v RP: 192.0.2.1
      Address Family: IPv4 (1)
      Encoding Type: Native (0)
      Unicast: 192.0.2.1
    v Group 0: 224.0.0.0/4
      Address Family: IPv4 (1)
      Encoding Type: Native (0)
  > Flags: 0x00
  Masklen: 4
  Group: 224.0.0.0
  
```

Um BSR-Nachrichten in Wireshark anzuzeigen, verwenden Sie diesen Anzeigefilter: `pim.type == 8`

3. Der BSR stellt den RP-Satz zusammen und kündigt ihn allen PIM-Nachbarn an:

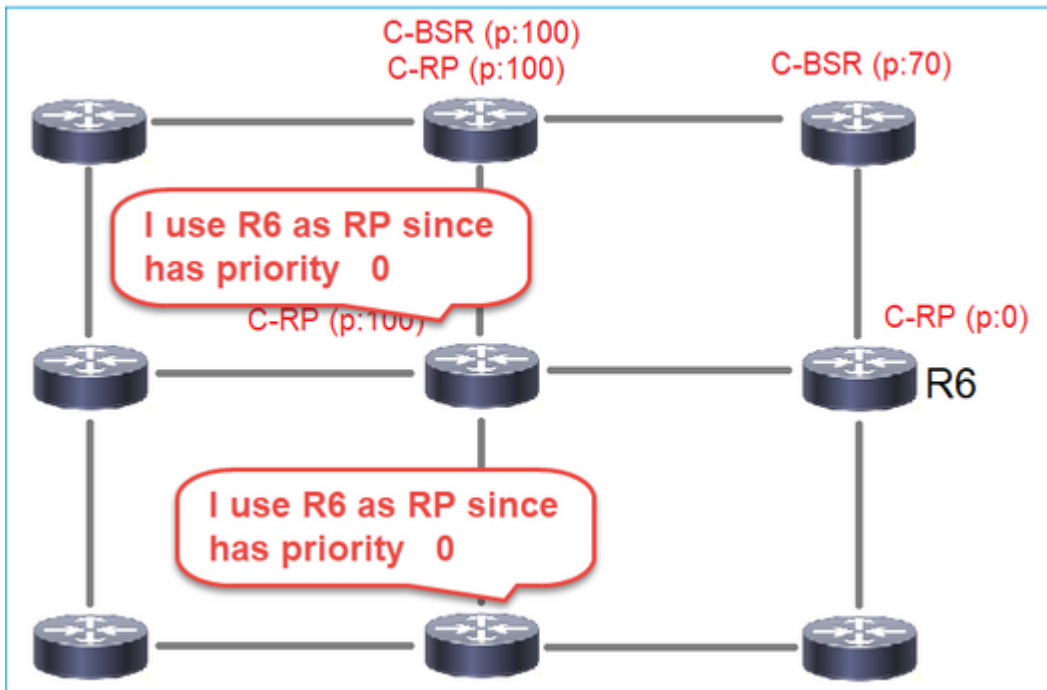


```

(ip.src == 192.168.105.60) && (pim.type == 4)
No.    Time          Delta           Source          Destination     Protocol  Identification  Length  Group
-----
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
<
> 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
v Protocol Independent Multicast
  0010 .... = Version: 2
  .... 0100 = Type: Bootstrap (4)
  Reserved byte(s): 00
  Checksum: 0x264f [correct]
  [Checksum Status: Good]
  v PIM Options
    Fragment tag: 0x2412
    Hash mask len: 0
    BSR priority: 100
  > BSR: 192.0.2.2
  v 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

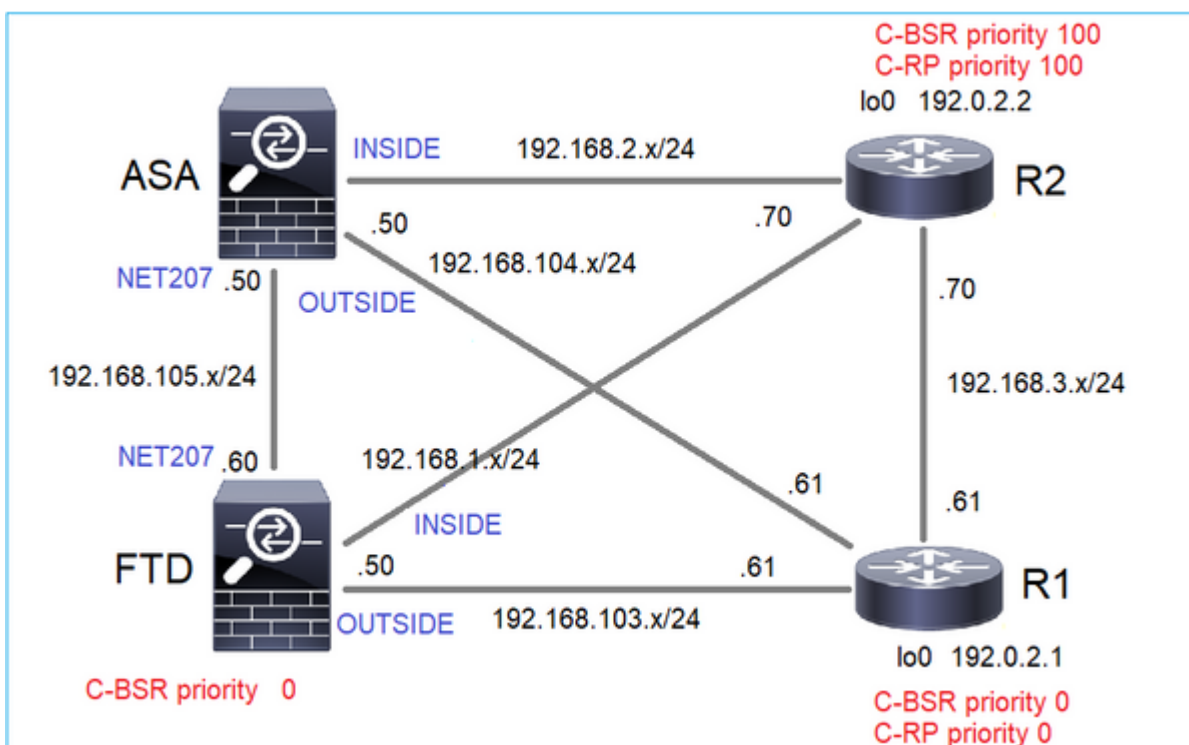
```

4. Die Router/Firewalls erhalten den RP-Satz und wählen den RP basierend auf der niedrigsten Priorität aus:



Voraussetzung für diese Aufgabe

Konfigurieren Sie die C-BSRs und C-RPs gemäß dieser Topologie:



Für diese Aufgabe muss sich die FTD als C-BSR auf der OUTSIDE-Schnittstelle mit BSR-Priorität 0 ankündigen.

Lösung

FMC-Konfiguration für FTD:

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 **Bo**

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	

Die bereitgestellte Konfiguration:

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

Konfiguration auf den anderen Geräten:

```
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)
```

Identisch mit R2, jedoch mit unterschiedlichen C-BSR- und C-RP-Prioritäten

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

Auf ASA ist nur Multicast global aktiviert. Dadurch wird PIM auf allen Schnittstellen aktiviert:

```
multicast-routing
```

Verifizierung

R2 ist aufgrund der höchsten Priorität der gewählte BSR:

```
<#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 wird aufgrund der niedrigsten Priorität als RP ausgewählt:

```
<#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
```

Die BSR-Meldungen **werden einer RPF-Prüfung unterzogen**. Sie können **debug pim bsr** aktivieren, um dies zu überprüfen:

```
<#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/
```

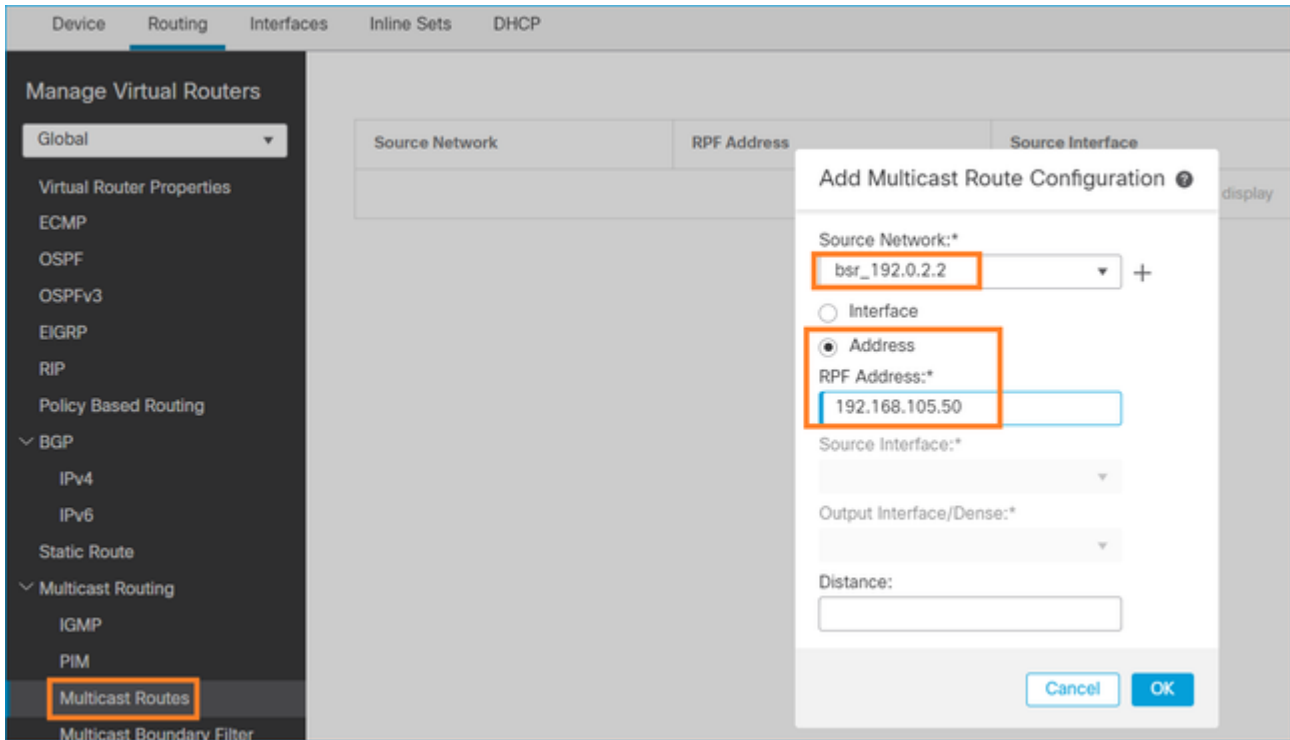
```
NET207
```

```
for 192.0.2.2
```

```
RPF failed, dropped
```

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

Wenn Sie die RPF-Schnittstelle ändern möchten, können Sie eine statische Route konfigurieren. In diesem Beispiel akzeptiert die Firewall BSR-Nachrichten von IP 192.168.105.50:



```
<#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
```

Jetzt werden BSR-Meldungen auf der NET207-Schnittstelle akzeptiert, aber auf INSIDE verworfen:

```
<#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
```

Aktivieren Sie die Erfassung mit Trace auf der Firewall, und überprüfen Sie, wie die BSR-Nachrichten verarbeitet werden:

```
<#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
```

Die PIM-Verbindungen werden an der Firewall terminiert. Damit die Ablaufverfolgung nützliche Informationen anzeigen kann, müssen die Verbindungen in der Box gelöscht werden:

```
<#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

Wenn das PIM-Paket aufgrund eines RPF-Fehlers verworfen wird, zeigt die Ablaufverfolgung Folgendes an:

```
<#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

Die ASP-Tabelle verwirft und erfasst Pakete mit RPF-Fehlern:

```
<#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

So erfassen Sie Pakete, die aufgrund eines RPF-Fehlers verworfen wurden:

```
<#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
```

Methodik der Fehlerbehebung

Die Methode zur Fehlerbehebung für die Firewall hängt hauptsächlich von der Rolle der Firewall in der Multicast-Topologie ab. Dies ist die Liste der empfohlenen Schritte zur Fehlerbehebung:

1. Klären Sie die Details der Problembeschreibung und Symptome. Versuchen Sie, den Bereich auf die Probleme mit der **Kontrollebene (IGMP/PIM)** oder der **Datenebene (Multicast-Stream)** zu beschränken.
2. Die obligatorische Voraussetzung für die Behebung von Multicast-Problemen auf der Firewall ist die Klärung der Multicast-Topologie. Sie müssen mindestens Folgendes identifizieren:
 - Rolle der Firewall in der Multicast-Topologie - FHR, LHR, RP oder eine andere zwischengeschaltete Rolle.
 - Eingangs- und Ausgangsschnittstellen für Multicast auf der Firewall erwartet.
 - Ank.
 - IP-Adressen der Absenderquelle.
 - Multicast fasst IP-Adressen und Ziel-Ports zusammen.
 - Empfänger des Multicast-Streams.
3. Identifizieren Sie die Art des Multicast-Routings - **Stub-** oder **PIM-Multicast-Routing**:
 - **Stub-Multicast-Routing**: Es ermöglicht die dynamische Host-Registrierung und vereinfacht das Multicast-Routing. Bei Konfiguration für Stub-Multicast-Routing fungiert die ASA als IGMP-Proxy-Agent. Anstatt vollständig am Multicast-Routing teilzunehmen, leitet die ASA IGMP-Nachrichten an einen Upstream-Multicast-Router weiter, der die Übermittlung der Multicast-Daten übernimmt. Um das Routing im Stub-Modus zu identifizieren, verwenden Sie den Befehl **show igmp interface**, und überprüfen Sie die IGMP-Weiterleitungskonfiguration:

```
<#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)
```

PIM ist an den Schnittstellen aktiviert, es besteht jedoch keine Nachbarschaft:

```
<#root>
firepower#
show pim interface

Address          Interface          PIM  Nbr   Hello  DR      DR
                  Count Intvl  Prior
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 und IGMP-Weiterleitung werden **nicht** gleichzeitig unterstützt.

Sie können keine Optionen wie die RP-Adresse konfigurieren:

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

- **PIM-Multicast-Routing - Das PIM-Multicast-Routing ist die häufigste Bereitstellung.** Die Firewall unterstützt PIM-SM und bidirektionales PIM. PIM-SM ist ein Multicast-Routing-Protokoll, das die zugrunde liegende Unicast-Routing-Informationsbasis oder eine separate Multicast-fähige Routing-Informationsbasis verwendet. Er erstellt einen unidirektionalen Shared Tree, dessen Ursprung bei einem einzelnen Rendezvous Point (RP) pro Multicast-Gruppe liegt, und erstellt optional Shortest-Path Trees pro Multicast-Quelle. In diesem Bereitstellungsmodus konfigurieren die Benutzer im Gegensatz zum Stub-Modus in der Regel die RP-Adresskonfiguration, und die Firewall richtet PIM-Nachbarschaften mit den Peers ein:

```
<#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. Überprüfen Sie, ob die RP-IP-Adresse konfiguriert ist und ob Sie erreichbar sind:

```
<#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) <--- â€œusâ€œ
224.0.0.0/4     SM     static  0      0.0.0.0         RPF: ,0.0.0.0

```

Warnung: Bei der Firewall kann es sich nicht gleichzeitig um einen **RP** und einen **FHR handeln**.

5. Überprüfen Sie die zusätzlichen Ausgaben je nach der Rolle der Firewall in der Multicast-Topologie und den Problemsymptomen.

FHR

- Überprüfen Sie den Status der Schnittstelle **Tunnel0**. Diese Schnittstelle wird zum Kapseln des unformatierten Multicast-Verkehrs in die PIM-Nutzlast und zum Senden des Unicast-Pakets an den RP für mit dem PIM-Register-Bitsatz verwendet:

```
<#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

- Routen überprüfen:

```
<#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.
```

Wenn die Firewall ein PIM-Paket mit dem Register-Stopp-Bit empfängt, wird Tunnel0 aus dem OIL entfernt. Die Firewall stoppt dann die Kapselung und sendet rohen Multicast-Verkehr über die Ausgangsschnittstelle:

```
<#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-Registerzähler überprüfen:

```
<#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

```

- Überprüfen Sie die PIM-Paketerfassung für Unicast zwischen der Firewall und dem RP:

```
<#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

```

- Erfassen Sie zusätzliche Ausgaben (x.x.x.x steht für die Multicast-Gruppe, y.y.y für die RP-IP). Es wird empfohlen, die Ergebnisse **mehrmals** zu sammeln:

```
<#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
```

- Sammeln von Multicast-Rohschnittstellenpaketen und ASP-Verlusterfassungen

```
<#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 U
```

- Syslog-Meldungen - allgemeine IDs: 302015, 302016 und 710005.

RP

- Überprüfen Sie den Status der Schnittstelle Tunnel0. Diese Schnittstelle wird zum Kapseln des unformatierten Multicast-Verkehrs innerhalb der PIM-Nutzlast und zum Senden des Unicast-Pakets an die FHR mit dem PIM-Stopp-Bit-Satz verwendet:

```
<#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	-

- Routen überprüfen:

```
<#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-Zähler überprüfen:

<#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

- Erfassen Sie zusätzliche Ausgaben (x.x.x.x steht für die Multicast-Gruppe, y.y.y für die RP-IP). Es wird empfohlen, die Ergebnisse **mehrmals** zu sammeln:

```
<#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
```

- Sammeln von unformatierten Multicast-Schnittstellenpaketen und ASP-Drop-Erfassungen:

```
<#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 - allgemeine IDs: 302015, 302016 und 710005.

LHR

Berücksichtigen Sie die Schritte, die im Abschnitt für den RP beschrieben werden, sowie die folgenden zusätzlichen Prüfungen:

- Routen:

<#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-Gruppen:

<#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-Datenverkehrsstatistiken:

<#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	

Befehle zur PIM-Fehlerbehebung (Kurzreferenz)

Command	Beschreibung
show running-config multicast-routing	So prüfen Sie, ob Multicast-Routing auf der Firewall aktiviert ist:
Ausführungs-mroute	So zeigen Sie die auf der Firewall konfigurierten statischen Routen an
show running-config pim	So zeigen Sie die PIM-Konfiguration auf der Firewall an
show pim interface	Anzeigen, für welche Firewall-Schnittstellen PIM aktiviert ist und für welche PIM-Nachbarn.
show pim neighbor	PIM-Nachbarn anzeigen
PIM-Gruppenkarte anzeigen	So zeigen Sie die dem RP zugeordneten Multicast-Gruppen an
mroute anzeigen	So zeigen Sie die vollständige Multicast-Routing-Tabelle an
show mroute 230.10.10.10	So zeigen Sie die Multicast-Tabelle für eine bestimmte Multicast-Gruppe an
PIM-Tunnel anzeigen	Um festzustellen, ob zwischen der Firewall und dem RP ein PIM-

	Tunnel erstellt wurde
show conn all detail-Adresse RP_IP_ADDRESS	Um festzustellen, ob eine Verbindung (PIM-Tunnel) zwischen der Firewall und dem RP besteht
PIM-Topologie anzeigen	So zeigen Sie die Ausgabe der Firewall-PIM-Topologie an
Debug-PIM	Dieser Debugger zeigt alle PIM-Nachrichten von und zur Firewall an.
debug pim-Gruppe 230.10.10.10	Bei diesem Debugging werden alle PIM-Nachrichten von und zur Firewall für die jeweilige Multicast-Gruppe angezeigt.
PIM-Verkehr anzeigen	So zeigen Sie Statistiken über empfangene und gesendete PIM-Nachrichten an
ASP-Cluster-Zähler anzeigen	So überprüfen Sie die Anzahl der Pakete, die im Vergleich zu "Slow Path" und "Fast Path" und "Control Point" verarbeitet werden
asp drop anzeigen	So zeigen Sie alle Software-Level-Drops auf der Firewall an
capture CAP-Schnittstelle INSIDE trace match pim any any	So erfassen und verfolgen Sie eingehende PIM-Multicast-Pakete auf der Firewall
capture CAP interface INSIDE trace match udp host 224.1.2.3 any	So erfassen und verfolgen Sie den eingehenden Multicast-Stream
show pim bsr-router	So überprüfen Sie, wer der ausgewählte BSR-Router ist
show conn all address 224.1.2.3	So zeigen Sie die übergeordnete Multicast-Verbindung an
show local-host 224,1.2.3	So zeigen Sie untergeordnete/Stub-Multicast-Verbindungen an

Weitere Informationen zu Firewall-Erfassungen finden Sie unter [Arbeiten mit Firepower Threat Defense-Erfassungen und Packet Tracer](#).

Bekannte Probleme

FirePOWER-Multicast-Einschränkungen:

- IPv6 wird nicht unterstützt.
- PIM/IGMP-Multicast wird an Schnittstellen in einer Verkehrszone (EMCP) nicht unterstützt.
- Die Firewall darf nicht gleichzeitig ein RP und ein FHR sein.
- Der Befehl **show conn all** zeigt nur die Multicast-Identitätsverbindungen an. Um die Stub/Secondary Multicast-Verbindung anzuzeigen, verwenden Sie den Befehl **show local-host <group IP>**.

PIM wird auf einem vPC-Nexus nicht unterstützt

Wenn Sie versuchen, eine PIM-Adjacency zwischen einem Nexus vPC und der Firewall bereitzustellen, gelten für Nexus die folgenden Einschränkungen:

[Unterstützte Topologien für das Routing über Virtual Port Channel auf Nexus-Plattformen](#)

Aus Sicht der NGFW sehen Sie in der Aufzeichnung mit Trace diesen Dropdown:

```
<#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
```

Die Firewall kann die RP-Registrierung nicht abschließen:

```
<#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:

Tunnel0, Forward, 00:39:15/never

Zielzonen werden nicht unterstützt

Sie können keine Zielsicherheitszone für die Zugriffssteuerungsrichtlinienregel angeben, die mit Multicast-Verkehr übereinstimmt:

Firewall Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects Integration

FTD_Access_Control_Policy
Enter Description

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Pre

Filter by Device Search Rules

Misconfiguration! The Dest Zones must be empty!

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

There are no rules in this section. [Add Rule](#) or [Add Category](#)

Dies wird auch im FMC-Benutzerhandbuch dokumentiert:

Book Contents Find Matches in This Book

Book Title Page

- Getting Started with Device Configuration
- Device Operations
- Interfaces and Device Settings
- Routing
 - Static and Default Routes
 - Virtual Routers
 - ECMP
 - OSPF
 - BGP
 - RIP
 - Multicast**
 - Policy Based Routing

Internet multicast routing from address range 224.0.0/24 is not supported; IGMP g... multicast routing for the reserved addressess.

Clustering

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

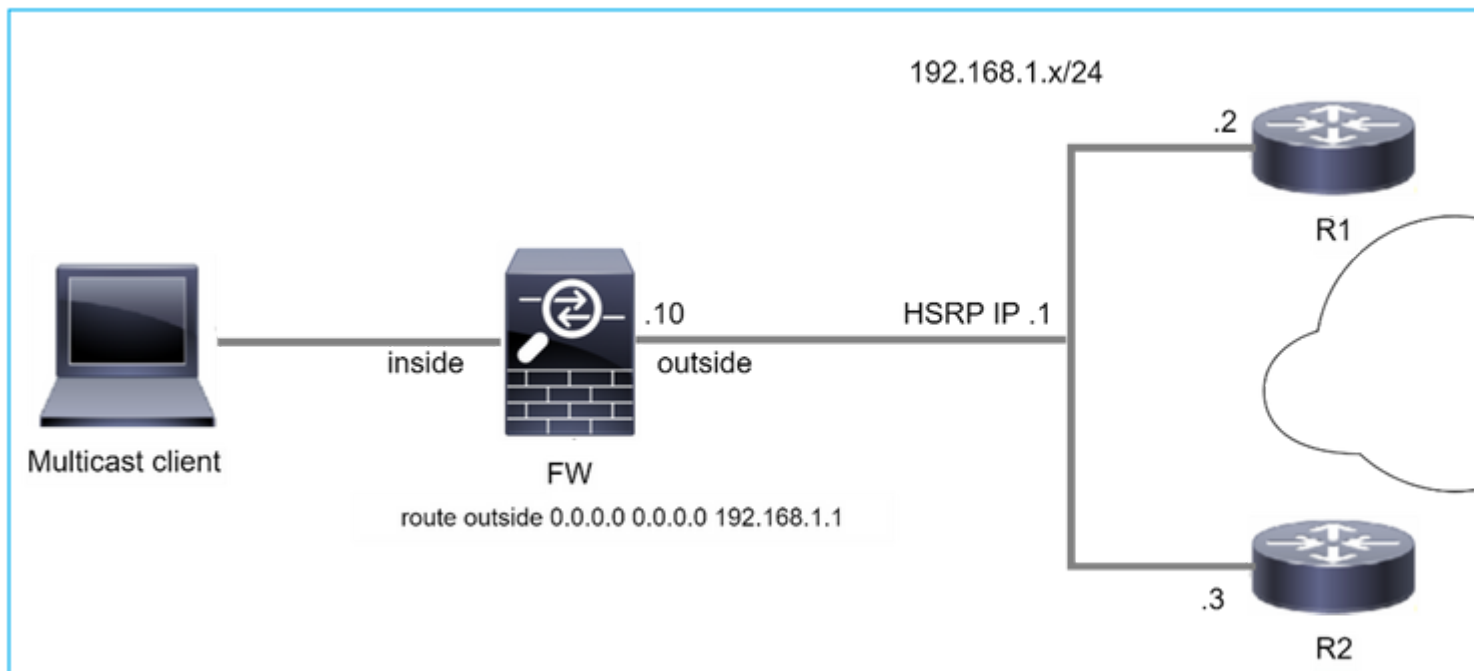
Additional Guidelines

- You must configure an access control or prefilter rule on the inbound security zone such as 224.1.2.3. However, you cannot specify a destination security zone for t multicast connections during initial connection validation.
- You cannot disable an interface with PIM configured on it. If you have configured **PIM Protocol**), disabling the multicast routing and PIM does not remove the PIM 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

Configure IGMP Features

IP hosts use IGMP to report their group memberships to directly-connected multica register individual hosts in a multicast group on a particular LAN. Hosts identify gro

Firewall sendet aufgrund von HSRP keine PIM-Nachrichten an Upstream-Router



In diesem Fall hat die Firewall eine Standardroute über das Hot Standby Redundancy Protocol (HSRP) IP 192.168.1.1 und die PIM-Nachbarschaft mit den Routern R1 und R2:

```
<#root>
firepower#
show run route
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

Die Firewall verfügt über eine PIM-Adjacency zwischen der Außenseite und der physischen Schnittstelle IP auf R1 und R2:

```
<#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)	

Die Firewall sendet keine PIM-Join-Nachricht an das Upstream-Netzwerk. Der PIM-Debug-Befehl **debug pim** zeigt folgende Ausgabe an:

```
<#root>
```

```
firepower#
```

```
debug pim
```

```
...
```

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

[RFC 2362](#) besagt, dass "ein Router eine periodische Join/Prune-Nachricht an jeden einzelnen RPF-Nachbarn sendet, der jedem (S,G)-, (*,G)- und (*,*,RP)-Eintrag zugeordnet ist. Join/Prune-Nachrichten werden nur gesendet, wenn der RPF-Nachbar ein PIM-Nachbar ist."

Um das Problem zu beheben, kann der Benutzer der Firewall einen statischen Routeneintrag hinzufügen. Der Router muss auf eine der beiden IP-Adressen für die Router-Schnittstelle verweisen, nämlich 192.168.1.2 oder 192.168.1.3, in der Regel die IP des aktiven HSRP-Routers.

Beispiel:

```
<#root>
```

```
firepower#
```

```
show run mroute
```

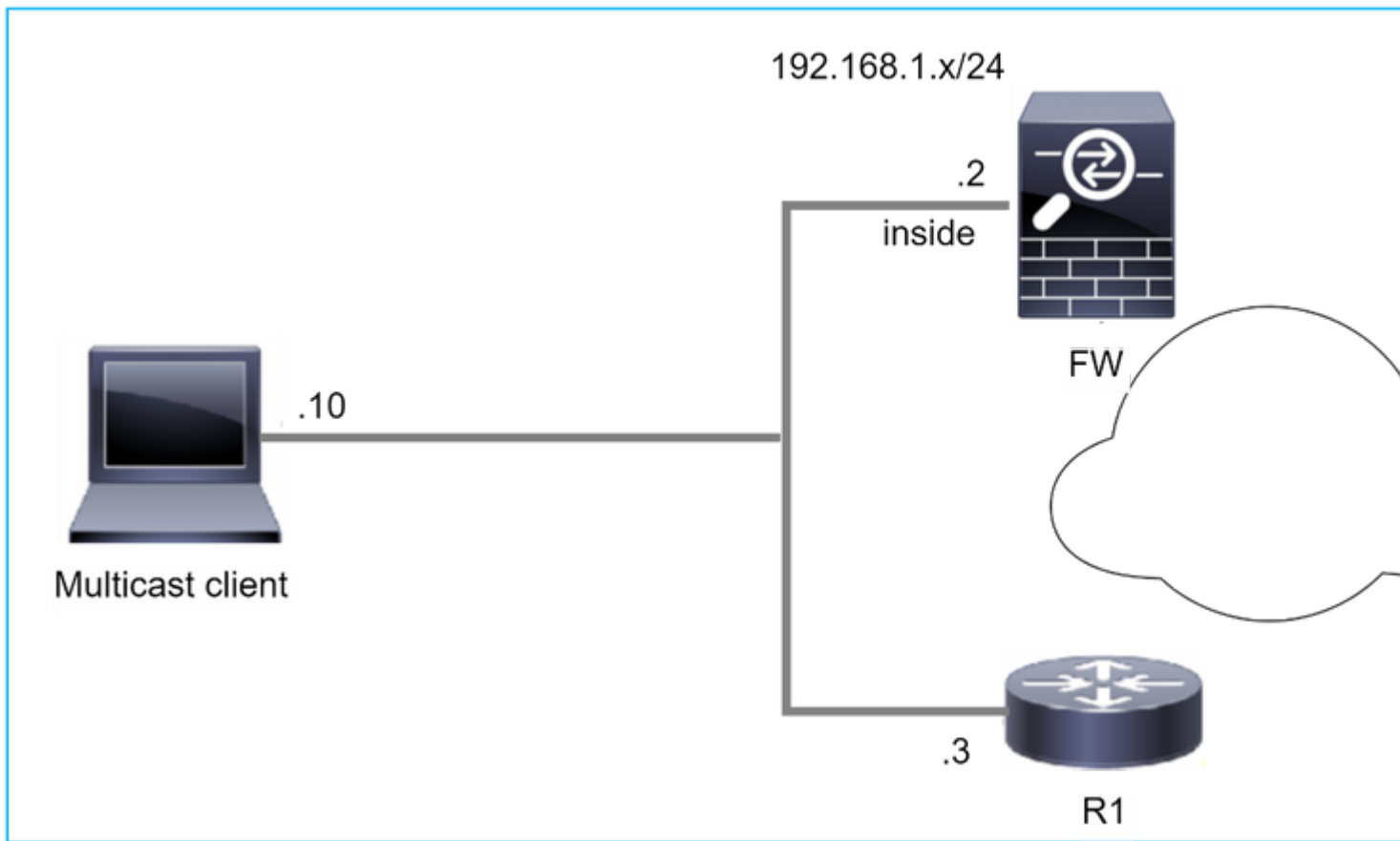
```
firepower#
```

```
mroute 172.16.1.1 255.255.255.255 192.168.1.2
```

Sobald die statische Routenkonfiguration für die RPF-Suche eingerichtet ist, legt die Firewall den Schwerpunkt auf die Multicast-Routing-Tabelle anstelle der Unicast-Routing-Tabelle der ASA und sendet die PIM-Nachrichten direkt an den Nachbarn 192.168.1.2.

Hinweis: Die statische Routing-Funktion macht in gewisser Hinsicht den Nutzen der HSRP-Redundanz zunichte, da die Route nur einen Next-Hop pro Adresse/Netzmaske-Kombination akzeptiert. Wenn der im Befehl mroute angegebene nächste Hop ausfällt oder nicht erreichbar ist, greift die Firewall nicht auf den anderen Router zurück.

Die Firewall wird nicht als LHR betrachtet, wenn sie nicht der DR im LAN-Segment ist.



Die Firewall hat R1 als PIM-Nachbarn im LAN-Segment. R1 ist der PIM DR:

```
<#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)	

Wenn eine IGMP-Bitrittsanfrage vom Client eingeht, wird die Firewall nicht zum LHR.

Die Route zeigt zusätzlich **Null** als OIL an und hat das Flag **Pruned**:

```
<#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
```

Um die Firewall zur LHR zu machen, kann die Priorität der Schnittstelle DR erhöht werden.

```
<#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		

Der PIM-Debug-Befehl **debug pim** zeigt folgende Ausgabe an:

```
<#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
```

Das Flag 'Abgeschnitten' und der Nullwert werden aus der mroute entfernt:

```
<#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
```

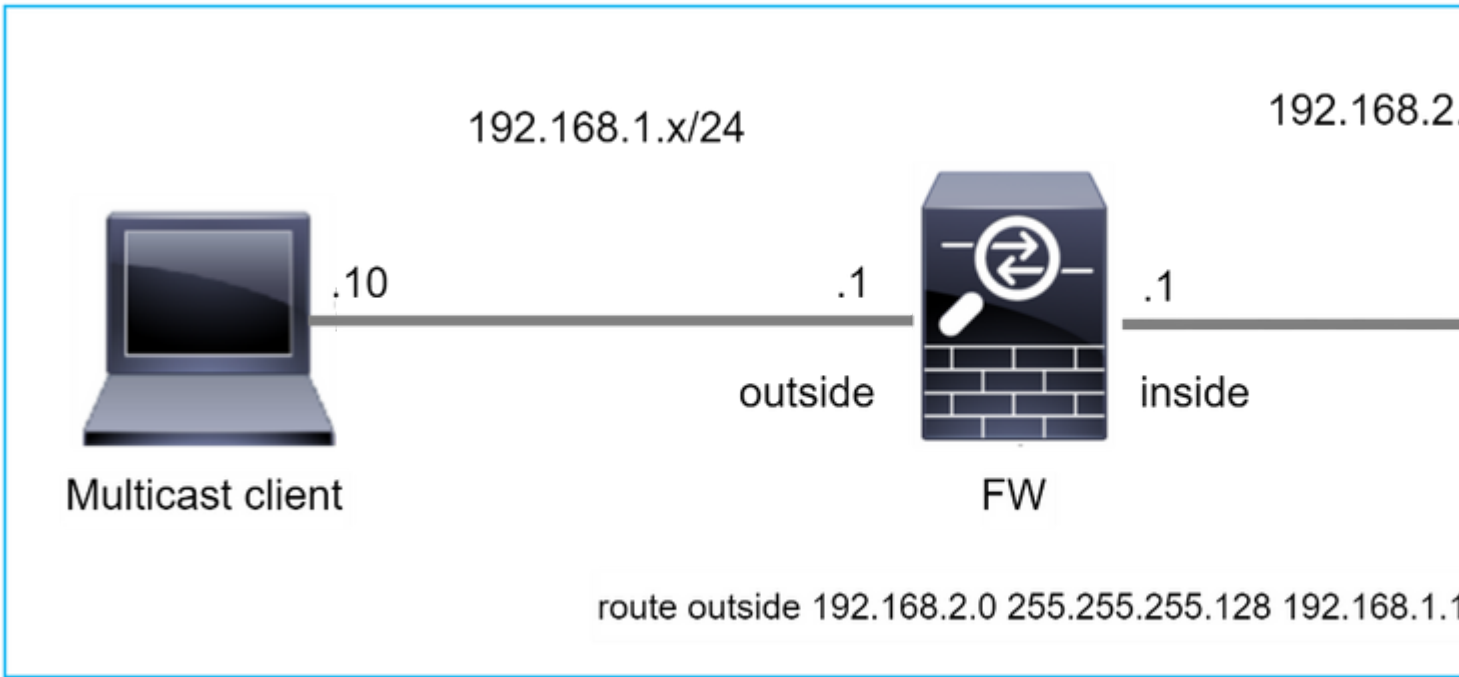
```
  Incoming interface: Null
```

```
  RPF nbr: 0.0.0.0
```

```
  Immediate Outgoing interface list:
```

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

Die Firewall lässt Multicast-Pakete aufgrund eines Fehlers bei der Überprüfung der Umkehrpfad-Weiterleitung verloren



In diesem Fall werden die Multicast-UDP-Pakete aufgrund eines RPF-Fehlers verworfen, da die Firewall über die externe Schnittstelle eine spezifischere Route mit der Maske 255.255.255.128 hat.

```
<#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-Drop-Captures zeigen den Grund für **das** Verwerfen von **RPF-Angriffen** an:

<#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 Path Forwarding (RPF) check failed
2: 09:00:53.708032      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Reverse Path Forwarding (RPF) check failed
3: 09:00:53.812152      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Reverse Path Forwarding (RPF) check failed
4: 09:00:53.908613      192.168.2.2.12345 > 230.1.1.1.12354:  udp 500 Drop-reason: (rpf-violated) Reverse Path Forwarding (RPF) check failed
```

Die RPF-Fehlerindikatoren in der MFIB-Ausgabe erhöhen sich wie folgt:

```
<#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
```

Die Lösung besteht darin, den Fehler bei der RPF-Prüfung zu beheben. Eine Option besteht darin, die statische Route zu entfernen.

Wenn keine RPF-Prüfung mehr fehlschlägt, werden die Pakete weitergeleitet, und der **Weiterleitungszähler** in der MFIB-Ausgabe erhöht sich:

<#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,

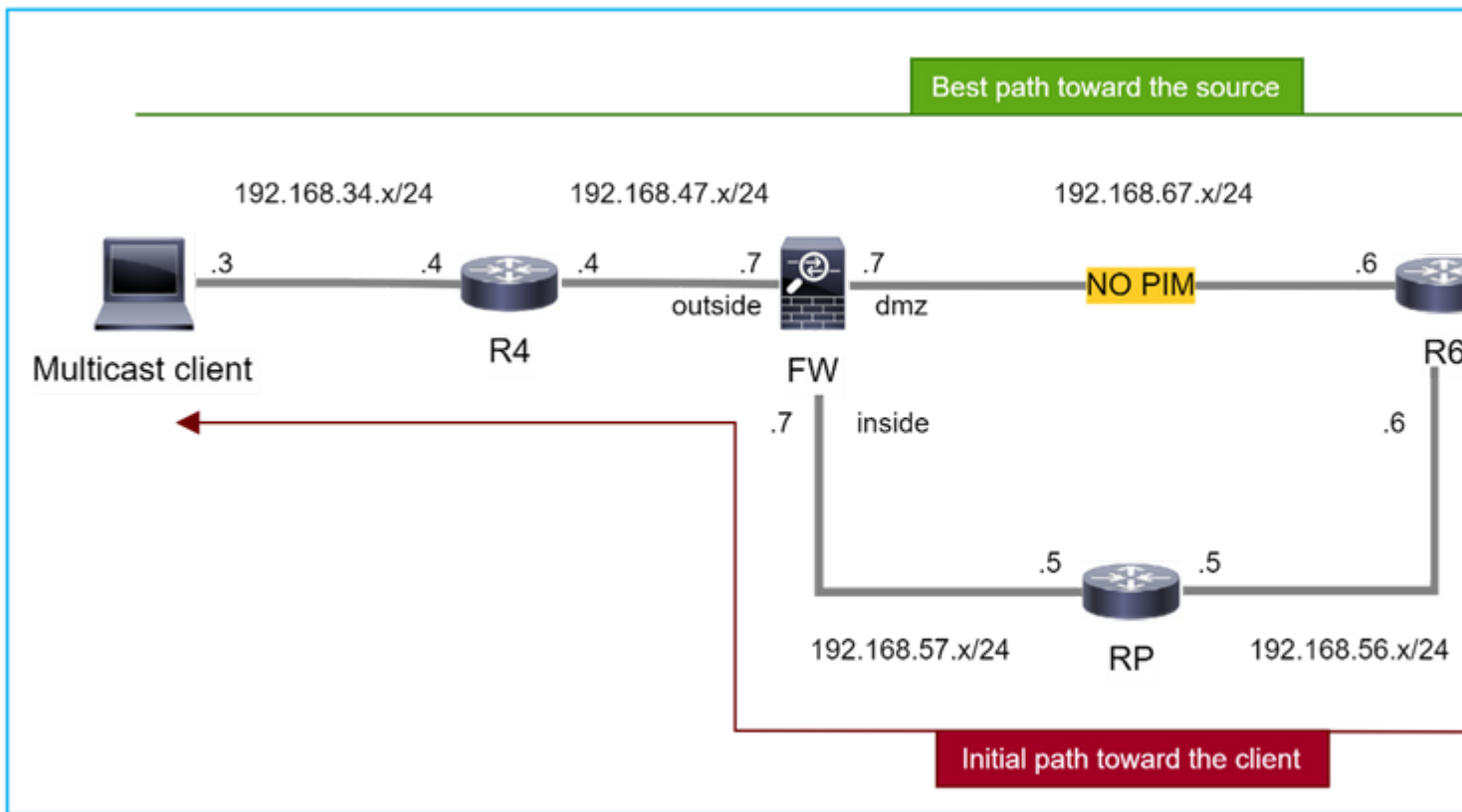
Forwarding: 1044/10/528/41

, Other: 0/0/0

<--- Forward counter increased

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

Firewall generiert beim PIM-Switchover zum Source-Tree keinen PIM-Join



In diesem Fall erkennt die Firewall den Pfad zur Multicast-Quelle über die **DMZ-Schnittstelle R4 > FW > R6**, während der ursprüngliche Datenverkehrspfad von der Quelle zum Client **R6 > RP > DW > R4** ist:

```
<#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 initiiert den SPT-Switchover und sendet eine quellspezifische PIM-Join-Nachricht, sobald der SPT-Switchover-Grenzwert erreicht ist. In der Firewall findet der SPT-Switchover nicht statt, die (S,G)-Route verfügt nicht über das **T-Flag**:


```
<#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
```

Der PIM-Debug-Befehl **debug pim** zeigt 2 empfangene PIM-Join-Anforderungen vom Peer R4 an - für **(* ,G) und (S,G)**. Die Firewall hat eine PIM-Join-Anforderung für (* ,G) Upstream gesendet und konnte aufgrund des ungültigen Nachbarn 192.168.67.6 keine quellspezifische Anforderung senden:

```
<#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

Die Ausgabe der Befehle **show pim neighbour** enthält kein R6:

<#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	

PIM ist auf der Firewall-Schnittstelle dmz aktiviert:

<#root>

firepower#

show pim interface

Address	Interface	PIM	Nbr Count	Hello Intvl	DR Prior	DR
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

PIM ist auf der R6-Schnittstelle deaktiviert:

```
<#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
```

Die Lösung besteht in der Aktivierung von PIM an der GigabitEthernet0/3-Schnittstelle auf R6:

```
<#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
```

Die Firewall installiert das T-Flag, das einen SPT-Switchover anzeigt.:

```
<#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
```

Firewall verwirft die ersten paar Pakete aufgrund von Punt-Rate Limit

Wenn die Firewall die ersten Pakete eines **neuen** Multicast-Streams in FP empfängt, kann eine zusätzliche Verarbeitung durch den CP erforderlich sein. In diesem Fall sendet das FP die Pakete über SP an den CP (FP > SP > CP), um weitere Vorgänge auszuführen:

- Erstellung einer **übergeordneten** Verbindung im FP zwischen den Eingangsschnittstellen und den Identitätsschnittstellen.
- Zusätzliche Multicast-spezifische Prüfungen, z. B. die RPF-Validierung, die PIM-Kapselung (falls es sich bei der Firewall um die FHR handelt), die OIL-Prüfung usw.
- Erstellen eines (S,G)-Eintrags mit den ein- und ausgehenden Schnittstellen in der mroute-Tabelle.
- Erstellung einer **untergeordneten/Stub**-Verbindung im FP zwischen den eingehenden und ausgehenden Schnittstellen.

Als Teil des Schutzes der Kontrollebene begrenzt die Firewall intern die Paketrage, die an den CP gesendet wird.

Pakete, die die Übertragungsrage überschreiten, werden in der mit dem Grund **für das** Verwerfen der **Durchsatzratenbegrenzung verworfen**:

```
<#root>
```

```
firepower#
```

```
show asp drop
```

Frame drop:

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

Verwenden Sie den Befehl **show asp cluster counter**, um die Anzahl der Multicast-Pakete zu überprüfen, die vom SP an den CP gesendet werden:

```
<#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

Verwenden Sie den Befehl **show asp event dp-cp punt**, um die Anzahl der Pakete in der FP > CP-Warteschlange und die Rate von 15 Sekunden zu überprüfen:

```
<#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

```

Wenn die Route aufgefüllt wird und die übergeordneten/untergeordneten Verbindungen im FP eingerichtet werden, werden die Pakete im FP als Teil der bestehenden Verbindungen weitergeleitet. In diesem Fall werden die Pakete von FP nicht an den CP gesendet.

Wie verarbeitet die Firewall die ersten Pakete eines neuen Multicast-Streams?

Wenn die Firewall die ersten Pakete eines **neuen** Multicast-Streams in datapath empfängt, führt sie die folgenden Aktionen aus:

1. Überprüft, ob die Sicherheitsrichtlinien Pakete zulassen.
2. Versendet Pakete über Pfad FP an den CP.
3. Erstellt eine **übergeordnete** Verbindung zwischen den Eingangsschnittstellen und den Identitätsschnittstellen:

```
<#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

Syslogs:

```
<#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)
```

Diese Verbindung wird in der Ausgabe des Befehls **show conn all** angezeigt:

```
<#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 0
```

4. Der CP aktiviert den Multicast-Prozess für zusätzliche Multicast-spezifische Prüfungen, z. B. die RPF-Validierung, die PIM-Kapselung (falls es sich bei der Firewall um die FHR handelt), die ÖL-Prüfung usw.
5. Der CP erstellt einen (S,G)-Eintrag mit den eingehenden und ausgehenden Schnittstellen in der Route:

```
<#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. Der CP weist den FP über den Pfad CP > SP > FP an, eine **untergeordnete/Stub**-Verbindung zwischen den eingehenden und ausgehenden Schnittstellen zu erstellen:

Diese Verbindung ist nur in der Ausgabe des Befehls **show local-host** sichtbar:

```
<#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
```

In den Softwareversionen mit der Cisco Bug-ID [CSCwe21280](#) wird auch die Syslog-Meldung 302015 für die untergeordnete Verbindung/Stub-Verbindung generiert:

```
<#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
```

Wenn sowohl über- als auch untergeordnete/Stub-Verbindungen hergestellt werden, stimmen die eingehenden Pakete mit der vorhandenen Verbindung überein und werden in FP:

```
<#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-Multicast-Datenverkehr filtern

Sie können ICMP-Multicast-Datenverkehr nicht mit einer ACL filtern. Sie müssen Control Plane Policy (ICMP) verwenden:

Cisco Bug-ID [CSCs126860](#) ASA filtert Multicast-ICMP-Pakete nicht

Bekannte PIM-Multicast-Fehler

Sie können das Bug Search Tool für bekannte Fehler verwenden: <https://bst.cloudapps.cisco.com/bugsearch>

Die meisten ASA- und FTD-Fehler sind unter dem Produkt "Cisco Adaptive Security Appliance (ASA) Software" aufgeführt:

Bug Search Tool

Search For

PIM 1


Product

Series/Model

Cisco Adaptive Security Appliance (ASA) Software 2

Release

Affecting or Fixed in Releases

 Save Search

 Email Search

Clear

The results

Filters

Clear Filters

Severity

Show All

Status

Show All

94 Results | Sorted by Severity

Sort By: Show

[CSCsy08778 no pim on one subif disables eigrp on same physical of 4](#)

Symptom: eigrp stops working on one subinterface, if "no pim" is issued on another subinterf same physical interface. **Conditions:** The physical interface belongs to the 4-GE module. If us

Severity: 2 | Status: Fixed | Updated: Nov 09, 2016 | Cases:3 | ★ ★ ★ ★ ★

[CSCtg52478 PIM nbr jp_buffer can be corrupted under stress](#)

Symptom: memory corruption of pim nbr structure **Conditions:** multicast w/ PIM-SM and hea

Zugehörige Informationen

- [Fehlerbehebung und allgemeine Probleme mit ASA Multicast](#)
- [FirePOWER Management Center-Multicast](#)
- [Zusammenfassung der FirePOWER-Multicast-Flags](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.