Probleemoplossing voor Firepower Threat Defense IGMP en Multicast Basics

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren **IGMP-grondbeginselen** Taak 1 - Control-Plane Multicast-verkeer Taak 2 - Basis multicast configureren **IGMP-controle** Taak 3 - IGMP-statische groep vs IGMP-groep IGMP statische groep **IGMP-groep** Taak 4 - IGMP Stub Multicast-routing configureren Bekende problemen Filter multicast verkeer op doelzones IGMP-rapporten worden ontkend door de firewall wanneer de IGMP-interfacelimiet wordt overschreden Firewall negeert IGMP-rapporten voor het 232.x.x/8-adresbereik Gerelateerde informatie

Inleiding

Dit document beschrijft de basisbeginselen van multicast en hoe Firepower Threat Defence (FTD) het Internet Group Management Protocol (IGMP) implementeert.

Voorwaarden

Vereisten

Basiskennis over IP-routing.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

De inhoud van dit artikel is ook van toepassing op de software voor adaptieve security applicatie (ASA).

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

• Cisco Firepower 4125 Threat Defence versie 7.1.0.

- Firepower Management Center (FMC) versie 7.1.0.
- ASA versie 9.19.1.

Achtergrondinformatie

Definities

- Unicast = van één host naar een andere host (één-op-één).
- Uitzending = van één host naar ALLE mogelijke hosts (one-to-all).
- Multicast = van een host van een groep hosts naar een groep hosts (één-naar-veel of veel-naar-veel).
- Anycast = van een host naar de dichtstbijzijnde host van een groep (een-op-een-veel).

Grondbeginselen

- Multicast RFC 988 werd in 1986 geschreven door Steve Deering.
- IPv4-multicast gebruikt het bereik 224.0.0.0/4 (eerste 4-bits 110) 224.0.0.0 239.255.255.255.
- Voor IPv4 is het L2 MAC-adres afgeleid van L3 multicast IP: 01005e (24 bits) + 25th bit altijd 0 + 23 lagere bits van het multicast IPv4-adres.
- IPv6-multicast maakt gebruik van het bereik FF00::/8 en is flexibeler dan IPv4-multicast omdat hiermee Rendezvous Point (RP) IP kan worden ingesloten.
- Voor IPv6 is het L2 MAC-adres afgeleid van de L3 multicast: 3333 + 32 lagere bits van het multicast IPv6-adres.
- Multicastvoordelen: Efficiëntie door een lagere belasting op de bron. Prestaties, omdat het verkeer duplicatie of overstroming voorkomt.
- Multicastnadelen: onbetrouwbaar transport (op UDP gebaseerd), geen congestievermijding, levering na afloop van de sequentie.
- Multicast wordt niet ondersteund op het openbare internet omdat daarvoor alle apparaten op het pad nodig zijn. Meestal gebruikt wanneer alle apparaten onder een gemeenschappelijke administratieve autoriteit vallen.
- Typische Multicast-toepassingen: interne videostroom, videoconferentie.

Multicast versus gerepliceerde Unicast

In replicated Unicast maakt de bron meerdere kopieën van hetzelfde unicastpakket (replica's) en stuurt deze naar meerdere doelhosts. Multicast verplaatst de last van de bronhost naar het netwerk, terwijl in replicated Unicast al het werk wordt gedaan op de bronhost.

Configureren

IGMP-grondbeginselen

- IGMP is de 'taal' die wordt gesproken tussen de multicast-ontvangers en het lokale L3-apparaat (meestal een router).
- IGMP is een Layer 3-protocol (zoals ICMP) en gebruikt **IP-protocol nummer 2.**
- Er zijn momenteel 3 IGMP-versies. De standaard IGMP versie op de firewall is versie 2. **Op dit** moment worden alleen versie 1 en 2 ondersteund.
- Tussen IGMPv1 en IGMPv2 zijn de belangrijkste verschillen:
 - IGMPv1 heeft geen bericht van de Groep van het Verlof.
 - IGMPv1 heeft geen Group-Specific Query (gebruikt door de firewall wanneer een host een multicast groep verlaat).
 - IGMPv1 heeft geen snellere verkiezingsprocedure.

- **IGMPv3 wordt momenteel niet ondersteund** op ASA/FTD, maar als referentie is het belangrijke verschil tussen IGMPv2 en IGMPv3 de opname van een Group-and-Source-Specific Query in IGMPv3 die wordt gebruikt in Source-Specific Multicast (SSM).
- IGMPv1/IGMPv2/IGMPv3-vragen = **224.0.0.1** IGMPv2-verlof = **224.0.0.2** IGMPv3-lidmaatschapsrapport = **224.0.0.2**
- Als een host wil toetreden kan een ongevraagd IGMP Membership Report bericht verzenden:

l	<u>File</u> <u>E</u> dit	View Go Capture	Analyze Statistics Teleph	hony Wireless Tools	Help					
		🛛 🕺 🗋 📕	९ 🖛 🏓 🖀 Ŧ 🛓 📃	📃 Q Q Q 🎹						
ĺ	igmp									
	No.	Time	Delta	Source	Destination	Protocol	SGT Identi	ication	Length	Info
I		7 5.118518	0.000000	192.168.1.50	224.0.0.2	IGMPv2	0x01	a7 (423)	46	Leave Gro
I		8 5.127230	0.008712	192.168.1.50	230.10.10.10	IGMPv2	0x01	a8 (424)	46	Membersh:
		9 5.593022	0.465792	192.168.1.50	230.10.10.10	IGMPv2	0x01	a9 (425)	46	Membersh:
I		114 74.756894	69.163872	192.168.1.24	224.0.0.1	IGMPv2	0x72	80 (29312)	60	Membersh:
I		118 77.093155	2.336261	192.168.1.50	239.255.255.250	IGMPv2	0x01	e9 (489)	46	Membersh:
I		120 79.593298	2.500143	192.168.1.50	224.0.0.252	IGMPv2	0x01	eb (491)	46	Membersh:
I		122 81.093367	1.500069	192.168.1.50	230.10.10.10	IGMPv2	0x01	ec (492)	46	Membersh:
I		152 103.150111	22.056744	192.168.1.24	224.0.0.1	IGMPv2	0x10	5f (7263)	60	Membersh:
I		153 103.593643	0.443532	192.168.1.50	224.0.0.252	IGMPv2	0x02	06 (518)	46	Membersh:
I		154 104.593737	1.000094	192.168.1.50	239.255.255.250	IGMPv2	0x02	08 (520)	46	Membersh:
I		161 107.686998	3.093261	192.168.1.50	224.0.0.2	IGMPv2	0x02	0b (523)	46	Leave Gro
I		162 107.687972	0.000974	192.168.1.24	230.10.10.10	IGMPv2	0x9b	9d (39837)	60	Membersh:
I		163 107.695137	0.007165	192.168.1.50	230.10.10.10	IGMPv2	0x02	0c (524)	46	Membersh:
L		164 108.093934	0.398797	192.168.1.50	230.10.10.10	IGMPv2	0x02	0e (526)	46	Membersh:

- Vanuit het firewallstandpunt zijn er 2 typen IGMP-vragen: Algemene vragen en groepsspecifieke vragen
- Wanneer de firewall een bericht van de IGMP-verlofgroep ontvangt, moet het controleren of er andere leden van die groep op het subnetje staan. Om die reden stuurt de firewall een **Group-Specific Query:**

Eile Edit View Go Capture	Analyze Statistics Telep	hony Wireless Iools	Help					
📶 🔳 🖉 💿 📜 🛅 🗙 🙆	े ९ 🗰 🏓 🖀 Ŧ 🛓 🛄	📃 Q Q Q 🎹						
igmp								
No. Time	Delta	Source	Destination	Protocol	SGT	Identification	Length	Info
7 5.118518	0.000000	192.168.1.50	224.0.0.2	IGMPv2		0x01a7 (423)	46	Leave G
8 5.127230	0.008712	192.168.1.50	230.10.10.10	IGMPv2		0x01a8 (424)	46	Members
9 5.593022	0.465792	192.168.1.50	230.10.10.10	IGMPv2		0x01a9 (425)	46	Members
114 74.756894	69.163872	192.168.1.24	224.0.0.1	IGMPv2		0x7280 (29312)	60	Members
118 77.093155	2.336261	192.168.1.50	239.255.255.250	IGMPv2		0x01e9 (489)	46	Members
120 79.593298	2.500143	192.168.1.50	224.0.0.252	IGMPv2		0x01eb (491)	46	Members
122 81.093367	1.500069	192.168.1.50	230.10.10.10	IGMPv2		0x01ec (492)	46	Members
152 103.150111	22.056744	192.168.1.24	224.0.0.1	IGMPv2		0x1c5f (7263)	60	Members
153 103.593643	0.443532	192.168.1.50	224.0.0.252	IGMPv2		0x0206 (518)	46	Members
154 104.593737	1.000094	192.168.1.50	239.255.255.250	IGMPv2		0x0208 (520)	46	Members
161 107.686998	3.093261	192.168.1.50	224.0.0.2	IGMPv2		0x020b (523)	46	Leave G
162 107.687972	0.000974	192.168.1.24	230.10.10.10	IGMPv2		0x9b9d (39837)	60	Members
163 107.695137	0.007165	192.168.1.50	230.10.10.10	IGMPv2		0x020c (524)	46	Members
164 108.093934	0.398797	192.168.1.50	230.10.10.10	IGMPv2		0x020e (526)	46	Members

• Op subnetten met meerdere routers/firewalls wordt een **query** (een apparaat dat alle IGMP-vragen verstuurt) geselecteerd:

<#root>

firepower#

show igmp interface INSIDE

INSIDE is up, line protocol is up Internet address is 192.168.1.97/24 IGMP is enabled on interface Current IGMP version is 2 IGMP query interval is 125 seconds IGMP querier timeout is 60 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: 2 Cumulative IGMP activity: 21 joins, 20 leaves

IGMP querying router is 192.168.1.97 (this system)

<-- IGMP querier

• Op FTD, gelijkend op een klassieke ASA, kunt u **debug igmp** toelaten om IGMP-gerelateerde berichten te zien:

<#root>

firepower#

debug igmp

IGMP debugging is on IGMP: Received v2 Query on DMZ from 192.168.6.1 IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 239.255.255.250 <-- Received an IGMP packet IGMP: group_db: add new group 239.255.255.250 on INSIDE IGMP: MRIB updated (*,239.255.255.250) : Success IGMP: Switching to EXCLUDE mode for 239.255.255.250 on INSIDE IGMP: Updating EXCLUDE group timer for 239.255.255.250 IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 230.10.10.10 IGMP: group_db: add new group 230.10.10.10 on INSIDE IGMP: MRIB updated (*,230.10.10.10) : Success IGMP: Switching to EXCLUDE mode for 230.10.10.10 on INSIDE IGMP: Updating EXCLUDE group timer for 230.10.10.10 IGMP: Send v2 general Query on INSIDE IGMP: Received v2 Query on INSIDE from 192.168.1.97 IGMP: Send v2 general Query on OUTSIDE IGMP: Received v2 Query on OUTSIDE from 192.168.103.91 IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 239.255.255.250 IGMP: Updating EXCLUDE group timer for 239.255.255.250 IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 230.10.10.10 IGMP: Updating EXCLUDE group timer for 230.10.10.10

• Een host verlaat normaal een multicast groep met een Leave Group bericht (IGMPv2).

<u>F</u> ile	<u>E</u> dit <u>V</u> iew	v <u>G</u> o <u>C</u> apture <u>A</u>	Analyze Statistics	Telephony Wireless	<u>T</u> ools <u>H</u> elp		
	. 0	📜 🛅 🕱 🙆 🔍	🕻 🖛 🏓 🖀 有	👲 📃 📃 🔍 Q (€. ⊞		
📕 ig	mp.type == 0x	47					
No.		Time	Delta	Source	Destination	Protocol	Identification
	7	5.118518	0.00000	192.168.1.50	224.0.0.2	IGMPv2	0x01a7 (423)
	161	107.686998	102.568480	192.168.1.50	224.0.0.2	IGMPv2	0x020b (523)

Taak 1 - Control-Plane Multicast-verkeer

FTD				ASA
-@-	.91	192.168.103.x/24 FC00:103::/64	.50	-@-
	E1/4 OUTSIDE	OSPF area 0	G1/4 OUTSIDE	

Configureer een OSPFv2 en OSPFv3 tussen de FTD en de ASA. Controleer hoe de 2 apparaten L2 en L3 Multicast verkeer behandelen dat door OSPF wordt geproduceerd.

Oplossing

OSPFv2-configuratie

Firewall Management	Center Over	rview Analysis	Policies D	evices Objects	Integration		D
FTD4125-1 Cisco Firepower 4125 Threat Defense Device Routing Interfaces	e s Inline Sets Di	нср					
Manage Virtual Routers	Process 1	ID:	1				
	OSPF Role:						
Global 👻	Internal Router	•	Enter Description her	re Ad	vanced		
Virtual Pouter Properties							
	Process 2	ID:					
ECMP	0005 0.1.						
OSPF	USPF Role:						
OSPFv3	Internal Router	Ψ.	Enter Description her	re Ad	vanced		
FIGPP							
Elono -	Area Redistribut	tion InterArea	Filter Rule Su	ummary Address In	terface		
RIP				,			
Policy Based Routing							
∨ BGP	OSPF Process	Area ID	Area Type	Networks	Options	Authentication	Cost
IPv4		0	a comel	ant 100 100 100	0. 614		
IPv6		0	normal	net_192.168.103	taise	none	

Device Routing	Interface	s Inline Se	ts DHCP								
Manage Virtual Ro	outers	Process	1	ID:	1						
Global	Υ.	OSPF Role: Internal Rou	iter	•	Enter De	scription here		Advanced			
Virtual Router Proper ECMP	ties	Process	2	ID:							
OSPF OSPFv3		OSPF Role: Internal Rou	iter	v	Enter De:	scription here		Advanced			
EIGRP		Area R	edistribution	InterArea	Filter	Rule Summary	Address	Interface			
Policy Based Routing											
∨ BGP		Interface	1	Authentication	1	Point-to-Point	C	ost	Pri	iority	MT
IPv4 IPv6		OUTSIDE	N	lone		false	10	D	1		fals

Op dezelfde manier voor OSPFv3

Configuratie op FTD CLI:

<#root>

```
router ospf 1
```

```
network 192.168.103.0 255.255.255.0 area 0
log-adj-changes
!
ipv6 router ospf 1
no graceful-restart helper
log-adjacency-changes
!
interface Ethernet1/4
nameif OUTSIDE
security-level 0
ip address 192.168.103.91 255.255.255.0
ipv6 address fc00:103::91/64
ospf authentication null
ipv6 ospf 1 area 0
```

De configuratie maakt deze vermeldingen in de FTD Accelerated Security Path (ASP)-vergunningstabellen zodat toegang tot multicast-verkeer niet wordt geblokkeerd:

```
<#root>
firepower#
show asp table classify domain permit
...
in id=0x14f922db85f0, priority=13,
domain=permit, deny=false
```

```
<-- permit the packets
        hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=89
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=224.0.0.5, mask=255.255.255.255,
port=0, tag=any, dscp=0x0, nsg_id=none <-- OSPF for IPv4</pre>
input_ifc=OUTSIDE
(vrfid:0), output_ifc=identity(vrfid:0) <-- ingress interface</pre>
in id=0x14f922db9350, priority=13,
domain=permit, deny=false
<-- permit the packets
        hits=0, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=89
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=224.0.0.6, mask=255.255.255.255
, port=0, tag=any, dscp=0x0, nsg_id=none <-- OSPF for IPv4</pre>
input_ifc=OUTSIDE
(vrfid:0), output_ifc=identity(vrfid:0)
                                           <-- ingress interface
Voor IPv6:
<#root>
. . .
in id=0x14f923fb16f0, priority=13,
domain=permit, deny=false
 <-- permit the packets
        hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=89
        src ip/id=::/0, port=0, tag=any
dst ip/id=ff02::5/128
, port=0, tag=any, , nsg_id=none <-- OSPF for IPv6</pre>
input ifc=OUTSIDE
(vrfid:0), output_ifc=identity(vrfid:0) <-- ingress interface</pre>
in id=0x14f66e9d4780, priority=13,
domain=permit, deny=false
<-- permit the packets
        hits=0, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=89
        src ip/id=::/0, port=0, tag=any
dst ip/id=ff02::6/128
```

, port=0, tag=any, , nsg_id=none <-- OSPF for IPv6</pre>

```
input_ifc=OUTSIDE
```

```
(vrfid:0), output_ifc=identity(vrfid:0) <-- ingress interface
...</pre>
```

De nabijheid van OSPFv2 en OSPFv3 zijn UP:

<#root>

firepower#

show ospf neighbor

Neighbor ID Pri State Dead Time Address Interface 192.168.103.50 1

FULL/BDR

0:00:35 192.168.103.50 OUTSIDE <-- OSPF neighbor is up

firepower#

show ipv6 ospf neighbor

Neighbor ID Pri State Dead Time Interface ID Interface 192.168.103.50 1

FULL/BDR

```
0:00:34 3267035482 OUTSIDE <-- OSPF neighbor is up
```

Dit zijn de multicast OSPF-sessies die in het vak worden afgesloten:

<#root>

firepower#

show conn all | include OSPF

OSPF OUTSIDE fe80::2be:75ff:fef6:1d8e NP Identity Ifc ff02::5, idle 0:00:09, bytes 5924, flags OSPF OUTSIDE 192.168.103.50 NP Identity Ifc 224.0.0.5, idle 0:00:03, bytes 8904, flags OSPF OUTSIDE ff02::5 NP Identity Ifc fe80::f6db:e6ff:fe33:442e, idle 0:00:01, bytes 6304, flags OSPF OUTSIDE 224.0.0.5 NP Identity Ifc 192.168.103.91, idle 0:00:00, bytes 25220, flags

Schakel als test Opname voor IPv4 in en wis de verbindingen met het apparaat:

<#root>

firepower#

capture CAP interface OUTSIDE trace

firepower#

clear conn all

12 connection(s) deleted.
firepower#

clear capture CAP

firepower# !

Waarschuwing: dit veroorzaakt een storing! Dit voorbeeld is alleen voor demonstratiedoeleinden te zien!

De opgenomen OSPF-pakketten:

<#root>

firepower# show capture CAP | include proto-89

```
1: 12:25:33.142189 192.168.103.50 > 224.0.0.5 ip-proto-89, length 60
2: 12:25:33.702691 192.168.103.91 > 224.0.0.5 ip-proto-89, length 60
7: 12:25:36.317000 192.168.206.100 > 224.0.0.5 ip-proto-89, length 56
8: 12:25:36.952587 fe80::2be:75ff:fef6:1d8e > ff02::5 ip-proto-89 40 [flowlabel 0xe] [hlim 1]
12: 12:25:41.282608 fe80::f6db:e6ff:fe33:442e > ff02::5 ip-proto-89 40 [flowlabel 0xe] [hlim 1]
```

Hier is hoe het OSPFv2 multicast pakket door de firewall wordt behandeld:

<#root>

firepower#

show capture CAP packet-number 1 trace

115 packets captured

1: 12:25:33.142189 192.168.103.50 > 224.0.0.5 ip-proto-89, length 60

<-- The first packet of the flow Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Elapsed time: 6344 ns Config: Additional Information: MAC Access list

Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 6344 ns Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: ROUTE-LOOKUP Subtype: No ECMP load balancing Result: ALLOW Elapsed time: 10736 ns Config: Additional Information: Destination is locally connected. No ECMP load balancing. Found next-hop 192.168.103.50 using egress ifc OUTSIDE(vrfid:0) Phase: 4 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 5205 ns Config: Implicit Rule Additional Information: Phase: 5 Type: NAT Subtype: per-session Result: ALLOW Elapsed time: 5205 ns Config: Additional Information: Phase: 6 Type: IP-OPTIONS Subtype: Result: ALLOW Elapsed time: 5205 ns Config: Additional Information: Phase: 7 Type: CLUSTER-REDIRECT Subtype: cluster-redirect Result: ALLOW Elapsed time: 29280 ns Config: Additional Information: Phase: 8 Type: MULTICAST Subtype: Result: ALLOW Elapsed time: 976 ns Config: Additional Information: Phase: 9

Type: OSPF

<-- The OSPF process

Subtype: ospf

Result: ALLOW

Elapsed time: 488 ns

Config:

Additional Information:

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 13176 ns
Config:
Additional Information:
New flow created with id 620, packet dispatched to next module
Result:
input-interface: OUTSIDE(vrfid:0)
input-status: up
input-line-status: up

output-interface: OUTSIDE(vrfid:0) output-status: up output-line-status: up Action: allow Time Taken: 82959 ns

Dit is hoe het OSPFv3 multicast pakket door de firewall wordt behandeld:

<#root>
firepower#
show capture CAP packet-number 8 trace
274 packets captured
8: 12:25:36.952587 fe80::2be:75ff:fef6:1d8e > ff02::5 ip-proto-89 40 [flowlabel 0xe] [hlim 1]
<-- The first packet of the flow
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 7564 ns
Config:
Additional Information:</pre>

Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 7564 ns Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: ROUTE-LOOKUP Subtype: No ECMP load balancing Result: ALLOW Elapsed time: 8296 ns Config: Additional Information: Destination is locally connected. No ECMP load balancing. Found next-hop ff02::5 using egress ifc identity(vrfid:0) Phase: 4 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 8784 ns Config: Implicit Rule Additional Information: Phase: 5 Type: NAT Subtype: per-session Result: ALLOW Elapsed time: 8784 ns Config: Additional Information: Phase: 6 Type: CLUSTER-REDIRECT Subtype: cluster-redirect Result: ALLOW Elapsed time: 27816 ns Config: Additional Information: Phase: 7 Type: OSPF <-- The OSPF process Subtype: ospf Result: ALLOW

MAC Access list

Elapsed time: 976 ns

Config:

Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 13664 ns
Config:
Additional Information:
New flow created with id 624, packet dispatched to next module
Result:
input-interface: OUTSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
Time Taken: 83448 ns

Taak 2 - Basis multicast configureren

Topologie



Vereiste

Configureer de firewall zodat multicast verkeer van de server naar de multicast client op IP 230.10.10.10 wordt gestreamd

Oplossing

Vanuit het firewallstandpunt is de minimumconfiguratie om multicast routing wereldwijd mogelijk te maken. Dit schakelt op de achtergrond IGMP en PIM op alle firewall interfaces in.

FMC UI:

Firewall Management Ce Devices / NGFW Routing	enter	Overview	Analysis	Policies	Devices	Objects	Integration
FTD4125-1 Cisco Firepower 4125 Threat Defense							
Device Routing Interfaces	Inline Sets	DHCP					
Manage Virtual Pouters	Enable Multi	cast Routing (Er	nabling Mult	icast Routing ch	eckbox will e	nable both	IGMP and PIM on all Inte
Participal	Protocol	Neighbor Filter	Bidirect	ional Neighbor I	Filter Rer	ndezvous Po	pints Route Tree
Global Virtual Router Properties							
ECMP	nterface			PIM Enabled			DR Priority
OSPF							No record
OSPFv3							
PIP							
Policy Based Routing							
∨ BGP							
IPv4							
IPv6							
Static Route							
✓ Multicast Routing							
IGMP							
РІМ							

Op de firewall CLI is dit de gedrukte configuratie:

<#root>

firepower#

show run multicast-routing

multicast-routing

<-- Multicast routing is enabled

IGMP-verificatie

<#root>

firepower#

show igmp interface

diagnostic is up, line protocol is up Internet address is 0.0.0.0/0 IGMP is disabled on interface

```
INSIDE is up, line protocol is up
<-- The interface is UP
 Internet address is 192.168.1.24/24
 IGMP is enabled on interface
<-- IGMP is enabled on the interface
 Current IGMP version is 2
<-- IGMP version
 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: 1
 Cumulative IGMP activity: 4 joins, 3 leaves
 IGMP querying router is 192.168.1.24 (this system)
OUTSIDE is up, line protocol is up
<-- The interface is UP
 Internet address is 192.168.103.91/24
 IGMP is enabled on interface
<-- IGMP is enabled on the interface
 Current IGMP version is 2
<-- IGMP version
 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: 1
 Cumulative IGMP activity: 1 joins, 0 leaves
 IGMP querying router is 192.168.103.91 (this system)
<#root>
firepower#
```

show igmp group

IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 239.255.255.250 INSIDE 00:09:05 00:03:19 192.168.1.50 239.255.255.250 OUTSIDE 00:06:01 00:02:33 192.168.103.60

<#root>

firepower#

show igmp traffic

IGMP Traffic Counters Elapsed time since counters cleared: 03:40:48 Received Sent

	Received	Sent
Valid IGMP Packets	21	207
Queries	0	207
Reports	15	0
Leaves	6	0
Mtrace packets	0	0
DVMRP packets	0	0
PIM packets	0	0
Errors:		
Malformed Packets	0	
Martian source	0	
Bad Checksums	0	

<-- IGMP Reports received and sent

PIM-verificatie

<#root>

firepower#

show pim interface

Address	Interface	PIM Nbr Count	Hell Intvl	o DR Prior	DR
0.0.0.0	diagnostic	off 0	30	1	not elected
192.168.1.24	INSIDE	on 0	30	1	this system
192.168.103.91	OUTSIDE	on 0	30	1	this system

MFIB-verificatie

<#root>

firepower#

show mfib

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, K - Keepalive Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface Flags: A - Accept, F - Forward, NS - Negate Signalling IC - Internal Copy, NP - Not platform switched SP - Signal Present Interface Counts: FS Pkt Count/PS Pkt Count

(*,224.0.1.39) Flags: S K

Forwarding: 0/0/0/0

, Other: 0/0/0 <-- The Forwarding counters are: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

```
(*,224.0.1.40) Flags: S K
Forwarding: 0/0/0/0,
Other: 8/8/0
<-- The Other counters are: Total/RPF failed/Other drops
(*,232.0.0.0/8) Flags: K
Forwarding: 0/0/0/0, Other: 0/0/0</pre>
```

Multicastverkeer via de firewall

In dit geval wordt de VLC media player applicatie gebruikt als multicast server en client om multicast verkeer te testen:



VLC-multicast serverconfiguratie:



Open Media	
Ele Opsc Disc Opsc Opsc <tho< th=""><th>1</th></tho<>	1
C:\Users\Public\Videos\Sample Videos\Wildlife.wmv 2	Add Remove
Use a subțite file	Browse

Selecteer op het volgende scherm gewoon Volgende.

Selecteer het formaat:

nation Setup ect destinations to stream to		
P		
dd destinations following the streaming	ng methods you need. Be sure to check with transcoding that th	e format is compatible with the
vethod used.		
nethod used.		
nethod used.	1	2
iethod used.	RTP / MPEG Transport Stream	2 • Add
iew destination	1 RTP / MPEG Transport Stream	2 Add
iew destination	1 RTP / MPEG Transport Stream	2 • Add

Specificeer multicast IP en poort:

sect destination	tions to stream t	0						
ф —	RTP/TS 🔀							
This module	outputs the tran	scoded str	eam to a ne	twork via RTP.				
		_						
Address	230.10.10.10	D						
Address Base port	230.10.10.10	0 4 @						
Address Base port Stream nam	230.10.10.10 500-	0 4 💽						
Address Base port Stream nam	230.10.10.10 5004	0 4 💽						
Address Base port Stream nam	230.10.10.10 5004	9						
Address Base port Stream nam	230, 10, 10, 10 500-	9			Ba	¢	Next	Can

Transcoding Options Select and choose transcoding options		
Activate Transcoding Profile	Video - H. 264 + MP3 (MP4)	- 🕅 🕱 🗐
		Back Next Cancel

LINA inschakelen voor opname op de FTD-firewall:

<#root>

firepower#

capture INSIDE interface INSIDE match ip host 192.168.103.60 host 230.10.10.10

firepower#

capture OUTSIDE interface OUTSIDE trace match ip host 192.168.103.60 host 230.10.10.10

Selecteer de knop **Stream** voor het apparaat om de multicast-stroom te starten:

Set up any additional options for streaming Miscellaneous Options ✓ Stream all elementary streams Generated stream output string :sout=#transcode{vcodec=h264,acodec=mpga,ab=128,channels=2,samplerate=44100}:rtp{dst=230.10.10.10,port=5004,m} > :sout-all :sout-keep	?
Miscellaneous Options Image: Stream all elementary streams Generated stream output string :sout=#transcode(vcodec=h264,acodec=mpga,ab=128,channels=2,samplerate=44100):rtp(dst=230.10.10.10.port=5004,m) > :sout-all :sout-keep	
Stream all elementary streams Generated stream output string :sout=#transcode(vcodec=h264,acodec=mpga,ab=128,channels=2,samplerate=44100):rtp(dst=230.10.10.10.port=5004,m) > :sout-all :sout-keep	
Generated stream output string :sout=#transcode{vcodec=h264,acodec=mpga,ab=128,channels=2,samplerate=44100}:rtp{dst=230.10.10.10,port=5004,m } :sout-all :sout-keep	
:sout=#transcode{vcodec=h264,acodec=mpga,ab=128,channels=2,samplerate=44100}:rtp{dst=230.10.10.10,port=5004,m } :sout-all :sout-keep	

Schakel de optie â€[~]loopâ€[™] in, zodat de stream continu wordt verstuurd:



Verificatie (niet-operationeel scenario)

Dit scenario is een demonstratie van een niet-operationeel scenario. Het doel is het gedrag van de firewall te demonstreren.

Het firewallapparaat krijgt de multicast stroom, maar door:sturen het niet:

<#root>

firepower#

show capture

capture INSIDE type raw-data interface INSIDE

[Capturing - 0 bytes]

<-- No packets sent or received
match ip host 192.168.103.60 host 230.10.10.10
capture OUTSIDE type raw-data trace interface OUTSIDE</pre>

```
[Buffer Full - 524030 bytes]
```

<-- The buffer is full match ip host 192.168.103.60 host 230.10.10.10

Firewall LINA ASP drops tonen:

<#root>

firepower#

clear asp drop

firepower#

show asp drop

Frame drop:

Punt rate limit exceeded (punt-rate-limit)	232
< The multicast packets were dropped Flow is denied by configured rule (acl-drop) FP L2 rule drop (l2_acl)	2 2
Last clearing: 18:38:42 UTC Oct 12 2018 by enable_15	
Flow drop:	
Last clearing: 08:45:41 UTC May 17 2022 by enable_15	

Om een pakket te overtrekken is het nodig het eerste pakket van de multicast stroom op te nemen. Om deze reden de huidige stromen te zuiveren:

<#root>
firepower#
clear capture OUTSIDE
firepower#
clear conn all addr 230.10.10.10
2 connection(s) deleted.

```
firepower#
```

show capture OUTSIDE

379 packets captured

1: 08:49:04.537875 192.168.103.60.54100 > 230.10.10.10.5005: udp 64 2: 08:49:04.537936 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328 3: 08:49:04.538027 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328 4: 08:49:04.538058 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328 5: 08:49:04.538058 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328 6: 08:49:04.538073 192.168.103.60.54099 > 230.10.10.10.5004: udp 1328

De â€[~]detailâ€TM optie onthult het multicast MAC-adres:

<#root>

firepower#

show capture OUTSIDE detail

379 packets captured

1: 08:49:04.537875 0050.569d.344a

0100.5e0a.0a0a

0x0800 Length: 106 192.168.103.60.54100 > 230.10.10.10.5005: [udp sum ok] udp 64 (ttl 100, id 19759) 2: 08:49:04.537936 0050.569d.344a

0100.5e0a.0a0a

0x0800 Length: 1370 192.168.103.60.54099 > 230.10.10.10.5004: [udp sum ok] udp 1328 (ttl 100, id 19760) 3: 08:49:04.538027 0050.569d.344a 0100.5e0a.0a0a 0x0800 Length: 1370 192.168.103.60.54099 > 230.10.10.10.5004: [udp sum ok] udp 1328 (ttl 100, id 19761) ...

Het spoor van een echt pakket toont aan dat het pakket wordt toegestaan, maar dit is niet wat werkelijk gebeurt:

<#root>

firepower#

show capture OUTSIDE packet-number 1 trace

379 packets captured

1: 08:49:04.537875 192.168.103.60.54100 > 230.10.10.10.5005: udp 64

Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Elapsed time: 11712 ns Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 11712 ns Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: ROUTE-LOOKUP Subtype: No ECMP load balancing Result: ALLOW Elapsed time: 7808 ns Config: Additional Information: Destination is locally connected. No ECMP load balancing. Found next-hop 192.168.103.60 using egress ifc OUTSIDE(vrfid:0) Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Elapsed time: 5246 ns Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432 access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: mzafeiro_empty - Default access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE Additional Information: This packet will be sent to snort for additional processing where a verdict will be reached Phase: 5 Type: CONN-SETTINGS Subtype: Result: ALLOW Elapsed time: 5246 ns Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Phase: 6 Type: NAT Subtype: per-session Result: ALLOW Elapsed time: 5246 ns Config:

Additional Information: Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Elapsed time: 5246 ns Config: Additional Information: Phase: 8 Type: CLUSTER-REDIRECT Subtype: cluster-redirect Result: ALLOW Elapsed time: 31232 ns Config: Additional Information: Phase: 9 Type: MULTICAST <-- multicast process Subtype: Result: ALLOW Elapsed time: 976 ns Config: Additional Information: Phase: 10 Type: FLOW-CREATION <-- the packet belongs to a new flow Subtype: Result: ALLOW Elapsed time: 20496 ns Config: Additional Information: New flow created with id 3705, packet dispatched to next module Result: input-interface: OUTSIDE(vrfid:0) input-status: up input-line-status: up output-interface: OUTSIDE(vrfid:0) output-status: up output-line-status: up Action: allow <-- The packet is allowed Time Taken: 104920 ns

Gebaseerd op de route en mfib tellers, worden de pakketten gelaten vallen omdat de Uitgaande Lijst van de Interface (OIL) leeg is:

<#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 (192.168.103.60, 230.10.10.10), 00:01:33/00:01:56, flags: SPF Incoming interface: OUTSIDE RPF nbr: 192.168.103.60 Outgoing interface list: Null <-- The OIL is empty! (*, 239.255.255.250), 00:01:50/never, RP 0.0.0.0, flags: SCJ Incoming interface: Null RPF nbr: 0.0.0.0 Immediate Outgoing interface list: INSIDE, Forward, 00:01:50/never

De MFIB-tellers tonen RPF-storingen, wat in dit geval niet het geval is:

<#root> firepower# show mfib 230.10.10.10 Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, K - Keepalive firepower# show mfib 230.10.10.10 Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, K - Keepalive Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second <-- Multicast forwarding counters Other counts: Total/RPF failed /Other drops <-- Multicast drop counters Interface Flags: A - Accept, F - Forward, NS - Negate Signalling IC - Internal Copy, NP - Not platform switched SP - Signal Present Interface Counts: FS Pkt Count/PS Pkt Count (192.168.103.60,230.10.10.10) Flags: K Forwarding: 0/0/0/0

Other: 650/650

,

/0 <-- Allowed and dropped multicast packets</pre>

Vergelijkbare RPF-fouten in de output 'toon mfib count':

<#root>

firepower#

show mfib 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: 224.0.1.39 RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0 Group: 224.0.1.40 RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0 Group: 230.10.10.10 Source: 192.168.103.60, Forwarding: 0/0/0/0, Other: 1115/1115 <-- Allowed and dropped multicast packets</pre> /0 Tot. shown: Source count: 1, pkt count: 0 Group: 232.0.0.0/8 RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0 Group: 239.255.255.250 RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0

Configureer de VLC multicast-ontvanger:

🛓 v	LC media player				
Med	dia Playback Audio Video	Subtitle	Tools	View	Help
	Open File	Ctrl+C)		
	Open Multiple Files	Ctrl+S	hift+O		
	Open Folder	Ctrl+F			
٢	Open Disc	Ctrl+D)		
쁳	Open Network Stream	Ctrl+N	1		
	Open Capture Device	Ctrl+C			
	Open Location from clipboard	Ctrl+V			
	Open Recent Media				
	Save Playlist to File	Ctrl+Y	1		
	Convert / Save	Ctrl+R			
((•))	Stream	Ctrl+S			
	Quit at the end of playlist				
	Quit	Ctrl+Q	2		

Specificeer de multicast IP-bron en selecteer Afspelen:

A VLC media player Media Playback Audio Video Subtitle Tools View Help	
🚊 Open Media	
Ele Disc Network Capture Device Network Protocol Please enter a network URL: Image: Capture Device rtp://@230.10.10.10:5004 http://www.example.com/stream.avi http://www.example.com/stream.avi modifier/124	
rtspillens.examples.com/stream.asx rtspillenver.example.org/8060/test.sdp http://www.yourtube.com/watch?v=gg64x	
Show more options	Stream V Carrel
	Enqueue Alt+E Play Alt+P
	Stream Alt+S Convert Alt+O

In het backend, zodra u **Spel** selecteert, kondigt de gastheer zijn bereidheid aan om zich bij de specifieke multicast groep aan te sluiten en verzendt een bericht van het **IGMP- Rapport**:



Als u een debug inschakelt, kunt u de IGMP-rapportberichten zien:

<#root>

firepower#

debug igmp group 230.10.10.10

IGMP: Received v2 Report on INSIDE from 192.168.1.50 for 230.10.10.10

<-- IGMPv2 Report received IGMP: group_db: add new group 230.10.10.10 on INSIDE IGMP: MRIB updated (*,230.10.10.10) : Success IGMP: Switching to EXCLUDE mode for 230.10.10.10 on INSIDE IGMP: Updating EXCLUDE group timer for 230.10.10.10

De stream start:



Verificatie (operationeel scenario)

<#root>

firepower#

show capture

capture INSIDE type raw-data interface INSIDE

[Buffer Full - 524156 bytes]

<-- Multicast packets on the egress interface match ip host 192.168.103.60 host 230.10.10.10 capture OUTSIDE type raw-data trace interface OUTSIDE

[Buffer Full - 524030 bytes]

<-- Multicast packets on the ingress interface
match ip host 192.168.103.60 host 230.10.10.10</pre>

De routekaart van de firewall:

<#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 (*, 230.10.10.10), 00:00:34/never, RP 0.0.0.0, flags: SCJ Incoming interface: Null RPF nbr: 0.0.0.0 Immediate Outgoing interface list: INSIDE, Forward, 00:00:34/never (192.168.103.60, 230.10.10.10), 00:01:49/00:03:29, flags: SFJT Incoming interface: OUTSIDE RPF nbr: 192.168.103.60 Inherited Outgoing interface list:

INSIDE, Forward, 00:00:34/never

```
<-- The OIL shows an interface
```

<#root> firepower# show mfib 230.10.10.10 Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, K - Keepalive Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface Flags: A - Accept, F - Forward, NS - Negate Signalling IC - Internal Copy, NP - Not platform switched SP - Signal Present Interface Counts: FS Pkt Count/PS Pkt Count (*,230.10.10.10) Flags: C K Forwarding: 0/0/0/0, Other: 0/0/0 INSIDE Flags: F NS Pkts: 0/0 (192.168.103.60,230.10.10.10) Flags: K Forwarding: 6373/0/1354/0, Other: 548/548/0 <-- There are multicast packets forwarded OUTSIDE Flags: A INSIDE Flags: F NS Pkts: 6373/6 mfib-tellers: <#root> firepower# show mfib count **IP Multicast Statistics** 10 routes, 5 groups, 0.40 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: 224.0.1.39

```
RP-tree:
    Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree:
    Forwarding: 0/0/0/0, Other: 0/0/0
Group: 230.10.10.10
  RP-tree:
    Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 192.168.103.60,
    Forwarding: 7763/0/1354/0,
Other: 548/548/0
                  <-- There are multicast packets forwarded</pre>
  Tot. shown: Source count: 1, pkt count: 0
Group: 232.0.0.0/8
  RP-tree:
    Forwarding: 0/0/0/0, Other: 0/0/0
Group: 239.255.255.250
  RP-tree:
    Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 192.168.1.50,
    Forwarding: 7/0/500/0, Other: 0/0/0
  Tot. shown: Source count: 1, pkt count: 0
```

IGMP-controle

- IGMP-controle is een mechanisme dat op switches wordt gebruikt om multicast-overstromingen te voorkomen.
- De switch bewaakt IGMP-rapporten om te bepalen waar hosts (ontvangers) zich bevinden.
- De switch bewaakt IGMP-vragen om te bepalen waar zich routers/firewalls (afzenders) bevinden.
- IGMP-controle is standaard ingeschakeld op de meeste Cisco-switches. Controleer de bijbehorende switchinghandleidingen voor meer informatie. Hier is de voorbeelduitvoer van een L3 Catalyst switch:

<#root>

switch#

show ip igmp snooping statistics

```
Current number of Statistics entries : 15
Configured Statistics database limit : 32000
Configured Statistics database threshold: 25600
Configured Statistics database limit : Not exceeded
Configured Statistics database threshold: Not exceeded
```

Snooping statistics for Vlan204
#channels: 3
#hosts : 5

Source/Group 0.0.0.0/230.10.10.10 0.0.0.0/230.10.10.10 0.0.0.0/230.10.10.10 0.0.0.0/239.255.255.250	Interface Vl204:Gi1/48 Vl204:Gi1/48 Vl204:Gi2/1 Vl204:Gi2/1	Reporter 192.168.1.50 192.168.1.97 192.168.1.50 192.168.1.50	Uptime 2d13h 2d13h 2d10h 2d10h 2d11h	Last-Join - 2d12h 02:20:05 02:20:05	Last-Leave 2d12h - 02:20:00 02:20:00
0.0.0/239.255.255.250	V1204:Gi2/1	192.168.2.50	2d14h	2d13h	-
0.0.0/239.255.255.250	V1204:G12/1	192.168.6.50	2d13h	-	2d13h
0.0.0.0/224.0.1.40	V1204:G12/26	192.168.2.1	2d14h	00:00:39	2d13h
<pre>Snooping statistics for Vlan206 #channels: 4 #hosts : 3</pre>					
Source/Group	Interface	Reporter	Uptime	Last-Join	Last-Leave
0.0.0.0/230.10.10.10	Vl206:Gi1/48	192.168.6.91	00:30:15	2d13h	2d13h
0.0.0/239.10.10.10	Vl206:Gi1/48	192.168.6.91	2d14h	2d13h	-
0.0.0/239.255.255.250	Vl206:Gi2/1	192.168.6.50	2d12h	00:52:49	00:52:45
0.0.0/224.0.1.40	V1206:Gi2/26	192.168.6.1	00:20:10	2d13h	2d13h
0.0.0/230.10.10.10	Vl206:Gi2/26	192.168.6.1	2d13h	2d13h	-
0.0.0.0/230.10.10.10	Vl206:Gi2/26	192.168.6.91	2d13h	-	2d13h
0.0.0.0/239.10.10.10	Vl206:Gi2/26	192.168.6.1	2d14h	2d14h	-
0.0.0.0/239.10.10.10	Vl206:Gi2/26	192.168.6.91	2d14h	-	2d14h

Taak 3 - IGMP-statische groep vs IGMP-groep

Overzicht

	Statische groep van IP-igmp	IP-igmp samenvoegen-groep
Van toepassing op FTD- interface?	Ja	Ja
Trekt de FTD een multicast stream aan? Vooruit het FTD multicast-	Ja, een PIM Join wordt verzonden naar het stroomopwaartse apparaat. de bron of naar het Rendezvous Point (RP). Dit gebeurt alleen als de FTD met deze opdracht de PIM Designated Router (DR) op die interface is.	Ja, een PIM Join wordt verzonden naar het stroomopwaartse apparaat. de bron of naar het Rendezvous Point (RP). Dit gebeurt alleen als de FTD met deze opdracht de PIM Designated Router (DR) op die interface is.
interface?		
Verbruikt de FTD en antwoordt deze op het multicast verkeer	Nee	Ja, de FTD straft de multicast stream naar de CPU, verbruikt deze en antwoordt op de bron.
CPU-impact	Minimaal omdat het pakket niet op CPU is afgestemd.	Kan invloed hebben op de FTD CPU omdat elk multicast pakket dat tot de groep

	behoort, wordt gepunteerd op de FTD CPU.
	CI U.

Taakvereiste

Overweeg deze topologie:



Schakel deze opnamen in op de firewall:

<#root>

firepower#

capture CAPI interface OUTSIDE trace match icmp host 192.168.103.62 any

firepower#

capture CAPO interface INSIDE match icmp host 192.168.103.62 any

- 1. Gebruik ICMP-ping vanuit de L3-switch om multicast verkeer naar IP 230.11.11.1 te verzenden en controleer hoe dit door de firewall wordt verwerkt.
- 2. Schakel de opdracht **statisch-groep igmp** in op de firewall INSIDE-interface en controleer hoe de multicast stream (IP 230.11.11.11) door de firewall wordt verwerkt.
- 3. Schakel de opdracht **statisch-groep igmp** in op de firewall INSIDE-interface en controleer hoe de multicast stream (IP 230.11.11.11) door de firewall wordt verwerkt.

Oplossing

De firewall heeft geen routes voor IP 230.11.11.11:

<#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), 00:43:21/never, RP 0.0.0.0, flags: SCJ
Incoming interface: Null
RPF nbr: 0.0.0.0
Immediate Outgoing interface list:
    OUTSIDE, Forward, 00:05:41/never
    INSIDE, Forward, 00:43:21/never
```

Een eenvoudige manier om multicast te testen is het ICMP-pinggereedschap te gebruiken. In dit geval, initieer pingelen van R2 aan het multicast IP adres 230.11.11.11:

<#root>

L3-Switch# ping 230.11.11.11 re 100 Type escape sequence to abort. Sending 100, 100-byte ICMP Echos to 230.11.11.11, timeout is 2 seconds:

Op de firewall wordt dynamisch een route gecreëerd en is de OIL leeg:

<#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
(192.168.103.62, 230.11.11.11), 00:02:33/00:00:56, flags: SPF
<-- The mroute is added
Incoming interface: OUTSIDE
RPF nbr: 192.168.103.62
Outgoing interface list: Null
<-- The OIL is empty</pre>
```

De opname op de firewall toont:

<#root>

firepower# show capture

capture CAPI type raw-data trace interface OUTSIDE

[Capturing - 1040 bytes]

<-- There are ICMP packets captured on ingress interface
match icmp host 192.168.103.62 any
capture CAPO type raw-data interface INSIDE</pre>

[Capturing - 0 bytes]

<-- There are no ICMP packets on egress match icmp host 192.168.103.62 any

De firewall maakt verbindingen voor elke ping, maar laat de pakketten stilzwijgend vallen:

```
<#root>
```

firepower#

show log | include 230.11.11.11

May 17 2022 11:05:47: %FTD-7-609001:

Built local-host identity:230.11.11.11

```
<-- A new connection is created
May 17 2022 11:05:47: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.1.99/6 gaddr 230.11
May 17 2022 11:05:47: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.103.62/6 gaddr 230.
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.1.99/6 gaddr 230.11.11.1
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11.1
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11</pre>
```

Teardown local-host identity:230.11.11.11 duration 0:00:02

<-- The connection is closed May 17 2022 11:05:51: %FTD-7-609001:

Built local-host identity:230.11.11.11

<

A new connection is created May 17 2022 11:05:51: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.1.99/6 gaddr 230.11 May 17 2022 11:05:51: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.103.62/6 gaddr 230. May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.1.99/6 gaddr 230.11.11.1 May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11.1 May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.11.1

Teardown local-host identity:230.11.11.11 duration 0:00:02

<-- The connection is closed

Opmerking: de LINA ASP-drop-opname toont de gedropte pakketten niet

De belangrijkste indicatie van multicast pakketdruppels is:

<#root> firepower# show mfib Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, K - Keepalive Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface Flags: A - Accept, F - Forward, NS - Negate Signalling IC - Internal Copy, NP - Not platform switched SP - Signal Present Interface Counts: FS Pkt Count/PS Pkt Count (*,224.0.1.39) Flags: S K Forwarding: 0/0/0/0, Other: 0/0/0 (*,224.0.1.40) Flags: S K Forwarding: 0/0/0/0, Other: 0/0/0 (192.168.103.62,230.11.11.11) <-- The multicast stream Flags: K Forwarding: 0/0/0/0, Other: 27/27/0 <-- The packets are dropped

IGMP statische groep

Configureer op FMC een statische IGMP-groep:

Firewall Management Devices / NGFW Routing	Center	Overview	Analysis	Policies	Devices	Objects	Integra
FTD4125-1 Cisco Firepower 4125 Threat Defense Device Routing Interfaces	Inline Sets	DHCP					
Manage Virtual Routers	Enable Multi Protocol	icast Routing (E Access Group	nabling Multic Static Gro	ast Routing c	heckbox will e Group	nable both IGN	P and PI
Virtual Router Properties							
ECMP OSPF	Interface				Add IGN	IP Static Gr	oup par
OSPFv3 Eigrp					INSIDE		
RIP Policy Based Routing					group_2	aroup:* 30.11.11.11	
 ✓ BGP In t 							[
IPv4 IPv6							
Static Route \sim Multicast Routing							
IGMP							

Dit wordt op de achtergrond ingezet:

```
<#root>
interface Port-channel1.205
vlan 205
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.24 255.255.255.0
igmp static-group 230.11.11.11
<--- IGMP static group is enabled on the interface</pre>
```

Pingelen mislukt, maar het ICMP-multicast verkeer wordt nu doorgestuurd door de firewall:

L3-Switch#

ping 230.11.11.11 re 10000

Type escape sequence to abort. Sending 10000, 100-byte ICMP Echos to 230.11.11.11, timeout is 2 seconds:

<#root>

firepower#

show capture

capture CAPI type raw-data trace interface OUTSIDE

[Capturing - 650 bytes]

<-- ICMP packets are captured on ingress interface
match icmp host 192.168.103.62 any
capture CAPO type raw-data interface INSIDE</pre>

[Capturing - 670 bytes]

<-- ICMP packets are captured on egress interface match icmp host 192.168.103.62 any

<#root>

firepower#

show capture CAPI

8 packets captured

1: 11:31:32.470541 192.168.103.62 > 230.11.11.11 icmp: echo request 2: 11:31:34.470358 192.168.103.62 > 230.11.11.11 icmp: echo request 3: 11:31:36.470831 192.168.103.62 > 230.11.11.11 icmp: echo request 4: 11:31:38.470785 192.168.103.62 > 230.11.11.11 icmp: echo request

firepower#

show capture CAPO

11 packets captured

```
1: 11:31:32.470587 802.10 vlan#205 P0 192.168.103.62 > 230.11.11.11 icmp: echo request
2: 11:31:34.470404 802.10 vlan#205 P0 192.168.103.62 > 230.11.11.11 icmp: echo request
3: 11:31:36.470861 802.10 vlan#205 P0 192.168.103.62 > 230.11.11.11 icmp: echo request
4: 11:31:38.470816 802.10 vlan#205 P0 192.168.103.62 > 230.11.11.11 icmp: echo request
```

Opmerking: het overtrekken van het pakket toont een onjuiste uitvoer (toegangsinterface is hetzelfde als uitgang). Controleer voor meer informatie Cisco bug-id <u>CSCvm89673.</u>

show capture CAPI packet-number 1 trace 1: 11:39:33.553987 192.168.103.62 > 230.11.11.11 icmp: echo request Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Elapsed time: 3172 ns Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 3172 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 192.168.103.62 using egress ifc OUTSIDE(vrfid:0) Phase: 4 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 5368 ns Config: Implicit Rule Additional Information: Phase: 5 Type: CONN-SETTINGS Subtype: Result: ALLOW Elapsed time: 5368 ns Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Phase: 6

```
Type: NAT
```

Subtype: per-session Result: ALLOW Elapsed time: 5368 ns Config: Additional Information: Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Elapsed time: 5368 ns Config: Additional Information: Phase: 8 Type: CLUSTER-REDIRECT Subtype: cluster-redirect Result: ALLOW Elapsed time: 31720 ns Config: Additional Information: Phase: 9 Type: INSPECT Subtype: np-inspect Result: ALLOW Elapsed time: 488 ns Config: class-map inspection_default match default-inspection-traffic policy-map global_policy class inspection_default inspect icmp service-policy global_policy global Additional Information: Phase: 10 Type: INSPECT Subtype: np-inspect Result: ALLOW Elapsed time: 2440 ns Config: Additional Information: Phase: 11 Type: MULTICAST <-- The packet is multicast Subtype: Result: ALLOW

Elapsed time: 976 ns

Additional Information: Phase: 12 Type: FLOW-CREATION <-- A new flow is created Subtype: Result: ALLOW Elapsed time: 56120 ns Config: Additional Information: New flow created with id 5690, packet dispatched to next module Phase: 13 Type: CAPTURE Subtype: Result: ALLOW Elapsed time: 10248 ns Config: Additional Information: MAC Access list Result: input-interface: OUTSIDE(vrfid:0) input-status: up input-line-status: up output-interface: OUTSIDE(vrfid:0) output-status: up output-line-status: up Action: allow <-- The packet is allowed Time Taken: 139568 ns

Tip: U kunt pingen met timeout 0 van de bronhost en u kunt de firewall mfib tellers controleren:

```
<#root>
firepower# clear mfib counters
firepower# !ping from the source host.
firepower#
show mfib 230.11.11.11
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,230.11.11.11) Flags: C K
 Forwarding: 0/0/0/0, Other: 0/0/0
 INSIDE Flags: F NS
    Pkts: 0/0
(192.168.103.62,230.11.11.11) Flags: K
Forwarding: 500/0/100/0, Other: 0/0/0
<-- 500 multicast packets forwarded. The average size of each packet is 100 Bytes
 OUTSIDE Flags: A
 INSIDE Flags: F NS
   Pkts: 500/0
```

IGMP-groep

Op FMC-afstandsbediening kunt u de eerder ingestelde statische groepsconfiguratie configureren en een IGMP-groepsgroep configureren:

Firewall Management	t Center	Overview	Analysis	Policies	Devices	Objects	Integration	
FTD4125-1								
Cisco Firepower 4125 Threat Defens	e							
Device Routing Interface	s Inline Set	s DHCP						
Manage Mithael Desiters	Enable Mu	Iticast Routing (I	Enabling Multic	ast Routing cl	neckbox will er	nable both IGI	MP and PIM on a	ll Interfaces.)
Manage Virtual Routers	Protocol	Access Group	Static Gro	up Join (Group			
Global 🔻								
Virtual Router Properties								
ECMP	Interface							Multicast Group Address
OSPF	INSIDE							group 230 11 11 11
OSPFv3	INCIDE							group_200.11.11.11
EIGRP								
RIP								
Policy Based Routing								
∨ BGP								
IPv4								
IPv6								
Static Route								
V Multicast Routing								
IGMP								
H1	gmp join-	group 23().11.11.1 1 ×/24			FTD		192.168.1



De geïmplementeerde configuratie:

<#root>

firepower#

show run interface Port-channel1.205

!
interface Port-channel1.205
vlan 205
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0

ip address 192.168.1.24 255.255.255.0

igmp join-group 230.11.11.11

<-- The interface joined the multicast group

De IGMP-groep:

<#root>

firepower#

show igmp group

IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 230.11.11.11 INSIDE 00:30:43 never 192.168.1.24 <-- The group is enabled on the interface</pre>

Probeer vanuit de bronhost de eerste ICMP-multicast test naar 230.11.11.11 IP:

<#root>

L3-Switch#

ping 230.11.11.11 repeat 10

Type escape sequence to abort. Sending 10, 100-byte ICMP Echos to 230.11.11.11, timeout is 2 seconds: Reply to request 0 from 192.168.1.24, 12 ms Reply to request 1 from 192.168.1.24, 8 ms Reply to request 2 from 192.168.1.24, 8 ms Reply to request 3 from 192.168.1.24, 8 ms Reply to request 4 from 192.168.1.24, 8 ms Reply to request 5 from 192.168.1.24, 12 ms Reply to request 6 from 192.168.1.24, 8 ms Reply to request 7 from 192.168.1.24, 8 ms Reply to request 7 from 192.168.1.24, 8 ms Reply to request 8 from 192.168.1.24, 8 ms Reply to request 9 from 192.168.1.24, 8 ms

Opmerking: als u niet alle antwoorden ziet, controleert u CSCvm90069 met bug-id van Cisco.

Taak 4 - IGMP Stub Multicast-routing configureren



Configureer stub multicast routing op FTD zodat IGMP Membership Report-berichten die op de BINNENKANT-interface worden ontvangen, naar de BUITENinterface worden doorgestuurd.

Oplossing

Firewall Management	Center	Overview	Analysis	Policies	Devices	Objects	Integratio
FTD4125-1 Cisco Firepower 4125 Threat Defense Device Routing Interfaces	Inline Sets	DHCP					
Manage Virtual Routers	Enable Multic Protocol	cast Routing (Access Group	Enabling Multica Static Gro	ast Routing ch up Join G	eckbox will ena aroup	able both IGN	IP and PIM o
Virtual Router Properties							
ECMP	Interface	En	abled	Forwa	ard Interface	Version	
OSPF OSPFv3	INSIDE	tru	e	OUTS	IDE	2	
EIGRP							
RIP							
Policy Based Routing							
∽ BGP							
IPv4							
IPv6							
Static Route							
✓ Multicast Routing							
IGMP							

De geïmplementeerde configuratie:

<#root>

firepower#

show run multicast-routing

multicast-routing

<-- Multicast routing is enabled firepower#

show run interface Port-channel1.205

```
!
interface Port-channel1.205
vlan 205
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.24 255.255.255.0
```

igmp forward interface OUTSIDE

<-- The interface does stub multicast routing

Verificatie

Opnamen op FTD inschakelen:

<#root>

firepower#

capture CAPI interface INSIDE trace match igmp any host 230.10.10.10

firepower#

capture CAPO interface OUTSIDE match igmp any host 230.10.10.10

Verificatie

Om een IGMP Membership Report af te dwingen, kunt u een applicatie als VLC gebruiken:

File	Ø Disc	B Network	Capture De	vice		
Network I	Protocol					
Please er	ter a netwo	rk URL:				
rtp://@	230.10.10.1	0:5004				•
http://w rtp://@ mms:// rtsp://s	www.example :1234 imms.example erver.example	.com/stream.avi s.com/stream.asx .org:8080/best.sdp				
http://v	www.yourtube	s.com/watch?v=gg6	Ax			
Show mor	e options					
Show mor	e options				Stream 💌	Cancel
Show mor	e options				Stream 💌 Enqueue	Cancel Alt+E

De FTD-proxy's van de IGMP-pakketten:

<#root>

firepower#

show capture

capture CAPI type raw-data trace interface INSIDE

[Capturing - 66 bytes]

<-- IGMP packets captured on ingress match igmp any host 230.10.10.10 capture CAPO type raw-data interface OUTSIDE

[Capturing - 62 bytes]

<-- IGMP packets captured on egress match igmp any host 230.10.10.10

De FTD wijzigt de IP-bron:

<#root>

firepower#

show capture CAPI

1 packet captured

1: 12:21:12.820483 802.1Q vlan#205 P6

192.168.1.50

> 230.10.10.10 ip-proto-2, length 8 <-- The source IP of the packet on ingress interface 1 packet shown firepower#

show capture CAPO

1 packet captured

1: 12:21:12.820743

192.168.103.91

```
> 230.10.10.10 ip-proto-2, length 8 <-- The source IP of the packet on egress interface 1 packet shown
```

Als u het pakket in Wireshark controleert, kunt u zien dat het pakket volledig door de firewall wordt geregenereerd (de IP-identificatie verandert).

Er wordt een groepsvermelding aangemaakt op FTD:

<#root>

firepower#

show igmp group

IGMP Connected Group Membership
Group AddressUptimeExpiresLast Reporter230.10.10.10INSIDE00:15:2200:03:28192.168.1.50<-- IGMP group is enabled on the ingress interface
239.255.255.250INSIDE00:15:2700:03:29192.168.1.50

De FTD-firewall maakt 2 besturingsplane verbindingen:

<#root>

firepower#

show conn all address 230.10.10.10

9 in use, 28 most used Inspect Snort: preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

IGMP INSIDE 192.168.1.50 NP Identity Ifc 230.10.10.10, idle 0:00:09, bytes 8, flags

<-- Connection terminated on the ingress interface

IGMP OUTSIDE 230.10.10.10 NP Identity Ifc 192.168.103.91, idle 0:00:09, bytes 8, flags

<-- Connection terminated on the egress interface

Soort eerste pakket:

<#root>

firepower#

show capture CAPI packet-number 1 trace

6 packets captured

1: 12:21:12.820483 802.1Q vlan#205 P6 192.168.1.50 > 230.10.10.10 ip-proto-2, length 8

<-- The first packet of the flow Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Elapsed time: 5124 ns Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 5124 ns Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: ROUTE-LOOKUP Subtype: No ECMP load balancing Result: ALLOW Elapsed time: 7808 ns Config: Additional Information: Destination is locally connected. No ECMP load balancing. Found next-hop 192.168.1.50 using egress ifc INSIDE(vrfid:0) Phase: 4 Type: CLUSTER-DROP-ON-SLAVE Subtype: cluster-drop-on-slave Result: ALLOW Elapsed time: 5368 ns Config: Additional Information: Phase: 5 Type: ACCESS-LIST Subtype: Result: ALLOW Elapsed time: 5368 ns Config:

Implicit Rule Additional Information: Phase: 6 Type: IP-OPTIONS Subtype: Result: ALLOW Elapsed time: 5368 ns Config: Additional Information: Phase: 7 Type: NAT Subtype: per-session Result: ALLOW Elapsed time: 5368 ns Config: Additional Information: Phase: 8 Type: CLUSTER-REDIRECT Subtype: cluster-redirect Result: ALLOW Elapsed time: 40504 ns Config: Additional Information: Phase: 9 Type: MULTICAST <-- The packet is multicast Subtype: Result: ALLOW Elapsed time: 976 ns Config: Additional Information:

Phase: 10

Type: FLOW-CREATION

<-- A new flow is created

Subtype:

Result: ALLOW

Elapsed time: 17568 ns

Config:

Additional Information:

New flow created with id 5945, packet dispatched to next module

Phase: 11

```
Type: FLOW-CREATION
```

<-- A second flow is created

Subtype:

Result: ALLOW

Elapsed time: 39528 ns

Config:

Additional Information:

New flow created with id 5946, packet dispatched to next module

Phase: 12 Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP Subtype: Lookup Nexthop on interface Result: ALLOW Elapsed time: 6344 ns Config: Additional Information: Found next-hop 230.10.10.10 using egress ifc OUTSIDE(vrfid:0) Phase: 13 Type: CAPTURE Subtype: De 14 MURCE

Result: ALLOW Elapsed time: 9760 ns Config: Additional Information: MAC Access list

```
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: 154208 ns
```

Bekende problemen

Filter multicast verkeer op doelzones

U kunt geen doelbeveiligingszone opgeven voor de regel Toegangsbeheer die overeenkomt met het multicastverkeer:



Dit wordt ook gedocumenteerd in de FMC-gebruikershandleiding:

Book Contents	Q Find Matches in This Book
Book Title Page	Internet multicast routing from address range 224.0.0/24 is not supported; IGMP g multicast routing for the reserved addressess.
Configuration	Clustering
> Device Operations	In clustering, for IGMP and PIM, this feature is only supported on the primary unit.
> Interfaces and Device Settings	Additional Guidelines
\sim Routing	You must configure an access control or prefilter rule on the inbound security zo
Static and Default Routes	such as 224.1.2.3. However, you cannot specify a destination security zone for multicast connections during initial connection validation.
Virtual Routers	You cannot disable an interface with PIM configured on it. If you have configured
ECMP	PIM Protocol), disabling the multicast routing and PIM does not remove the PIM the PIM configuration to disable the interface.
OSPF	 PIM/IGMP Multicast routing is not supported on interfaces in a traffic zone.
BGP	Do not configure FTD to simultaneously be a Rendezvous Point (RP) and a First
RIP	
Multicast	Configure IGMP Features
Policy Based Routing	IP hosts use IGMP to report their group memberships to directly-connected multicate register individual hosts in a multicast group on a particular LAN. Hosts identify group on a particular LAN.

IGMP-rapporten worden ontkend door de firewall wanneer de IGMP-interfacelimiet wordt overschreden

Standaard staat de firewall maximaal 500 actieve verbindingen (rapporten) toe op een interface. Als deze drempelwaarde wordt overschreden, negeert de firewall extra inkomende IGMP-rapporten van de multicast ontvangers.

Om de IGMP-limiet en actieve verbindingen te controleren, voert u de opdracht **show igmp interface** *name*:

<#root>

asa#

```
show igmp interface inside
```

inside is up, line protocol is up Internet address is 10.10.10.1/24 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: 500

Cumulative IGMP activity: 0 joins, 0 leaves IGMP querying router is 10.10.10.1 (this system)

Het IGMP debug commando **debug igmp** toont deze uitvoer:

<#root>

asa#

debug igmp

Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: Group 230.1.2.3 limit denied on inside

<u>CSCuw84390</u> bug-id van Cisco houdt de verbetering bij om de IGMP-limiet te verhogen.

Firewall negeert IGMP-rapporten voor het 232.x.x/8-adresbereik

Het 232.x.x.x/8-adresbereik is bedoeld voor gebruik met Source Specific Multicast (SSM). De firewall ondersteunt geen PIM Source Specific Multicast (SSM)-functionaliteit en bijbehorende configuratie.

Het IGMP debug commando debug igmp toont deze uitvoer:

<#root>

asa#

debug igmp

Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: Received v2 Report on inside from 10.10.10.11 for 232.179.89 Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: group_db: add new group 232.179.89.253 on inside

Apr 20 2023 09:37:10: %ASA-7-711001: IGMP: Exclude report on inside ignored for SSM group 232.179.89.253

Cisco bug-id CSCsr53916 houdt de verbetering bij om het SSM-bereik te ondersteunen.

Gerelateerde informatie

- Multicast-routing voor FirePOWER Threat Defense
- <u>Probleemoplossing voor Firepower Threat Defence en ASA Multicast PIM</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.