Firepower威脅防禦IGMP和組播基礎知識故障排除

| 目錄 |
|------------------------------------|
| |
| <u>必要條件</u> |
| |
| 採用元件 |
| <u>背景資訊</u> |
| 設定 |
| IGMP基礎知識 |
| <u>任務1 — 控制平面組播流量</u> |
| 任務2 — 配置基本組播 |
| IGMP窺探 |
| <u>任務3 - IGMP靜態組與IGMP加入組</u> |
| igmp static-group |
| igmp join-group |
| <u>任務4 — 配置IGMP Stub組播路由</u> |
| <u>已知的問題</u> |
| <u>在目的地區域過濾多點傳送流量</u> |
| 超過IGMP介面限制時,防火牆會拒絕IGMP報告 |
| <u>防火牆忽略232.x.x.x/8地址範圍的IGMP報告</u> |
| 相關資訊 |

簡介

本檔案介紹多點傳送的基礎知識和Firepower威脅防禦(FTD)如何實施網際網路群組管理通訊協定 (IGMP)。

必要條件

需求

基本IP路由知識。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

本文內容也適用於自適應安全裝置(ASA)軟體。

本文中的資訊係根據以下軟體和硬體版本:

- Cisco Firepower 4125威脅防禦版本7.1.0。
- Firepower管理中心(FMC)版本7.1.0。
- ASA版本9.19.1。

背景資訊

定義

- 單播=從一台主機到另一台主機(一對一)。
- 廣播=從一台主機到所有可能的主機(一對全)。
- 組播=從一組主機的主機到一組主機(一對多或多對多)。
- 任播=從主機到組的最近主機(一對多對一)。

基礎知識

- 組播RFC 988由Steve Deering於1986年編寫。
- IPv4多點傳送使用範圍224.0.0.0/4(前4位1110) --- 224.0.0.0 239.255.255.255。
- 對於IPv4,第2層MAC地址來自第3層組播IP:01005e(24位)+25^{位(}always 0 + 23位組播 IPv4地址的更低位)。
- IPv6多點傳送使用FF00::/8範圍,比IPv4多點傳送更靈活,因為它可以嵌入集結點(RP)IP。
- 對於IPv6,第2層MAC地址來自第3層組播:3333+32位組播IPv6地址的更低位。
- 組播的優勢:由於源上的負載減少,效率提高。效能,因為它避免了流量重複或泛洪。
- 組播的缺點:傳輸不可靠(基於UDP)、無擁塞規避、傳送順序不當。
- 公共Internet不支援組播,因為它需要路徑中的所有裝置來啟用組播。通常在所有裝置都處於 公共管理許可權下時使用。
- 典型組播應用:內部影片流、視訊會議。

多點傳送與複製的單點傳送

在複製單播中,源建立同一單播資料包(複製副本)的多個副本,並將它們傳送到多個目標主機。 組播將負擔從源主機轉移到網路,而在複製單播中,所有工作都在源主機上完成。

設定

IGMP基礎知識

- IGMP是組播接收器和本地L3裝置(通常為路由器)之間的「語言」。
- IGMP是第3層通訊協定(類似ICMP),並使用IP通訊協定編號2。
- 目前有3個IGMP版本。防火牆上的預設IGMP版本是版本2。目前僅支援版本1和2。
- IGMPv1和IGMPv2之間的主要差異如下:
 - IGMPv1沒有離開組消息。
 - IGMPv1沒有特定於組的查詢(當主機離開組播組時防火牆使用)。

• IGMPv1沒有查詢器選擇過程。

- ASA/FTD目前不支援IGMPv3,但作為參考,IGMPv2和IGMPv3之間的重要區別在於在 IGMPv3中包含一個源和組特定查詢,該查詢用於源特定多點傳送(SSM)。
- IGMPv1/IGMPv2/IGMPv3查詢= 224.0.0.1
 IGMPv2離開= 224.0.0.2
 IGMPv3成員報告= 224.0.0.22
- 如果主機要加入,可以傳送未經請求的IGMP成員報告消息:

| <u>File</u> | dit <u>V</u> iew <u>G</u> o <u>C</u> apture An | alyze Statistics Tel | ephony Wireless Tools | Help | | | | |
|-----------------------|--|----------------------|-----------------------|-----------------|----------|-----|----------------|--|
| A . E . | | 부부절 속 오. | ् 📃 व व व 🔟 | | | | | |
| igmp | | | | | | | | |
| No. | Time | Delta | Source | Destination | Protocol | SGT | Identification | Length Info |
| | 7 5.118518 | 0.0000 | 00 192.168.1.50 | 224.0.0.2 | IGMPv2 | | 0x01a7 (423) | 46 Leave Group 230.10.10.10 |
| | 8 5.127230 | 0.0087 | 12 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x01a8 (424) | 46 Membership Report group 230.10.10.10 |
| | 9 5.593022 | 0.4657 | 92 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x01a9 (425) | 46 Membership Report group 230.10.10.10 |
| | 114 74.756894 | 69.1638 | 72 192.168.1.24 | 224.0.0.1 | IGMPv2 | | 0x7280 (29312) | 60 Membership Query, general |
| | 118 77.093155 | 2.3362 | 51 192.168.1.50 | 239.255.255.250 | IGMPv2 | | 0x01e9 (489) | 46 Membership Report group 239.255.255.250 |
| | 120 79.593298 | 2.5001 | 43 192.168.1.50 | 224.0.0.252 | IGMPv2 | | 0x01eb (491) | 46 Membership Report group 224.0.0.252 |
| | 122 81.093367 | 1.5000 | 59 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x01ec (492) | 46 Membership Report group 230.10.10.10 |
| | 152 103.150111 | 22.05674 | 44 192.168.1.24 | 224.0.0.1 | IGMPv2 | | 0x1c5f (7263) | 60 Membership Query, general |
| | 153 103.593643 | 0.4435 | 32 192.168.1.50 | 224.0.0.252 | IGMPv2 | | 0x0206 (518) | 46 Membership Report group 224.0.0.252 |
| | 154 104.593737 | 1.0000 | 94 192.168.1.50 | 239.255.255.250 | IGMPv2 | | 0x0208 (520) | 46 Membership Report group 239.255.255.250 |
| | 161 107.686998 | 3.0932 | 51 192.168.1.50 | 224.0.0.2 | IGMPv2 | | 0x020b (523) | 46 Leave Group 230.10.10.10 |
| | 162 107.687972 | 0.0009 | 74 192.168.1.24 | 230.10.10.10 | IGMPv2 | | 0x9b9d (39837) | 60 Membership Query, specific for group 230.10.10.10 |
| | 163 107.695137 | 0.0071 | 65 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x020c (524) | 46 Membership Report group 230.10.10.10 |
| | 164 108.093934 | 0.3987 | 97 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x020e (526) | 46 Membership Report group 230.10.10.10 |

- 從防火牆的角度來看,IGMP查詢有兩種型別:常規查詢和組特定查詢
- 當防火牆收到IGMP離開組消息時,它必須檢查該組在子網中是否有其他成員。因此,防火牆 會傳送一個群組特定查詢:

Eile Edit View Go Capture Analyze Statistics Telephony Wireless Iools Help

| | u 🛯 📮 🗆 🗖 💌 🖪 🔶 | 7 H X X 🖂 | | | | | | |
|--------|-----------------|-----------|--------------|-----------------|----------|-----|----------------|--|
| 📕 igmp | | | | | | | | |
| No. | Time | Delta | Source | Destination | Protocol | SGT | Identification | Length Info |
| | 7 5.118518 | 0.00000 | 192.168.1.50 | 224.0.0.2 | IGMPv2 | | 0x01a7 (423) | 46 Leave Group 230.10.10.10 |
| | 8 5.127230 | 0.008712 | 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x01a8 (424) | 46 Membership Report group 230.10.10.10 |
| | 9 5.593022 | 0.465792 | 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x01a9 (425) | 46 Membership Report group 230.10.10.10 |
| | 114 74.756894 | 69.163872 | 192.168.1.24 | 224.0.0.1 | IGMPv2 | | 0x7280 (29312) | 60 Membership Query, general |
| | 118 77.093155 | 2.336261 | 192.168.1.50 | 239.255.255.250 | IGMPv2 | | 0x01e9 (489) | 46 Membership Report group 239.255.255.250 |
| | 120 79.593298 | 2.500143 | 192.168.1.50 | 224.0.0.252 | IGMPv2 | | 0x01eb (491) | 46 Membership Report group 224.0.0.252 |
| | 122 81.093367 | 1.500069 | 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x01ec (492) | 46 Membership Report group 230.10.10.10 |
| | 152 103.150111 | 22.056744 | 192.168.1.24 | 224.0.0.1 | IGMPv2 | | 0x1c5f (7263) | 60 Membership Query, general |
| | 153 103.593643 | 0.443532 | 192.168.1.50 | 224.0.0.252 | IGMPv2 | | 0x0206 (518) | 46 Membership Report group 224.0.0.252 |
| | 154 104.593737 | 1.000094 | 192.168.1.50 | 239.255.255.250 | IGMPv2 | | 0x0208 (520) | 46 Membership Report group 239.255.255.250 |
| | 161 107.686998 | 3.093261 | 192.168.1.50 | 224.0.0.2 | IGMPv2 | | 0x020b (523) | 46 Leave Group 230.10.10.10 |
| | 162 107.687972 | 0.000974 | 192.168.1.24 | 230.10.10.10 | IGMPv2 | | 0x9b9d (39837) | 60 Membership Query, specific for group 230.10.10.10 |
| | 163 107.695137 | 0.007165 | 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x020c (524) | 46 Membership Report group 230.10.10.10 |
| | 164 108.093934 | 0.398797 | 192.168.1.50 | 230.10.10.10 | IGMPv2 | | 0x020e (526) | 46 Membership Report group 230.10.10.10 |

• 在有多個路由器/防火牆的子網上,選擇querier(傳送所有IGMP查詢的裝置):

<#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

• 在FTD上(類似於傳統ASA),您可以啟用debug igmp以檢視與IGMP相關的消息:

<#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

• 主機通常使用離開組消息(IGMPv2)離開組播組。

| <u>F</u> ile | <u>E</u> dit <u>V</u> iev | v <u>G</u> o <u>C</u> apture | Analyze Statistics | Telephony <u>W</u> ireless | <u>T</u> ools <u>H</u> elp | | | | |
|--------------|---------------------------|--------------------------------|---------------------------------|--|---------------------------------------|------------------------------|--|--------------------|--|
| | 20 | 1 🖹 🖹 | ۹ 🔶 🚔 🗧 | 🛓 📃 📃 ભ્ ભ્ | Q. 🎹 | | | | |
| 📕 igm | p.type == 0 | x17 | | | | | | | |
| No. | | Time | Delta | Source | Destination | Protocol | Identification | Length | Info |
| | 7 | 5.118518 | 0.000000 | 192.168.1.50 | 224.0.0.2 | IGMPv2 | 0x01a7 (423) | 46 | Leave Group 230.10.10.1 |
| | 161 | 107.686998 | 102.568480 | 192.168.1.50 | 224.0.0.2 | IGMPv2 | 0x020b (523) | 46 | Leave Group 230.10.10.1 |
| No. | 7 | Time 5.118518 107.686998 | Delta 0.000000 102.568480 | Source 192.168.1.50 192.168.1.50 | Destination 224.0.0.2 224.0.0.2 | Protocol IGMPv2 IGMPv2 | Identification 0x01a7 (423) 0x020b (523) | Length 46 46 | Info Leave Group 230.10. Leave Group 230.10. |

任務1 — 控制平面組播流量

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

在FTD和ASA之間配置OSPFv2和OSPFv3。檢查2台裝置如何處理OSPF生成的L2和L3組播流量。

解決方案

OSPFv2配置

| Firewall Management Center Devices / NGFW Routing | r Overview Ar | nalysis Policies Devi | ices Objects II | ntegration | | Deploy | ९ 🗳 🔅 🛛 | ▼ sthate SECU |
|--|----------------------|--|----------------------|------------|----------------|--------|---------|---------------|
| FTD4125-1 | | | | | | | | Save |
| Cisco Firepower 4125 Threat Defense | | | | | | | | |
| Device Routing Interfaces Inli | ne Sets DHCP | | | | | | | |
| Manage Virtual Routers | cess 1 | ID: 1 | | | | | | |
| Global OSPF R | ole: | _ | | | | | | |
| Interna | al Router | Enter Description here | Advanc | ced | | | | |
| Virtual Router Properties | cess 2 | ID: | | | | | | |
| ECMP | | | | | | | | |
| OSPF R | ble: | Esta Description have | | | | | | |
| OSPFv3 | | Enter Description here | Advanc | | | | | |
| EIGRP | | | | | | | | |
| RIP | Redistribution Inter | Area Filter Rule Sum | mary Address Interfa | ace | | | | |
| Policy Based Routing | | | | 1 | | | | + Add |
| ✓ BGP OSPF | Process Area ID | Area Type | Networks | Options | Authentication | Cost | Range | Virtual-Link |
| IPv4 | | | | | | | | |
| IPv6 | 0 | normal | net_192.168.103.0 | false | none | | -9 | e /1 |
| | | | | | | | | |

| Device Routing Interface | s Inline Sets DHCI | 2 | | | | | | |
|---------------------------|---------------------|-----------------------------|----------------------|---------------|----------|------------|-----------------|----------|
| Manage Virtual Routers | Process 1 | ID: 1 | | | | | | |
| | OSPF Role: | | | | | | | |
| Global 👻 | Internal Router | Enter D | escription here | Advanced | | | | |
| Virtual Router Properties | - D D | 10: | | | | | | |
| ECMP | Process 2 | ID: | | | | | | |
| OSPF | OSPF Role: | | | | | | | |
| OSPFv3 | Internal Router | ▼ Enter D | escription here | Advanced | | | | |
| EIGRP | | | | | | | | |
| RIP | Area Redistribution | InterArea Filte | r Rule Summary Addre | ess Interface | | | | |
| Policy Based Routing | | | | | | | | |
| ∨ BGP | Interface | Authentication | Point-to-Point | Cost | Priority | MTU Ignore | Database Filter | Neighbor |
| IPv4 | OUTSIDE | Nees | false | 10 | | false | false | |
| IPv6 | OUTSIDE | None | raise | 10 | 1 | raise | raise | / |

類似地,對於OSPFv3

FTD CLI上的組態:

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

此組態在FTD加速安全路徑(ASP)允許表中建立這些專案,以便入口多點傳播流量不會受到封鎖:

<#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</pre>

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 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</pre>

dst ip/id=224.0.0.6, mask=255.255.255.255

, port=0, tag=any, dscp=0x0, nsg_id=none <-- OSPF for IPv4

input_ifc=OUTSIDE

對於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</pre>

dst ip/id=ff02::5/128

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

input_ifc=OUTSIDE

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

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>
```

OSPFv2和OSPFv3鄰接關係已啟動:

<#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

以下是終止到該盒的組播OSPF會話:

<#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

作為測試,啟用IPv4捕獲並清除與裝置的連線:

<#root>

firepower#

capture CAP interface OUTSIDE trace

firepower#

clear conn all

12 connection(s) deleted.
firepower#

clear capture CAP

firepower# !



捕獲的OSPF資料包:

<#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]

以下是防火牆處理OSPFv2多點傳送封包的方式:

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

以下是防火牆處理OSPFv3多點傳送封包的方式:

<#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: MAC Access list 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 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

任務2 — 配置基本組播

拓撲



需求

配置防火牆,以便將來自伺服器的組播流量流傳輸到IP 230.10.10.10上的組播客戶端

解決方案

從防火牆的角度來看,最低配置是啟用全域性組播路由。這將在所有防火牆介面上啟用後台的 IGMP和PIM。

在FMC UI上:

| Firewall Management Center Overview An Devices / NGFW Routing | alysis Policies Devices Obje | cts Integration | Deploy |
|--|--|--|--------------------|
| FTD4125-1 Cisco Firepower 4125 Threat Defense Device Routing Interfaces Inline Sets DHCP | | | |
| Manage Virtual Routers Protocol Neighbor Filter | ng Multicast Routing checkbox will enable bo Bidirectional Neighbor Filter Rendezvous | oth IGMP and PIM on all Interfaces.) s Points Route Tree Request Filter | r Bootstrap Router |
| Virtual Router Properties | DIM Enabled | DD Driarity | Hallo Interval |
| OSPF OSPFv3 | PIM Enabled | No records to display | |
| EIGRP RIP | | | |
| Policy Based Routing V BGP IPv4 | | | |
| IPv6 Static Route | | | |
| V Multicast Routing IGMP | | | |

在防火牆CLI上,這是推送的配置:

<#root>

firepower#

show run multicast-routing

multicast-routing

<-- Multicast routing is enabled

IGMP驗證

```
<#root>
firepower#
 show igmp interface
diagnostic is up, line protocol is up
 Internet address is 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 | < IGMP Reports received and sent |
| 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 | | |

PIM驗證

<#root>

firepower#

show pim interface

| Address | Interface | PIM Nb Coun | or Hell t 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驗證
```

```
<#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 seco
(*,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
```

通過防火牆的組播流量

Multicast Source FTD **Multicast Receiver** H₂ (server) H1 (client) 1 230.10.10.10 192.168.1.x/24 192.168.103.x/24 .60 .91 .24 .50 Po1.205 E1/4 INSIDE OUTSIDE

在此案例中,VLC媒體播放器應用程式用作多點傳送伺服器和使用者端,以測試多點傳送流量:

VLC多點傳送伺服器組態:



| Open Me | dia | | | |
|-------------------|-----------------|--------------------------------------|--|----------------------|
| File | 🕖 Disc | e wetwork | Scapture Device | |
| File Sele | ction | | | 1 |
| You can C:\Use | select local fi | es with the follow deos\Sample Vi | ing list and buttons. deos\Wildlife.wmv 2 | Add Remove |
| Use a | a subțitle file | | | Browse |
| | | | | |
| | | | | |
| Show mo | re options | | | 3 Stream ▼ Cancel |

在下一個螢幕上,選擇Next。

選擇格式:

| tination Setup elect destinations to stream to | | |
|---|---|---|
| • | | |
| | | |
| | | |
| Add destinations following the | streaming methods you need. Be sure to check with transcoding that | the format is compatible with the |
| Add destinations following the method used. | streaming methods you need. Be sure to check with transcoding that | the format is compatible with the |
| Add destinations following the method used. | streaming methods you need. Be sure to check with transcoding that | the format is compatible with the |
| Add destinations following the method used. | streaming methods you need. Be sure to check with transcoding that 1 RTP / MPEG Transport Stream | the format is compatible with the 2 Add |

指定組播IP和埠:

| 🛓 Stream Outpu | t | | | | | ? 🗙 |
|------------------------------------|---------------------------|-------------------|------------------|------|------|--------|
| Destination Sel Select destinat | tup tions to stream to | | | | | |
| • | RTP/TS 🔀 | | | | | |
| This module | outputs the transco | ded stream to a r | network via RTP. | | | |
| Address Base port | 230.10.10.10 | 1 | | | | |
| Stream nam | e | | | | | |
| | | | | Back | Next | Cancel |

| 🛓 Stream Output | | | ? 💌 |
|--|----------------------------|-----------|---|
| Transcoding Options Select and choose transcoding options | | | |
| Activate Transcoding | | | |
| Profile | Video - H. 264 + MP3 (MP4) | - 🕅 🗸 | Image: Image: Image |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Back Next | Cancel |

在FTD防火牆上啟用LINA擷取:

<#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

為裝置選擇Stream按鈕以啟動組播流:

| 🛓 Stream Output | ? 💌 |
|---|--------------|
| Option Setup Set up any additional options for streaming | |
| Miscellaneous Options Stream all elementary streams | |
| Generated stream output string | |
| <pre>:sout=#transcode(vcodec=h264,acodec=mpga,ab=128,channels=2,samplerate=44100):rtp{dst=230.10.10.10,port= } :sout-all :sout-keep</pre> | ·S004,mux=ts |
| Back Stream | Cancel |

啟用「loop」選項,以便連續傳送流:



驗證(非操作方案)

此方案演示了一個非操作方案。目標是演示防火牆行為。

防火牆裝置會收到組播流,但不會轉發它:

<#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</pre>

防火牆LINA ASP丟棄顯示:

<#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) 2
FP L2 rule drop (12_acl) 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</pre>

要跟蹤資料包,需要捕獲組播流的第一個資料包。因此,請清除當前流量:

<#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 「detail」選項顯示組播MAC地址:

<#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 (tt] 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 (tt] 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 (tt] 100, id 19761)
...

實際封包的追蹤軌跡顯示封包允許通過,但實際發生的情況並非如此:

<#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

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

根據mroute和mfib計數器,由於傳出介面清單(OIL)為空,因此丟棄了資料包:

<#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

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 MFIB計數器顯示RPF失敗,在這種情況下,並非實際發生的情況: <#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 「show mfib count」輸出中的類似RPF失敗:

<#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 /0 <-- Allowed and dropped multicast packets</pre> Tot. shown: Source count: 1, pkt count: 0 Group: 232.0.0/8 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

設定VLC多點傳送接收器:

| 🛓 v | LC media player | | | | |
|-------|------------------------------|----------|--------|------|------|
| Mec | lia 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 | 6 | | |
| | Open Network Stream | Ctrl+N | I | | |
| 5 | Open Capture Device | Ctrl+C | 2 | | |
| | Open Location from clipboard | Ctrl+V | | | |
| | Open Recent Media | | ÷ | | |
| | Save Playlist to File | Ctrl+Y | 9 | | |
| | Convert / Save | Ctrl+R | 5 | | |
| ((*)) | Stream | Ctrl+S | | | |
| | Quit at the end of playlist | | | | |
| | Quit | Ctrl+Q | 2 | | |
| | | | | | |

指定組播源IP並選擇播放:



在後端中,只要選擇播放,主機就會宣佈願意加入特定組播組並傳送IGMP報告消息:



如果啟用調試,可以看到IGMP報告消息:

<#root>

firepower#

debug igmp group 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</pre>

流開始:



驗證(操作方案)

<#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</pre>

[Buffer Full - 524030 bytes]

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

防火牆的mroute表: <#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</pre>
 OUTSIDE Flags: A
 INSIDE Flags: F NS
   Pkts: 6373/6
mfib計數器:
<#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
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窺探

- IGMP監聽是交換器上使用的一種機制,用於防止多點傳播泛濫。
- 交換機監控IGMP報告,以確定主機(接收器)的位置。
- 交換機監控IGMP查詢,以確定路由器/防火牆(發件人)的位置。
- 大多數思科交換機預設啟用IGMP監聽。有關詳細資訊,請參閱相關交換指南。以下是L3 Catalyst交換器的輸出範例:

<#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 | Interface | Reporter | Uptime | Last-Join | Last-Leave |
|--|--------------|--------------|--------|-----------|------------|
| 0.0.0/230.10.10.10 | V1204:Gi1/48 | 192.168.1.50 | 2d13h | - | 2d12h |
| 0.0.0/230.10.10.10 | V1204:Gi1/48 | 192.168.1.97 | 2d13h | 2d12h | - |
| 0.0.0/230.10.10.10 | V1204:Gi2/1 | 192.168.1.50 | 2d10h | 02:20:05 | 02:20:00 |
| 0.0.0/239.255.255.250 | V1204:Gi2/1 | 192.168.1.50 | 2d11h | 02:20:05 | 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:Gi2/1 | 192.168.6.50 | 2d13h | - | 2d13h |
| 0.0.0/224.0.1.40 | V1204:Gi2/26 | 192.168.2.1 | 2d14h | 00:00:39 | 2d13h |
| Snooping statistics for Vlan #channels: 4 #hosts : 3 | 206 | | | | |
| Source/Group | Interface | Reporter | Uptime | Last-Join | Last-Leave |

| Source/Group | Interface | Reporter | Uptime | Last-Join | Last-Leave |
|-----------------------|--------------|--------------|----------|-----------|------------|
| 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 | V1206: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 | V1206:Gi2/26 | 192.168.6.1 | 2d13h | 2d13h | - |
| 0.0.0/230.10.10.10 | V1206:Gi2/26 | 192.168.6.91 | 2d13h | - | 2d13h |
| 0.0.0/239.10.10.10 | V1206:Gi2/26 | 192.168.6.1 | 2d14h | 2d14h | - |
| 0.0.0/239.10.10.10 | V1206:Gi2/26 | 192.168.6.91 | 2d14h | - | 2d14h |

任務3 - IGMP靜態組與IGMP加入組

概觀

| | ip igmp static-group | ip igmp join-group |
|----------------------------|---|---|
| 是否應用於 FTD介面? | 是 | 是 |
| FTD是否會吸 引多點傳播流 ? | 是,將PIM加入傳送到上游裝置。源裝 置或到集結點(RP)。僅當使用此命令的 FTD是該介面上的PIM指定路由器 (DR)時,才會發生這種情況。 | 是,將PIM加入傳送到上游裝置。源裝置 或到集結點(RP)。僅當使用此命令的 FTD是該介面上的PIM指定路由器(DR)時 ,才會發生這種情況。 |
| FTD是否將多 點傳播流量轉 送出介面? | 是 | 是 |
| FTD會消耗並 回覆多點傳播 流量嗎 | 否 | 是,FTD將多點傳播流傳送到CPU、使用 它,然後回覆來源。 |
| CPU影響 | 最小,因為資料包未傳送到CPU。 | 可影響FTD CPU,因為屬於該組的每個 多點傳送封包都會被傳送到FTD CPU。 |

任務要求

請考慮使用此拓樸:



在防火牆上啟用以下擷取:

<#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. 使用來自第3層交換器的ICMP ping將多點傳播流量傳送到IP 230.11.11.11,並檢查防火牆處 理此問題的方式。
- 2. 在防火牆INSIDE介面上啟用igmp static-group命令,並檢查防火牆如何處理組播流(IP 230.11.11.11)。
- 在防火牆INSIDE介面上啟用igmp static-group命令,並檢查防火牆如何處理組播流(IP 230.11.11.11)。

解決方案

防火牆沒有IP 230.11.11.11的任何路由:

<#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

測試多點傳送的簡單方法是使用ICMP ping工具。在這種情況下,從R2對組播IP地址 230.11.11.11發起ping:

<#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: <#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 防火牆上的擷取顯示: <#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 [Capturing - 0 bytes]

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

防火牆會為每個ping建立連線,但會以靜默方式捨棄封包:

<#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 230.1
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.
May 17 2022 11:05:49: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.1
May 17 2022 11:05:49: %FTD-7-609002:
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 230.1
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.
May 17 2022 11:05:53: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.103.62/6 gaddr 230.11.1
May 17 2022 11:05:53: %FTD-7-609002:
Teardown local-host identity:230.11.11.11 duration 0:00:02
```

```
<-- The connection is closed
```

✎注意:LINA ASP丟棄捕獲不會顯示丟棄的資料包

組播資料包丟棄的主要指示是:

<#root>

firepower#

show mfib

```
(*,224.0.1.40) Flags: S K
Forwarding: 0/0/0/0, Other: 0/0/0
```

```
(192.168.103.62,230.11.11.11)
```

```
Flags: K <-- The multicast stream Forwarding: 0/0/0/0,
```

Other: 27/27/0

<-- The packets are dropped

igmp static-group

在FMC上配置靜態IGMP組:



下面是後台部署的內容:

<#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

ping失敗,但ICMP多點傳播流量現在通過防火牆轉送:

<#root>

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</pre>

<#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

◆ 注意:資料包的跟蹤顯示不正確的輸出(輸入介面與輸出相同)。如需更多詳細資訊,請檢查 Cisco錯誤ID <u>CSCvm89673。</u>

<#root>

firepower#

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

Config:

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

<#root>

L3-Switch#

ping 230.11.11.11 re 500 timeout 0

Type escape sequence to abort. Sending 1000, 100-byte ICMP Echos to 230.11.11.11, timeout is 0 seconds:

<#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 join-group

在FMC遠端交換機上,配置先前配置的靜態組配置並配置IGMP加入組:

| 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 Routers | Enable Multicast Routing (E Protocol Access Group | nabling Multic Static Gro | ast Routing cl oup Join (| heckbox will e Group | nable both IGN | IP and PIM on a | II Interfaces.) |
| Virtual Router Properties | nterface | | | | | | Multicast Group Address |
| OSPF OSPFv3 | NSIDE | | | | | | group_230.11.11.11 |
| EIGRP RIP Policy Based Routing | | | | | | | |
| ∨ BGP IPv4 | | | | | | | |
| IPv6 Static Route | | | | | | | |
| IGMP | | | | | | | |



部署的配置:

<#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

IGMP組:

<#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

在來源主機中,嘗試對230.11.11.11 IP進行第一個ICMP多點傳送測試:

<#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

註:如果您沒有看到所有回覆,請檢查Cisco錯誤ID <u>CSCvm90069。</u>

任務4 — 配置IGMP Stub組播路由



在FTD上設定存根多點傳送路由,以便將INSIDE介面上收到的IGMP成員身份報告訊息轉送到 OUTSIDE介面。

解決方案

| Firewall Management (Devices / NGFW Routing | Center _{Overvi} | ew Analysis | Policies Devices (| Objects Integration | | | |
|--|--------------------------|-------------|--------------------|---------------------|----------------|---------------|--|
| FTD4125-1 Cisco Firepower 4125 Threat Defense Device Routing Interfaces Inline Sets DHCP | | | | | | | |
| Manage Virtual Routers C Enable Multicast Routing (Enabling Multicast Routing checkbox will enable both IGMP and PIM on all Interfaces.) Protocol Access Group Static Group Join Group | | | | | | | |
| Global Virtual Router Properties | | | | | | | |
| ECMP | Interface | Enabled | Forward Interface | Version | Query Interval | Response Time | |
| OSPF | INSIDE | true | OUTSIDE | 2 | | | |
| OSPFv3 | | | | | | | |
| EIGRP | | | | | | | |
| RIP | | | | | | | |
| Policy Based Routing | | | | | | | |
| ∼ BGP | | | | | | | |
| IPv4 | | | | | | | |
| IPv6 | | | | | | | |
| Static Route | | | | | | | |
| ✓ Multicast Routing | | | | | | | |
| IGMP | | | | | | | |

部署的配置:

<#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

驗證

在FTD上啟用擷取:

<#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

驗證

要強制IGMP成員報告,您可以使用類似VLC的應用程式:

| 🚖 Open Media | |
|---|-----------------|
| File Olisc Retwork Capture Device | |
| Network Protocol | |
| Please enter a network URL: | |
| rtp://@230.10.10.10:5004 | • |
| http://www.example.com/stream.avi rtp://@:1234 mms://mms.examples.com/stream.asx rtsp://server.example.org:8080/test.sdp | |
| http://www.yourtube.com/watch?v=gg64x | |
| | |
| | |
| | |
| | |
| | |
| | |
| Show more options | |
| | Stream 👻 Cancel |
| | Enqueue Alt+E |
| | Play Alt+P |
| | Stream Alt+S |
| | Convert Alt+O |

FTD代理IGMP封包:

<#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</pre>

FTD會變更來源IP:

<#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#</pre>

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

如果您在Wireshark中檢查pcap,可以看到該資料包完全由防火牆重新生成(IP標識更改)。

在FTD上建立一個組專案:

<#root>

firepower#

show igmp group

| IGMP Connected Group Membership Group Address Interface | Uptime | Expires | Last Reporter |
|--|------------------------|-----------------|---------------|
| 230.10.10.10 INSIDE | 00:15:22 | 00:03:28 | 192.168.1.50 |
| <pre>< IGMP group is enabled on the ingr 239.255.255.250 INSIDE</pre> | ess interf 00:15:27 | ace 00:03:29 | 192.168.1.50 |

FTD防火牆建立2個控制平面連線:

<#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</pre>

第一個封包的追蹤軌跡:

<#root>

firepower#

show capture CAPI packet-number 1 trace

6 packets captured

1: 12:21:12.820483 802.12 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:

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: 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

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

已知的問題

Time Taken: 154208 ns

在目的地區域過濾多點傳送流量

無法為與組播流量匹配的訪問控制策略規則指定目標安全區域:

| Firewall N Policies / Acc | lanagement C ass Control / Policy I | enter d Editor | Overview | Analysis | Policies | Devices | Objects | Integratio | n | | | Deploy | ۹ (| ¢ 💡 | 🕜 mzaf | eiro \ ad | imin v | -ihah cisco | SEC | URE |
|--|--|-------------------|-----------------|--------------------|----------|---------|---------|------------|-------------------------|------------|------|---------------------------------|-----------------------------|--------------------|---------|-----------|---------------------------|----------------|-----|-----|
| FTD_Access_Control_Policy Enter Description | | | | | | | | el | | | | | | | | | | | | |
| Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy: SSL Policy: None Identity Policy: None | | | | | | | | | t <u>ts (0)</u> Vone | | | | | | | | | | | |
| Misconfiguration! The Dest Zones must be empty! Filter by Device Y Search Rules Y Search Rules Add Category | | | | | | | | | | | | | | | | | | | | |
| II Name | Source Zones | Dest Zones | Source Netwo | e Dest rks Netw | orks VL | AN Tags | Users | Applicati | Source Ports | Dest Ports | URLs | Source Dynamic Attributes | Destina Dynam Attribu | ati lic ites | Action | Po 🖤 | E, / | | 0 = | ٥ |
| V Mandatory - FTD_Access_Control_PC cy (1-1) | | | | | | | | | | | | | | | | | | | | |
| 1 allow_multicast | INSIDE_ZONE | OUTSIDE_ZONE | Any | 224. | 1.2.3 An | ¥. | Any | Any | Any | Any | Any | Any | Any | | C Allow | 15 単 | $B_{0} = \mathcal{J}_{0}$ | | 0 | 11 |
| V Default - FTD_Access_Control_Policy (-) | | | | | | | | | | | | | | | | | | | | |
| There are no rules in this section. Add Rule or Add Category | | | | | | | | | | | | | | | | | | | | |

FMC使用手冊中也有相關說明:

| Book Contents | | C Find Matches in This Book | | | | | |
|--|---|---|--|--|--|--|--|
| Book Title Page | ^ | Internet multicast routing from address range 224.0.0/24 is not supported; IGMP group is not created when enabling multicast routing for the reserved addressess. | | | | | |
| Getting Started with Device Configuration | | Clustering | | | | | |
| > Device Operations | | In clustering, for IGMP and PIM, this feature is only supported on the primary unit. | | | | | |
| \geq Interfaces and Device Settings | | Additional Guidelines | | | | | |
| \sim Routing | | You must configure an access control or prefilter rule on the inbound security zone to allow traffic to the multicast host, such as 224.1.2.3. However, you cannot specify a destination security zone for the rule, or it cannot be applied to | | | | | |
| Static and Default Routes | | multicast connections during initial connection validation. | | | | | |
| Virtual Routers | | • You cannot disable an interface with PIM configured on it. If you have configured PIM on the interface (see Configure | | | | | |
| ECMP | | PIM Protocol), disabling the multicast routing and PIM does not remove the PIM configuration. You must remove (delete) the PIM configuration to disable the interface. | | | | | |
| 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 Hop Router. | | | | | |
| RIP | | | | | | | |
| Multicast | | Configure IGMP Features | | | | | |
| Policy Based Routing | | IP hosts use IGMP to report their group memberships to directly-connected multicast routers. IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP | | | | | |

超過IGMP介面限制時,防火牆會拒絕IGMP報告

預設情況下,防火牆允許介面上最多有500個當前活動聯接(報告)。如果超出此閾值,防火牆將 忽略來自組播接收器的其他傳入IGMP報告。

要檢查IGMP限制和活動聯接,請運行命令show igmp interface nameif:

<#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)

IGMP debug指令debug igmp 顯示以下輸出:

<#root>

asa#

debug igmp

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



修正了思科錯誤ID <u>CSCvw60976的軟體版本</u> 允許使用者為每個介面配置最多5000個組。

防火牆忽略232.x.x.x/8地址範圍的IGMP報告

232.x.x.x/8位址範圍用於來源特定多點傳送(SSM)。防火牆不支援PIM源特定組播(SSM)功能和相關 配置。

IGMP debug指令debug igmp 顯示以下輸出:

<#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

思科錯誤<u>ID CSCsr53916</u>



跟蹤增強功能以支援SSM範圍。

相關資訊

- <u>適用於Firepower威脅防禦的多點傳送路由</u>
- 排除Firepower威脅防禦和ASA組播PIM故障

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。