Dépannage de la suppression de paquets multidiffusion via des membres de pont sans nom BVI if

Table des matières

Problème

Les paquets de multidiffusion via les interfaces membres du groupe de pontage sont abandonnés sur le pare-feu avec les symptômes suivants :

1. Les paquets de multidiffusion ne quittent pas l'interface de sortie prévue :

<#root>

```
firewall#

show bridge-group


Static mac-address entries:  0 (in use), 16384 (max)
Dynamic mac-address entries: 2 (in use), 16384 (max)


 Bridge Group: 100


 Interfaces:

 GigabitEthernet0/2



 GigabitEthernet0/3


firewall#

show nameif
```

```
Interface                Name                    Security
..

GigabitEthernet0/2       inside                  100



GigabitEthernet0/3       outside                 0



firewall#

show capture


capture capi type raw-data trace interface inside[

Capturing - 15642 bytes

]
  match udp any host 239.1.1.1
capture capo type raw-data interface outside [

Capturing - 0 bytes

]
  match udp any host 239.1.1.1
```

2. Les octets dans le résultat de la commande show conn appropriée sont 0 :

<#root>

```
firewall#

show conn address 239.1.1.1


16 in use, 17 most used

UDP inside  192.0.2.1:50609 outside  239.1.1.1:5555, idle 0:01:03,

bytes 0

, flags -
```

3. L’interface entrante S, G mroute est nulle :

<#root>

```
firewall#
```

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

(*, 239.1.1.1), 3d01h/never, RP 198.51.100.100, flags: SCJ
  Incoming interface: rp
  RPF nbr: 198.51.100.100
  Immediate Outgoing interface list:
    outside, Forward, 3d01h/never

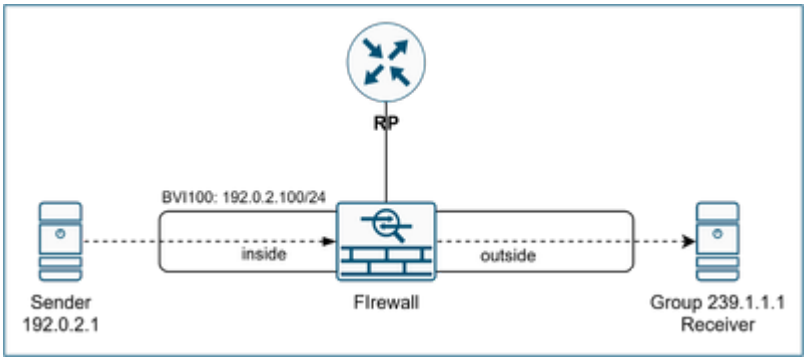
(192.0.2.1, 239.1.1.1), 00:02:48/00:00:41, flags: SJ
```

Incoming interface: Null

```
  RPF nbr: 0.0.0.0
  Inherited Outgoing interface list:
    outside, Forward, 3d01h/never
```

Environnement

Topologie



- Firepower 4115 exécutant Secure Firewall Threat Defense, d'autres plates-formes

matérielles et Security ASA peut être affecté.

- FTD version 7.6.4 et d'autres versions logicielles peuvent être affectées.
- Le routage multidiffusion avec le mode intermédiaire PIM (Protocol Independent Multicast) est activé.
- Le chemin du trafic multidiffusion passe par les membres du groupe de ponts.
- L'interface virtuelle de pont (BVI) n'a pas de nom si.

<#root>

```
firewall#

show bridge-group


Static mac-address entries:  0 (in use), 16384 (max)
Dynamic mac-address entries: 2 (in use), 16384 (max)


 Bridge Group: 100


 Interfaces:

 GigabitEthernet0/2



 GigabitEthernet0/3



firewall#

show nameif


Interface                Name                    Security
..

GigabitEthernet0/2       inside                    100



GigabitEthernet0/3       outside                   0



firewall#
```

show run int bvi100

interface BVI100

no nameif

```
security-level 0
ip address 192.0.2.100 255.255.255.0
```

Résolution

Analyse

1. Augmentation du compteur d'autres abandons MFIB (Multicast Forwarding Information Base) :

<#root>

```
firewall#
```

show mfib 239.1.1.1

```
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

(*,239.1.1.1) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
   rp Flags: A NS
   outside Flags: F NS
     Pkts: 0/0
(192.0.2.1,239.1.1.1) Flags: K
   Forwarding: 0/0/0/0
```

, Other: 2620/0/2620

```
   OBNS-FWinside Flags: A
```

```
   outside Flags: F NS
     Pkts: 0/0

firewall#
```

show mfib 239.1.1.1

```
…
(192.0.2.1,239.1.1.1) Flags: K
   Forwarding: 0/0/0/0,
```

Other: 2629/0/2629

```
   rp Flags: A
   outside Flags: F NS
     Pkts: 0/0
```

2. Les débogages de paquets MFIB indiquent des abandons de paquets de multidiffusion :

<#root>

```
firewall#
```

debug mfib pak 239.1.1.1

```
MFIB IPv4 pak debugging enabled
  all MFIB debugging is for 239.1.1.1
```

MFIB: Pkt (192.0.2.1,239.1.1.1) from inside (PS) dropping

MFIB: Pkt (192.0.2.1,239.1.1.1) from inside (PS) dropping

3. Le résultat de la commande debug pim montre que la recherche RPF a échoué pour les messages racine 192.0.2.1 :

<#root>

```
firewall#
```

debug pim

```
IPv4 PIM:    RPF lookup failed for root 192.0.2.1
IPv4 PIM:    RPF lookup failed for root 192.0.2.1
```

4. PIM est activé sur les membres du groupe de ponts :

<#root>

```
firewall#
```

show pim interface

```
Address          Interface          PIM  Nbr   Hello  DR         DR
                                         Count Intvl  Prior

239.1.1.1        inside             on   0     30     1          this system

239.1.1.1        outside            on   0     30     1          this system
```

Les membres du groupe de ponts ne doivent pas participer aux protocoles de routage multidiffusion. Ce problème est suivi dans l'ID de bogue Cisco : CSCwv2349. La solution de contournement consiste à ajouter le nom if à l'interface BVI, puis à supprimer/ajouter à nouveau le nom d'interface membre du pont if. La suppression des noms a un impact et la discrétion de l'utilisateur est conseillée. Cette modification est recommandée uniquement pendant une fenêtre de maintenance contrôlée.

Motif

En raison de l'ID de bogue Cisco : CSCwv23349, si l'interface BVI n'a pas de nom if, les membres du groupe de pontage participant aux protocoles de routage multidiffusion (c'est-à-dire PIM et IGMP) sont activés sur ces interfaces. L'activation du protocole de routage multidiffusion entraîne l'application de tous les contrôles au niveau du protocole, dont le contrôle RPF (reverse path forwarding).

Le contrôle RPF compare l'interface d'entrée de multidiffusion (A) à l'interface vers l'expéditeur de multidiffusion selon la table de monodiffusion (B). Si les interfaces ne correspondent pas, les

paquets de multidiffusion sont abandonnés en raison d'une défaillance RPF. Dans ce cas, l'interface d'entrée est à l'intérieur. Dans la table de routage, il n’existe pas de route de monodiffusion vers l’expéditeur de multidiffusion avec l’adresse IP : 192.0.2.1 .

```
<#root>

firewall#

show route 192.0.2.1



% Network not in table

firewall#

show asp table routing address 192.0.2.1


route table timestamp: 46
```

Étant donné que les membres du groupe de raccordements ne participent pas au routage, les tables de routage ne disposent pas de routes sur les membres du groupe de raccordements. Cela entraîne des échecs de vérification RPF si les membres du groupe de pontage participent aux protocoles de routage. Les versions avec le correctif de l'ID de bogue Cisco : CSCwv2349 exempte ces interfaces des protocoles de routage multidiffusion.

Avertissement : Ce défaut concerne spécifiquement la participation des membres du groupe de pontage aux protocoles de routage multidiffusion. Elle ne s'applique pas à la multidiffusion immédiate via les membres du groupe de pontage, c'est-à-dire la connectivité multidiffusion entre les périphériques en amont et en aval.

Autres informations utiles

- ID de bogue Cisco CSCwv23349

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.