Comprendre la synchronisation des tables MAC haute disponibilité ASA en mode transparent avec les routeurs HSRP

Contenu

Introduction

Ce document décrit le comportement d'une paire d'ASA connectés à un cluster de routeurs qui utilisent HSRP.

Conditions préalables

- Appareil de sécurité adaptatif (ASA)
- Haute disponibilité ASA (HA).
- Protocole HSRP (Hot Standby Router Protocol) .
- Pare-feu en mode transparent.

Components Used

- 2 routeurs CSR avec HSRP.
- 2 ASA configuré dans HA qui pointe vers la paire HSRP.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

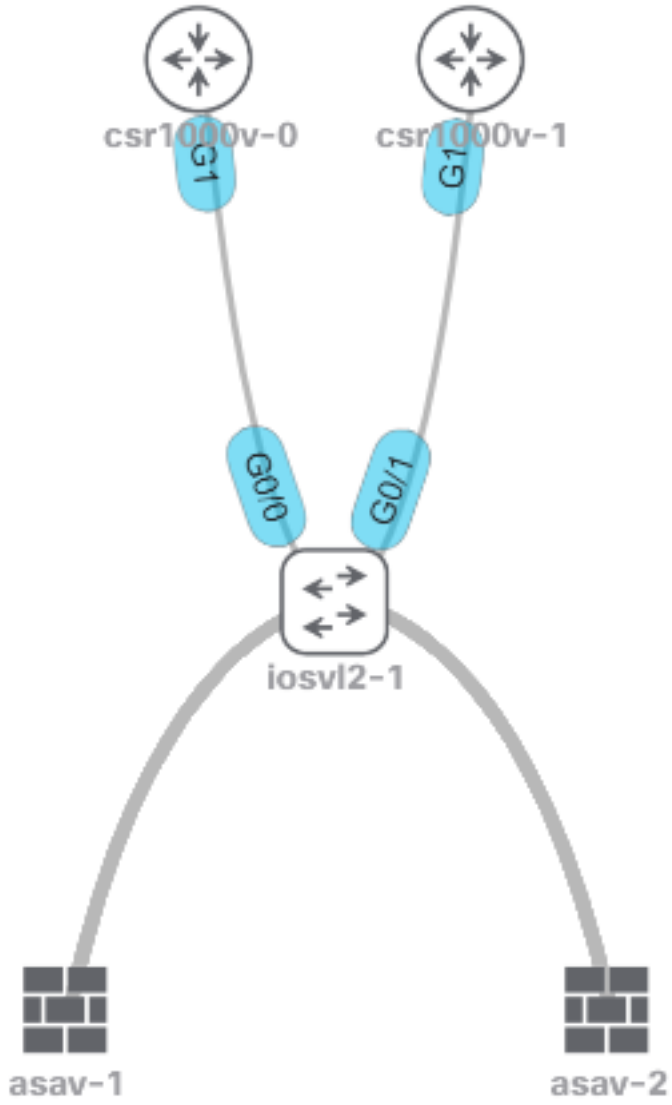
Informations générales

Pour une paire d'ASA configurée en mode transparent Haute disponibilité, si la paire de pare-feu est connectée en amont à un cluster de routeurs et que ces routeurs adjacents utilisent le protocole HSRP, le trafic des pare-feu est destiné à l'adresse IP du routeur qui pointe également vers l'adresse MAC d'un routeur spécifique. Cependant, si le trafic de retour provient de l'adresse

MAC d'une autre interface de routeur dans la paire HSRP, il peut provoquer une panne réseau.

Le problème est que le délai d'expiration de la table d'adresses MAC est de 5 minutes (300 secondes) et que le délai d'expiration du protocole ARP (Address Resolution Protocol) est de 14400 secondes par défaut. Étant donné que le routeur de tronçon suivant utilise HSRP, il n'y a jamais de trafic provenant de l'adresse MAC HSRP. Si cela se produit, l'entrée mac-address-table sur l'ASA expire et le trafic échoue.

Diagramme du réseau



Dépannage

Comprendre la synchronisation de la table MAC pour ASA HA en mode transparent avec HSRP

Ces résultats montrent comment les unités ASA synchronisent leur table MAC lorsque l'unité active apprend de nouvelles entrées et supprime les anciennes.

L'unité active **asav-1** perd l'adresse MAC **5254.0017.8a8c** de l'un des routeurs HSRP, dans ce

cas, csr1000v-0.

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
inside 5254.001f.dfa8 dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

Vous pouvez voir comment 5254.0017.8a8c disparaît après 5 minutes.

```
ASAv-primary# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------
----
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

L'unité en veille ne perd pas l'entrée MAC 5254.0017.8a8c. Ce comportement peut causer de la confusion, cependant, il est tout à fait prévu.

L'unité en veille ne met pas à jour la table d'adresses MAC, sauf si elle devient la nouvelle unité active.

L'unité en veille conserve 5254.0017.8a8c après plusieurs heures et reste à une (1) minute de l'âge temps tout le temps.

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

Vous pouvez attendre des heures/jours et exécuter la même commande et voir le même résultat.

```
ASAv-secondary(config)# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------
----
outside 5254.0017.8a8c dynamic 1 1
outside 5254.0008.7242 dynamic 5 1
outside 0000.0c07.ac01 dynamic 5 1
```

En outre, si vous émettez le **show failover** , il n'y a aucune modification sur le compteur L2BRIDGE Tbl lorsque l'unité active perd l'entrée HSRP.

```
Stateful Failover Logical Update Statistics
Link : failoverlink GigabitEthernet0/3 (up)
Stateful Obj xmit xerr rcv rerr
```

```
General 86751 0 77968 8
sys cmd 77854 0 77853 0
up time 0 0 0 0
RPC services 0 0 0 0
<--- More --->

TCP conn 0 0 0 0
UDP conn 8882 0 90 0
ARP tbl 4 0 1 0
L2BRIDGE Tbl 3 0 22 0
Xlate_Timeout 0 0 0 0
IPv6 ND tbl 0 0 0 0
SIP Session 0 0 0 0
SIP Tx 0 0 0 0
SIP Pinhole 0 0 0 0
Route Session 8 0 0 8
```

La table d'adresses MAC expire en raison du routage asymétrique

Lorsque le trafic circule directement entre deux adresses MAC via le pare-feu transparent, ces adresses ne expirent pas pendant que le trafic circule, car l'ASA reçoit des trames provenant des deux adresses MAC qui envoient le trafic.

Lorsque le flux de trafic est asymétrique, l'entrée expire si l'ASA ne reçoit pas de réponse de cette adresse MAC spécifique.

> **Note**: Le routage asymétrique signifie que l'ASA voit le trafic destiné à une adresse MAC spécifique, mais pas le trafic provenant de cette même adresse MAC

Les symptômes de ce problème sont qu'après l'expiration de l'entrée d'adresse MAC par l'ASA (après 5 minutes sans trafic provenant de cette adresse MAC), le trafic destiné à cette adresse MAC est abandonné jusqu'à ce que l'entrée MAC soit remplie à nouveau.

Généralement, le problème se présente lorsqu'il montre que la connectivité à un serveur est rétablie après une ou deux tentatives, et ceci parce que le premier paquet est abandonné afin que l'ASA puisse passer par les étapes pour apprendre l'emplacement d'une adresse MAC.

Solution suggérée

Afin de résoudre ce problème, ajoutez une table d'entrées d'adresses MAC statiques pour l'IP HSRP sur le pare-feu, ou augmentez le temps d'âge à une certaine valeur de sorte qu'une réponse ARP vienne du routeur HSRP correspondant avant que l'entrée expire.

La meilleure solution consiste à ajouter une entrée MAC statique car il n'est pas sûr que l'ASA reçoive une réponse ARP du routeur actif HSRP.

Informations connexes

- Support et documentation techniques - Cisco Systems

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.