# Inzicht in ASA MAC-tabelsynchronisatie met hoge beschikbaarheid in Transparent Mode met HSRP-routers

## Inhoud



## Inleiding

Dit document beschrijft het gedrag van een paar ASA's die zijn aangesloten op een groep routers die HSRP gebruiken.

## Voorwaarden

- Adaptieve security applicatie (ASA)
- ASA hoge beschikbaarheid (HA).
- Hot Standby Router Protocol (HSRP).
- Firewall in transparante modus.

### Gebruikte componenten

- 2 CSR-routers met HSRP.
- 2 ASA geconfigureerd in HA die naar het HSRP-paar wijst.

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.

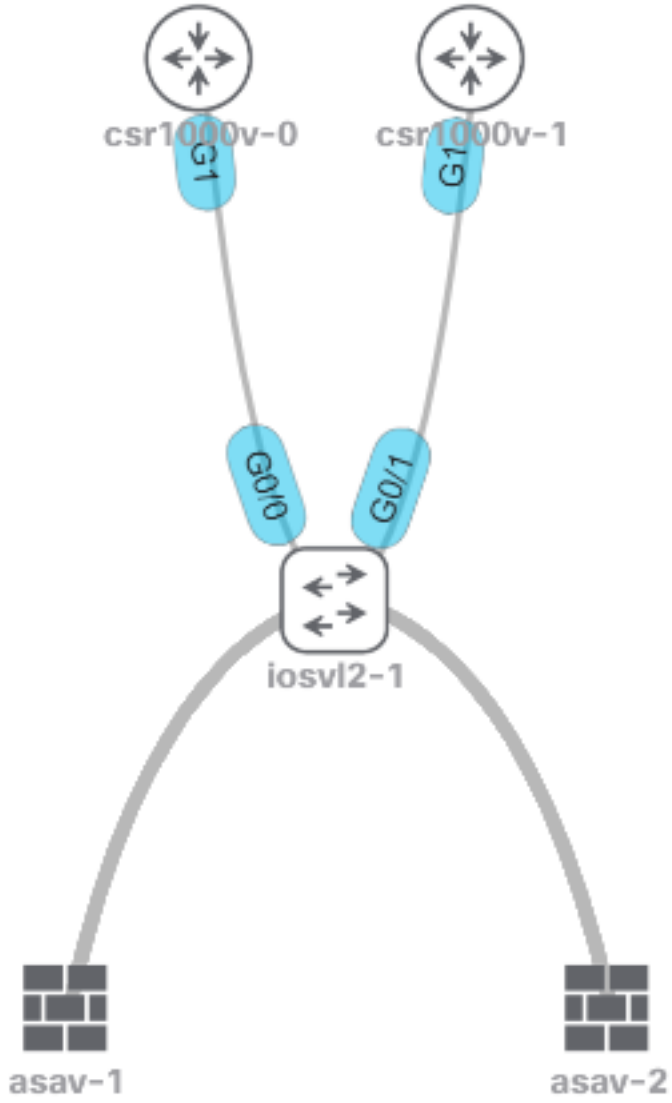
## Achtergrondinformatie

Voor een paar ASA dat in de transparante modus met hoge beschikbaarheid is geconfigureerd, als het paar firewalls upstream is aangesloten op een cluster van routers en die aangrenzende routers HSRP gebruiken, zal het verkeer van de firewalls naar het router IP-adres leiden dat ook

naar het MAC-adres van een specifieke router verwijst. Als het terugkeerverkeer echter afkomstig is van het MAC-adres van een andere routerinterface in het HSRP-paar, kan dit een netwerkstoring veroorzaken.

Het probleem is dat de time-out van de mac-adres-tabel 5 min (300 seconden) is en de ARP-time-out (Address Resolution Protocol) standaard 14400 seconden bedraagt. Omdat de next-hop router HSRP gebruikt, is er nooit verkeer afkomstig van het HSRP MAC-adres. Als dit gebeurt, verloopt de ingang in de MAC-adrestabel op de ASA en mislukt het verkeer.

### Netwerkdiagram




## Problemen oplossen

#### Begrijp MAC-tabelsynchronisatie voor ASA HA in transparante modus met HSRP

Deze uitgangen tonen hoe ASA-eenheden hun MAC-tabel synchroniseren wanneer de actieve eenheid nieuwe gegevens leert en oude gegevens verwijdert.

Active unit **asav-1** verliest **5254.0017.8a8c** MAC-adres van een van de HSRP-routers, in dit geval **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
```

Je ziet hoe **5254.0017.8a8c** na 5 minuten verdwijnt.

```
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
```

De stand-by unit verliest de **5254.0017.8a8c** MAC-ingang niet. Dit gedrag kan verwarring veroorzaken, maar dat wordt helemaal verwacht.

De stand-by unit werkt de MAC-adrestabel niet bij, tenzij deze de nieuwe actieve unit wordt.

De Standby-eenheid behoudt **5254.0017.8a8c** na enkele uren en blijft de hele tijd op één (1) minuut.

```
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
```

U kunt uren/dagen wachten en dezelfde opdracht uitvoeren en hetzelfde resultaat zien.

```
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
```

Bovendien, als u de **show failover** Als de opdracht is gegeven, zijn er geen wijzigingen op de **L2BRIDGE-teller** wanneer de actieve eenheid de HSRP-ingang verliest.

```
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
```

### MAC-adrestabelvermeldingen variëren vanwege asymmetrische routing

Wanneer het verkeer direct tussen twee MAC-adressen door de transparante firewall stroomt, verouderen die adressen niet terwijl het verkeer stroomt omdat de ASA frames ontvangt die afkomstig zijn van de twee MAC-adressen die het verkeer verzenden.

Wanneer de verkeersstroom asymmetrisch is, worden de invoertijden uitgeteld als de ASA geen antwoord ontvangt van dat specifieke MAC-adres.

> **Opmerking:** Asymmetrische routing betekent dat de ASA verkeer ziet dat bestemd is voor een specifiek MAC-adres, maar niet voor verkeer dat afkomstig is van hetzelfde MAC-adres.

De symptomen van dit probleem zijn dat nadat de ASA de MAC-adresinvoer uitleefde (na 5 minuten van geen verkeer afkomstig van dat MAC-adres), het verkeer dat bestemd is voor dat MAC-adres wordt gedropt tot de MAC-ingang opnieuw wordt bevolkt.

Meestal, het probleem zich voordoet wanneer het aantoont dat de connectiviteit aan een server na één of twee pogingen opnieuw wordt gevestigd, en dit is omdat het eerste pakket wordt gelaten vallen zodat ASA door de stappen kan gaan om de plaats van een adres van MAC te leren.

## Aanbevolen oplossing

Om dit probleem op te lossen, voeg een statische MAC-adresingstabel toe voor de HSRP IP op de firewall, of verhoog de leeftijdsduur tot een bepaalde waarde zodat een ARP-antwoord van de overeenkomstige HSRP-router komt voordat de ingangstijden uitvallen.

De betere oplossing is om een statische MAC-ingang toe te voegen omdat het niet zeker is of de ASA een ARP-antwoord van HSRP actieve router ontvangt.

## Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems

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.