Entender a sincronização de tabela MAC de alta disponibilidade ASA no modo transparente com roteadores HSRP

Contents

Introduction

Este documento descreve o comportamento de um par de ASA conectados a um cluster de roteadores que usam HSRP.

Prerequisites

- Dispositivo de segurança adaptável (ASA)
- Alta disponibilidade (HA) do ASA.
- Hot Standby Router Protocol (HSRP).
- Firewall em modo transparente.

Componentes Utilizados

- 2 roteadores CSR com HSRP.
- 2 ASA configurado em HA que aponta para o par 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

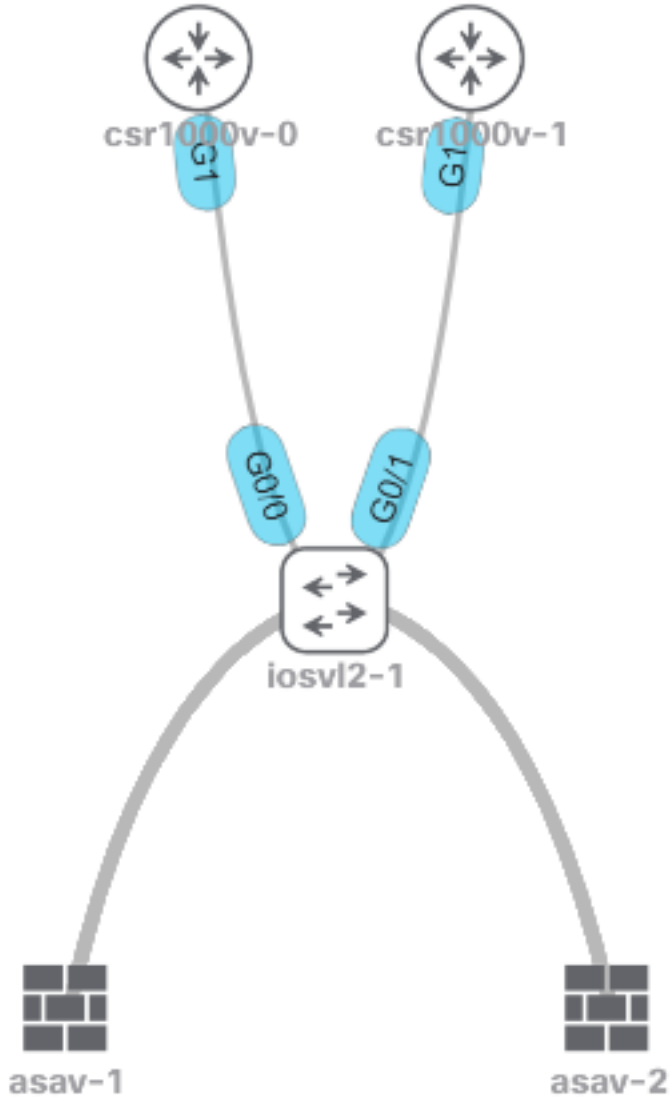
Informações de Apoio

Para um par de ASA configurado no modo transparente de alta disponibilidade, se o par de firewalls estiver conectado upstream a um cluster de roteadores e esses roteadores adjacentes usarem HSRP, o tráfego dos firewalls será direcionado para o endereço IP do roteador que também aponta para o endereço MAC de um roteador específico. No entanto, se o tráfego de

retorno for originado do endereço MAC de outra interface de roteador no par HSRP, pode causar uma interrupção de rede.

O problema é que o tempo limite de idade da tabela de endereços MAC é de 5 minutos (300 segundos) e o tempo limite do Address Resolution Protocol (ARP) é de 14400 segundos por padrão. Como o roteador do próximo salto usa o HSRP, nunca há tráfego originado do endereço MAC do HSRP. Se isso acontecer, a entrada mac-address-table no ASA expirará e o tráfego falhará.

Diagrama de Rede



Troubleshoot

Entender a sincronização da tabela MAC para ASA HA em modo transparente com HSRP

Essas saídas mostram como as unidades ASA sincronizam sua tabela MAC quando a unidade ativa aprende novas entradas e exclui entradas antigas.

A unidade ativa **asav-1** perde o endereço MAC **5254.0017.8a8c** de um dos roteadores HSRP, nesse caso, **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
```

Você pode ver como **5254.0017.8a8c** desaparece após 5 minutos.

```
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
```

A unidade de standby não perde a entrada MAC **5254.0017.8a8c**. Este comportamento pode causar confusão, no entanto, é totalmente esperado.

A unidade em standby não atualiza a tabela de endereços MAC a menos que ela se torne a nova unidade ativa.

A unidade em Standby mantém o **5254.0017.8a8c** após várias horas e permanece em um (1) minuto de tempo todo.

```
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
```

Você pode esperar horas/dias e executar o mesmo comando e ver o mesmo resultado.

```
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
```

Além disso, se você emitir o comando **show failover** não há alterações no contador **L2BRIDGE Tbl** quando a unidade ativa perde a entrada do 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
```

A entrada da tabela de endereços MAC expira devido ao roteamento assimétrico

Quando o tráfego flui diretamente entre dois endereços MAC através do firewall transparente, esses endereços não envelhecem enquanto o tráfego flui porque o ASA recebe quadros originados dos dois endereços MAC que enviam o tráfego.

Quando o fluxo de tráfego é assimétrico, a entrada expira se o ASA não receber uma resposta desse endereço MAC específico.

> **Note**: Roteamento assimétrico significa que o ASA vê o tráfego destinado a um endereço MAC específico, mas não o tráfego originado desse mesmo endereço MAC

Os sintomas desse problema são que depois que o ASA envelhece a entrada do endereço MAC (depois de 5 minutos sem nenhum tráfego originário desse endereço MAC), o tráfego destinado a esse endereço MAC é descartado até que a entrada MAC seja preenchida novamente.

Geralmente, o problema se apresenta quando mostra que a conectividade com um servidor é restabelecida após uma ou duas tentativas, e isso ocorre porque o primeiro pacote é descartado para que o ASA possa passar pelas etapas para aprender a localização de um endereço MAC.

Solução sugerida

Para resolver esse problema, adicione uma tabela de entrada de endereço MAC estático para o IP do HSRP no Firewall ou aumente o tempo de existência para algum valor, de forma que uma resposta ARP venha do roteador HSRP correspondente antes que o tempo de entrada expire.

A melhor solução é adicionar uma entrada MAC estática, já que não há certeza se o ASA recebe uma resposta ARP do roteador ativo HSRP.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.