Configurar o failover ativo/ativo do ASA no Firepower 4100 Series

Contents

Introdução

Este documento descreve como configurar o Failover Ativo/Ativo no Cisco Firepower 4145 NGFW Appliance.

Pré-requisitos

Requisitos

A Cisco recomenda ter conhecimento deste tópico:

- Failover ativo/standby no Cisco Adaptive Security Appliance (ASA).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivo NGFW Cisco Firepower 4145 (ASA) 9.18(3)56
- Sistema operacional extensível Firepower (FXOS) 2.12(0.498)
- Windows 10

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

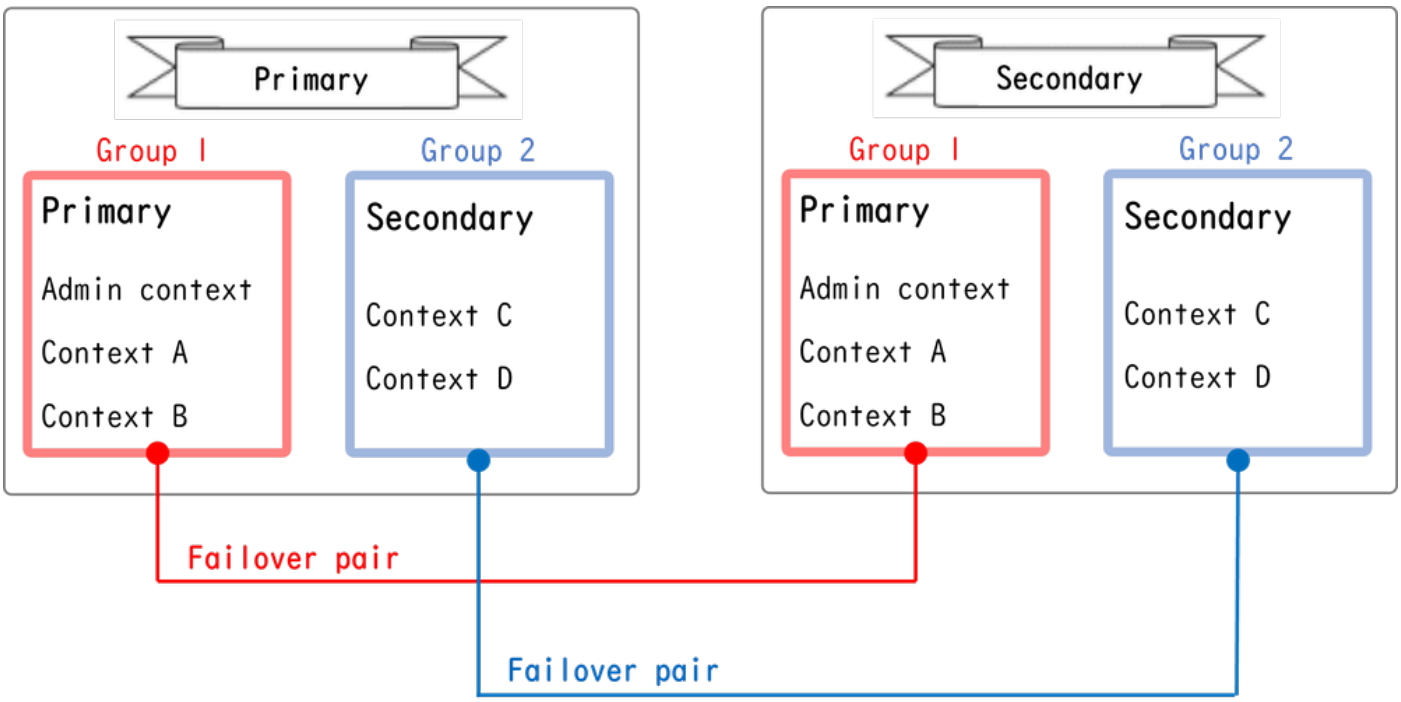
O Failover Ativo/Ativo está disponível apenas para aplicativos de segurança que estejam sendo executados no modo de contexto múltiplo. Nesse modo, o ASA é logicamente dividido em vários dispositivos virtuais, conhecidos como contextos. Cada contexto opera como um dispositivo independente, com sua própria política de segurança, interfaces e administradores.

O Failover Ativo/Ativo é um recurso do Adaptive Security Appliance (ASA) que permite que dois dispositivos Firepower passem o tráfego simultaneamente. Essa configuração é normalmente usada para um cenário de balanceamento de carga no qual você deseja dividir o tráfego entre dois dispositivos para maximizar o throughput. Ele também é usado para fins de redundância, portanto, se um ASA falhar, o outro pode assumir sem causar uma interrupção no serviço.

Mecanismo de failover ativo/ativo do ASA

Cada contexto no Failover Ativo/Ativo é atribuído manualmente ao grupo 1 ou ao grupo 2. O contexto Admin é atribuído ao grupo 1 por padrão. O mesmo grupo (grupo1 ou grupo2) nos dois chassis (unidades) forma um par de failover que está realizando a função de redundância. O comportamento de cada par de failover é basicamente igual ao comportamento de um failover Ativo/Standby. Para obter mais detalhes sobre o failover Ativo/Standby, consulte Configurar Failover Ativo/Standby. No Failover Ativo/Ativo, além da Função (Principal ou Secundário) de cada chassi, cada grupo também tem uma Função (Principal ou Secundário). Essas funções são predefinidas manualmente pelo usuário e são usadas para decidir o status de Alta Disponibilidade (HA) (Ativo ou Standby) de cada grupo de failover.

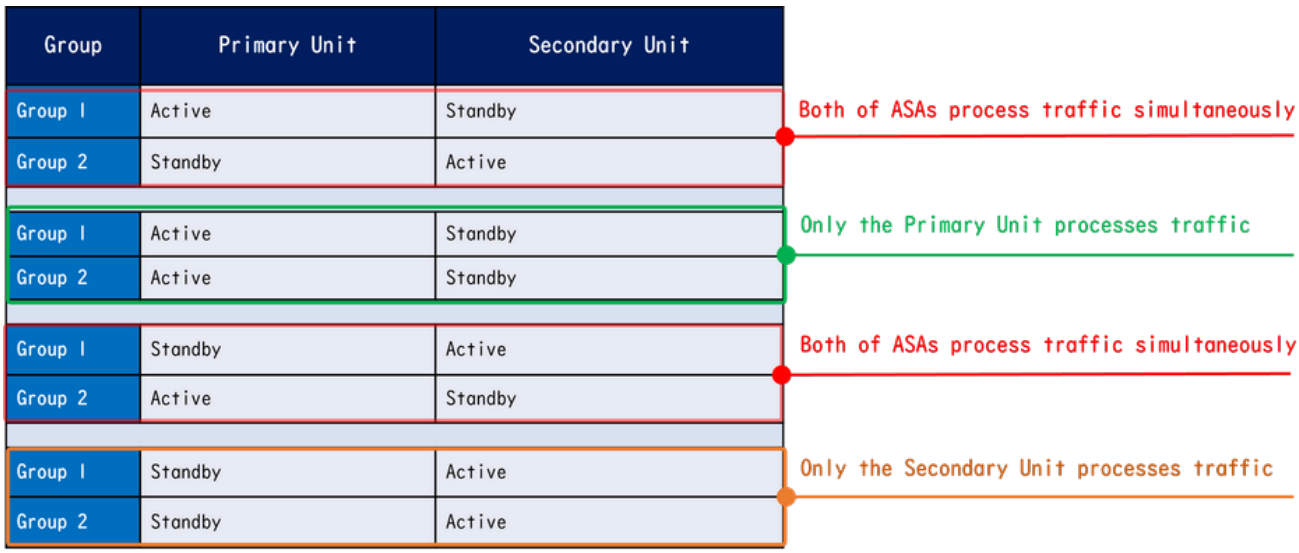
O Contexto de administração é um contexto especial que trata da conexão básica de gerenciamento de chassi (como SSH). Esta é uma imagem do Failover Ativo/Ativo.



Par de Failover em Failover Ativo/Ativo

Fluxo de tráfico

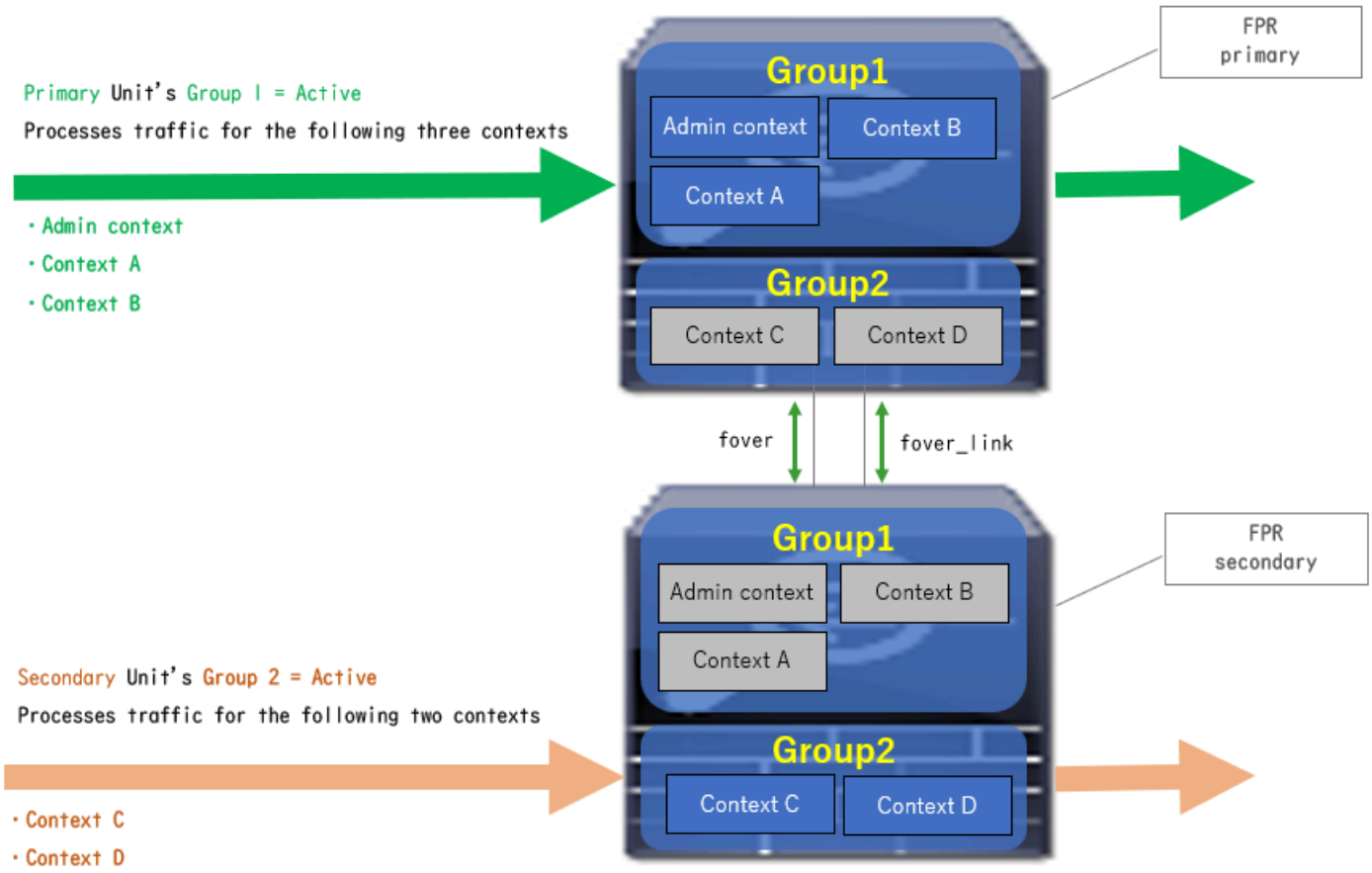
No Failover Ativo/Ativo, o tráfego pode ser tratado em vários padrões, como mostrado na imagem a seguir.



Fluxo de tráfico

Condição de fluxo de tráfego 1

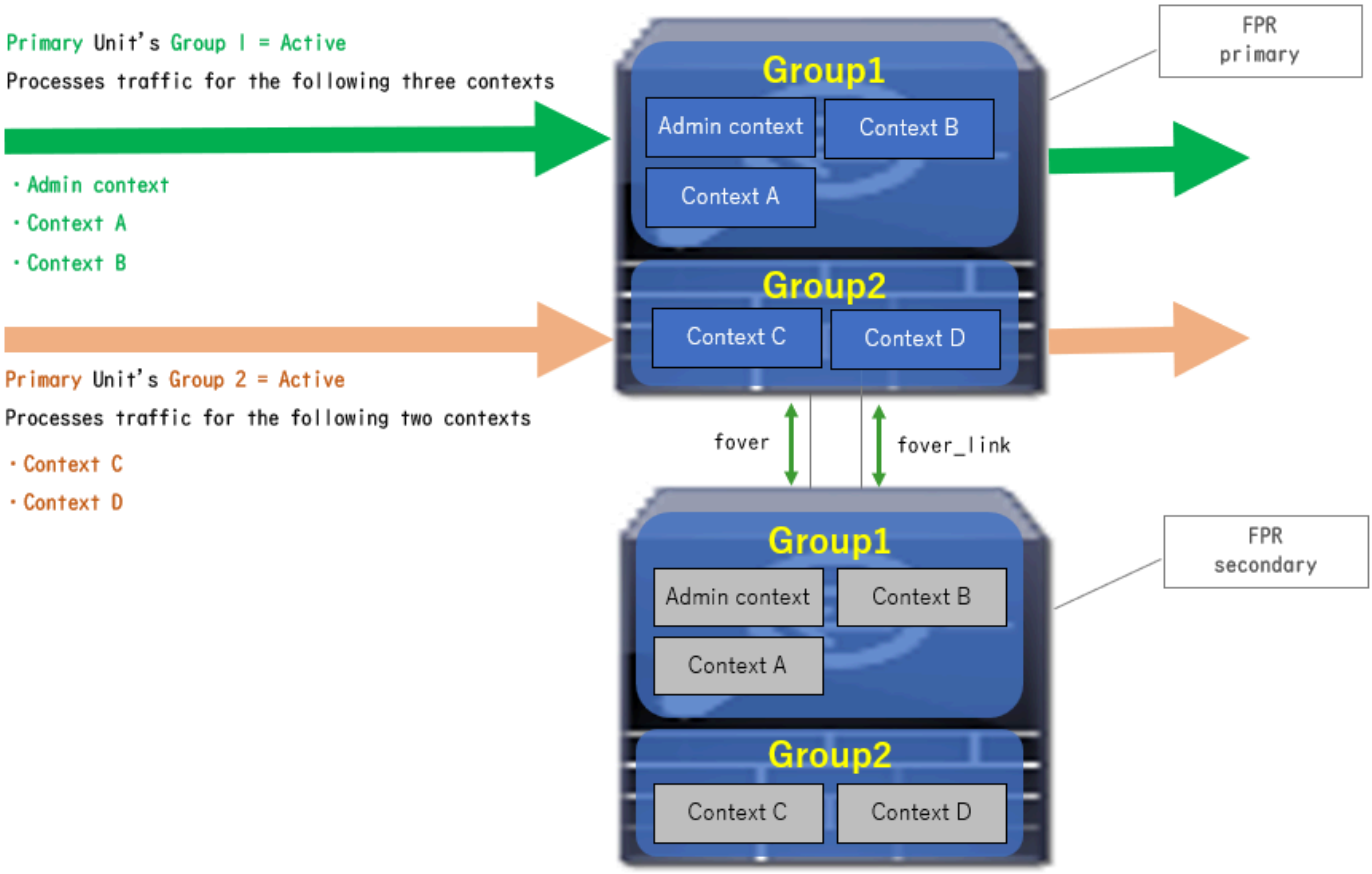
- Unidade Principal: Grupo 1 = Ativo, Grupo 2 = Em Espera
- Unidade Secundária: Grupo 1 = Em Espera, Grupo 2 = Ativo



Condição de fluxo de tráfego 1

Condição de fluxo de tráfego 2

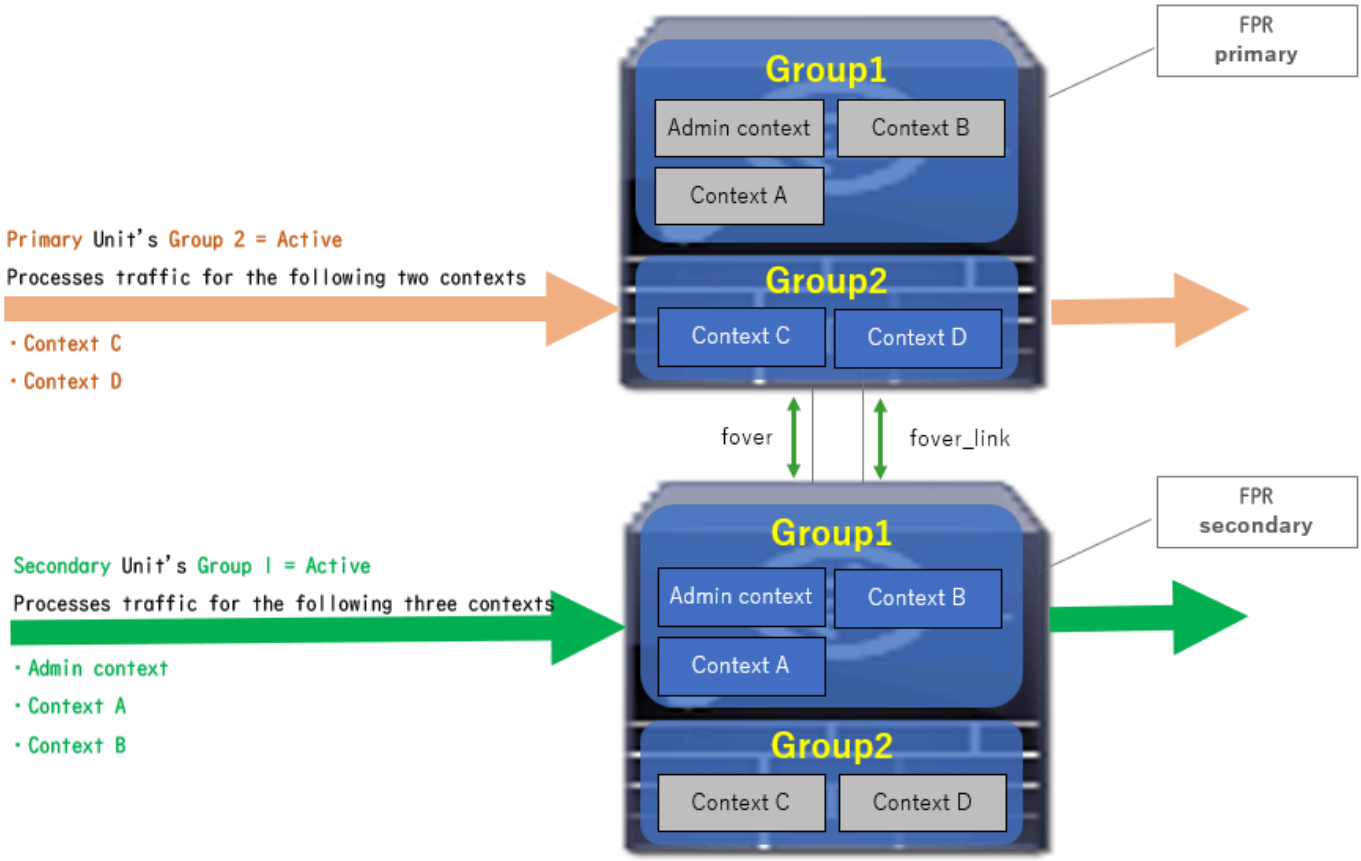
- Unidade Principal: Grupo 1 = Ativo, Grupo 2 = Ativo
- Unidade Secundária: Grupo 1 = Em Espera, Grupo 2 = Em Espera



Condição de fluxo de tráfego 2

Condição de fluxo de tráfego 3

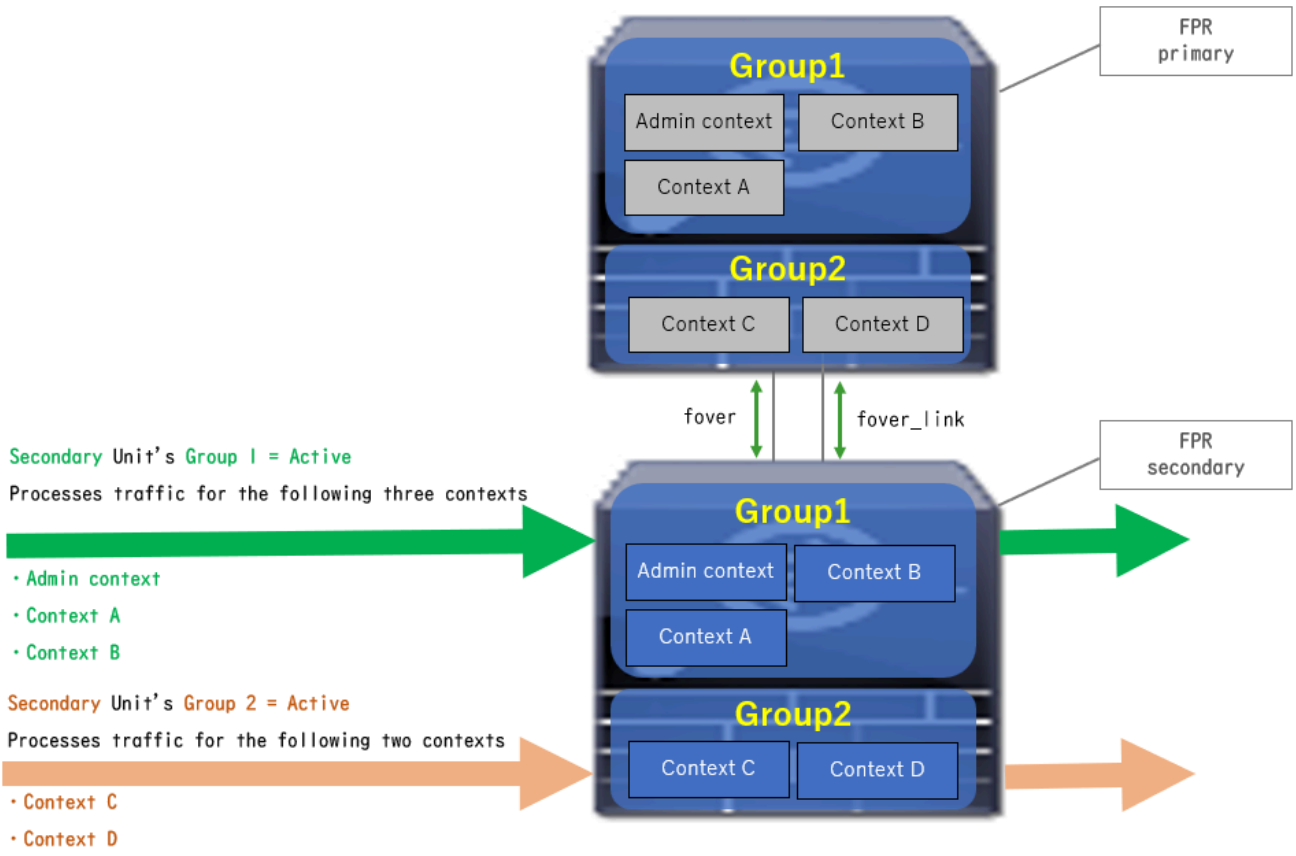
- Unidade Principal: Grupo 1 = Em Espera, Grupo 2 = Ativo
- Unidade Secundária: Grupo 1 = Ativo, Grupo 2 = Em Espera



Condição de fluxo de tráfego 3

Condição de fluxo de tráfego 4

- Unidade Principal: Grupo 1 = Em Espera, Grupo 2 = Em Espera
- Unidade Secundária: Grupo 1 = Ativo, Grupo 2 = Ativo



Condição de fluxo de tráfego 4

Regras de Seleção para Ativo/Em Espera

No Failover Ativo/Ativo , o status (ativo/standby) de cada grupo é determinado pelas seguintes regras:

- Suponha que dois dispositivos estejam sendo inicializados quase ao mesmo tempo, então uma das unidades (Primária ou Secundária) torna-se ativa primeiro.
- Quando o tempo de preempção passa, o grupo que tem a mesma função no chassi e no grupo se torna ativo.
- Quando há um evento de failover (como a interface INATIVA), o status do grupo muda da mesma forma que com o failover Ativo/Standby.
- O tempo de preempção não funciona após o failover manual.

Este é um exemplo da alteração de status.

- Os dois dispositivos estão sendo inicializados quase ao mesmo tempo. Status A →
- Tempo de apropriação passado. → de Status B
- Falha do dispositivo primário (o failover é acionado). → C de status
- Tempo de antecipação decorrido desde que o dispositivo primário se recuperou da falha. Status D →
- Dispare manualmente o failover. Status E

Para obter detalhes sobre disparadores de failover e monitoramento de integridade, consulte Eventos de failover.

1. Os dois dispositivos estão sendo inicializados quase ao mesmo tempo.

Operation	Primary Unit		Secondary Unit	
	Group 1: primary	Group 2: secondary	Group 1: primary	Group 2: secondary
Both devices started simultaneously	Active	Active	Standby	Standby
	or			
	Standby	Standby	Active	Active

Status A

2. Tempo de antecipação (30s neste documento) passado.

After 30 seconds (preempt time)	Active	Standby	Standby	Active

Status B

3. Ocorreu uma falha (como Interface Inativa) no grupo 1 da unidade Primária.

Failover event	Standby	Standby	Active	Active

Status C

4. Tempo de antecipação (30s neste documento) decorrido desde a recuperação do grupo 1 do Dispositivo primário após falha.

After 30 seconds since Primary Unit recovered	Active	Standby	Standby	Active

Status D

5. Definindo manualmente o grupo 2 da Unidade Principal como Ativo.

Manual failover	Active	Active	Standby	Standby

Status E

Diagrama de Rede

Este documento apresenta a configuração e a verificação do Failover Ativo/Ativo com base neste diagrama.

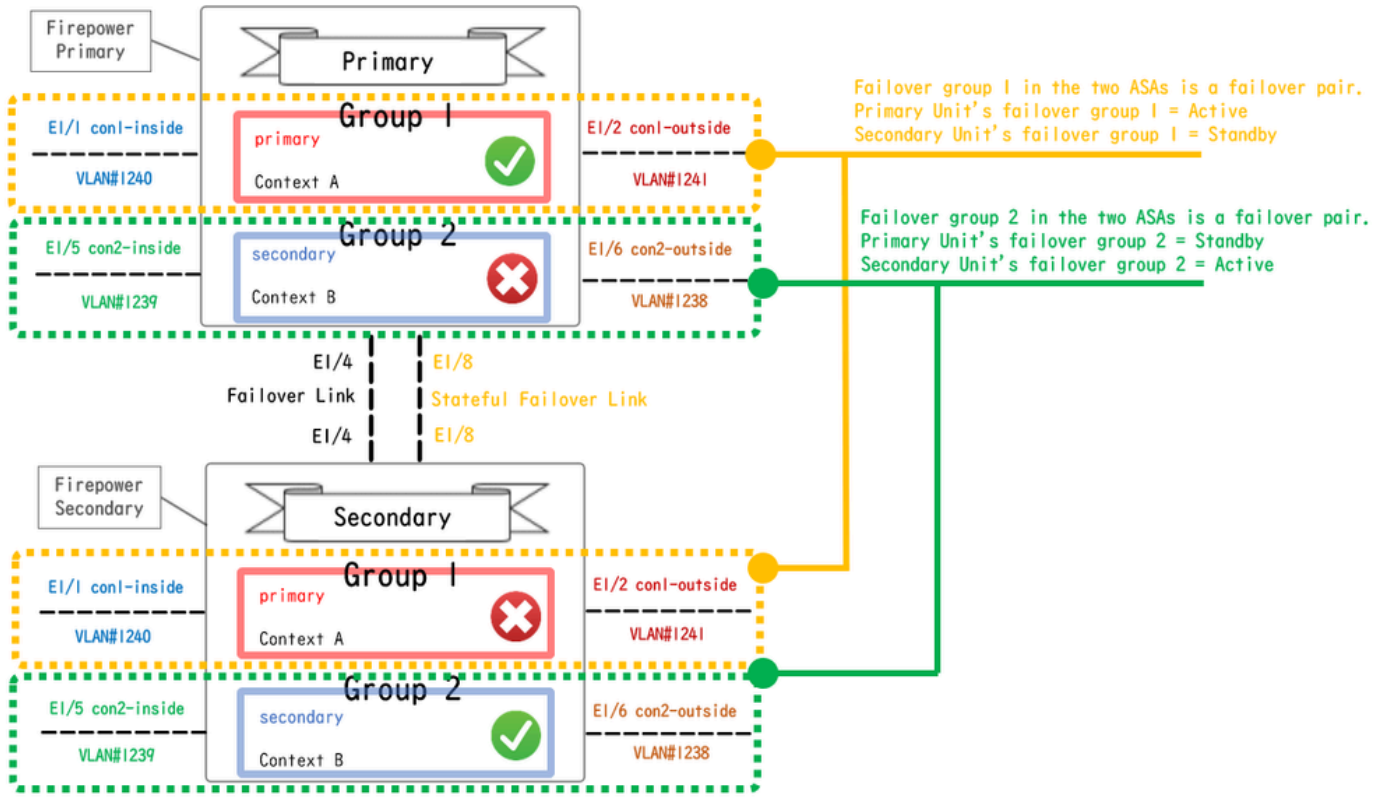


Diagrama de configuração lógica

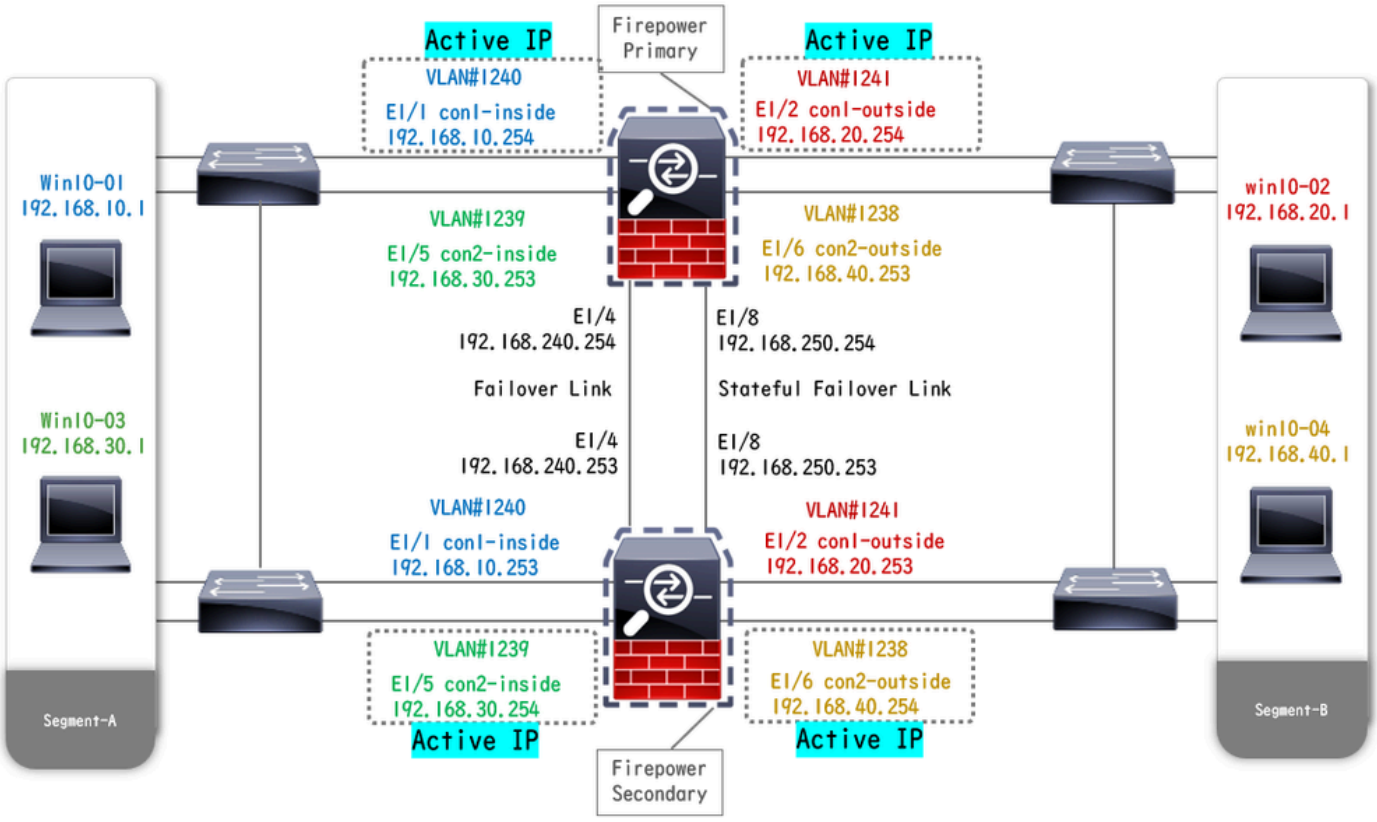
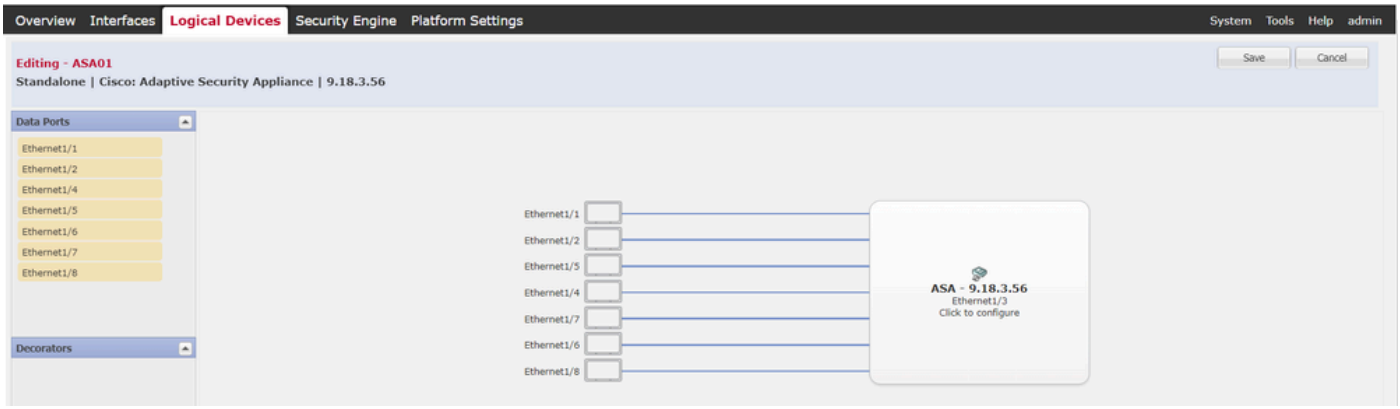


Diagrama de configuração física

Configuração

Etapa 1. Pré-configurar interfaces

Para os dois Firepower, faça logon na GUI do FCM. Navegue até Dispositivos lógicos > Editar. Adicione a interface de dados ao ASA, como mostrado na imagem.



Pré-configurar interfaces

Etapa 2. Configuração na unidade primária

Conecte-se ao CLI FXOS primário via SSH ou console. Execute **connect module 1 console** e connect asa o comando para entrar na CLI do ASA.

a. Configure o failover na unidade Principal (execute o comando no contexto do sistema da unidade Principal).

```
<#root>
```

failover lan unit primary failover lan interface fover E1/4 failover link fover_link E1/8 failover interface ip fover 192.168.240.254 255.255.255.0 standby 1

```
failover group 1
□□□<--- group 1 is assigned to primary by default preempt 30 failover group 2 secondary preempt 30 fai
```

b. Configure o grupo de failover para context (execute o comando no contexto do sistema da Unidade primária).

```
<#root>
```

admin-context admin

```
context admin
 <--- admin context is assigned to group 1 by default allocate-interface E1/3 config-url disk0:/admin.c
join-failover-group 1
 <--- add con1 context to group 1 ! context con2 allocate-interface E1/5 allocate-interface E1/6 config
join-failover-group 2
 <--- add con2 context to group 2
```

c. Execute changeto context con1 para conectar o contexto con1 do contexto do sistema . Configure o IP para a interface do contexto con1 (execute o comando no contexto con1 da unidade Primária).

interface E1/1 nameif con1-inside ip address 192.168.10.254 255.255.255.0 standby 192.168.10.253 security-level 100 no shutdown interface E1/2 nameif

d. Execute changeto context con2 para conectar o contexto con2 do contexto do sistema . Configure o IP para a interface do contexto con2 (execute o comando no contexto con2 da unidade Primária).

interface E1/5 nameif con2-inside ip address 192.168.30.254 255.255.255.0 standby 192.168.30.253 security-level 100 no shutdown interface E1/6 nameif

Etapa 3. Configuração na unidade secundária

a. Conecte-se à CLI FXOS secundária via SSH ou console. Configure o failover na unidade Secundária (execute o comando no contexto do sistema da unidade Secundária).

failover lan unit secondary failover lan interface fover E1/4 failover link fover_link E1/8 failover interface ip fover 192.168.240.254 255.255.255.0 standby

b. Executar failover comando (executar no contexto do sistema da unidade secundária).

failover

Etapa 4. Confirmar Status do Failover Após Sincronização Concluída com Êxito

a. Executar show failover no contexto do sistema da Unidade secundária.

<#root>

asa#

show failover

 Failover On Failover unit Secondary Failover LAN Interface: fover Ethernet1/4 (up) Version: Ours 9.18(

Secondary

<--- group 1 and group 2 are Standby status in Secondary Unit Group 1 State:

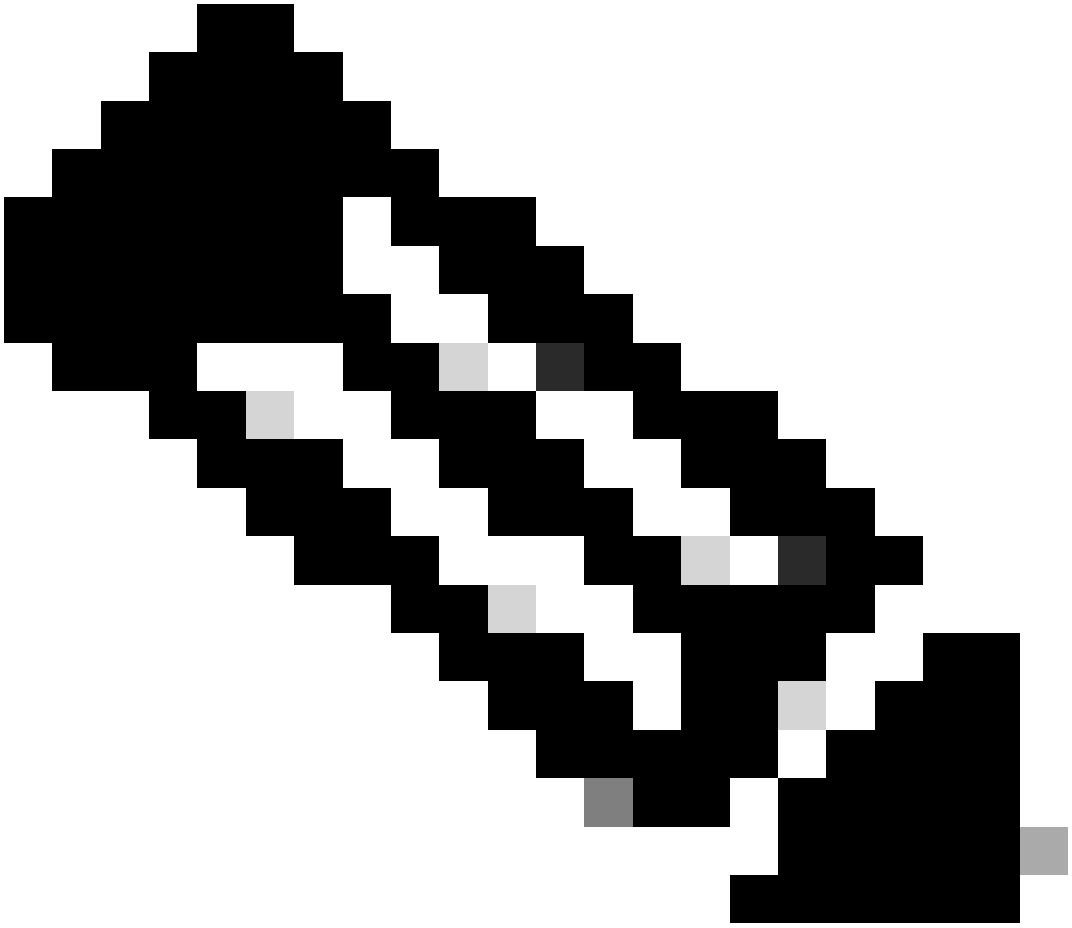
Standby Ready

```
 Active time: 0 (sec) Group 2 State:
Standby Ready
 Active time: 945 (sec) con1 Interface con1-inside (192.168.10.253): Unknown (Waiting) con1 Interface c
Primary
<--- group 1 and group 2 are Active status in Primary Unit Group 1 State:
Active
 Active time: 1637 (sec) Group 2 State:
Active
 Active time: 93 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface c
```

b. (Opcional) Execute o **no failover active group 2** comando para alternar manualmente o grupo 2 da unidade Primária para o status Standby (executado no contexto do sistema da unidade Primária). Isso pode equilibrar a carga de tráfego através do firewall.

<#root>

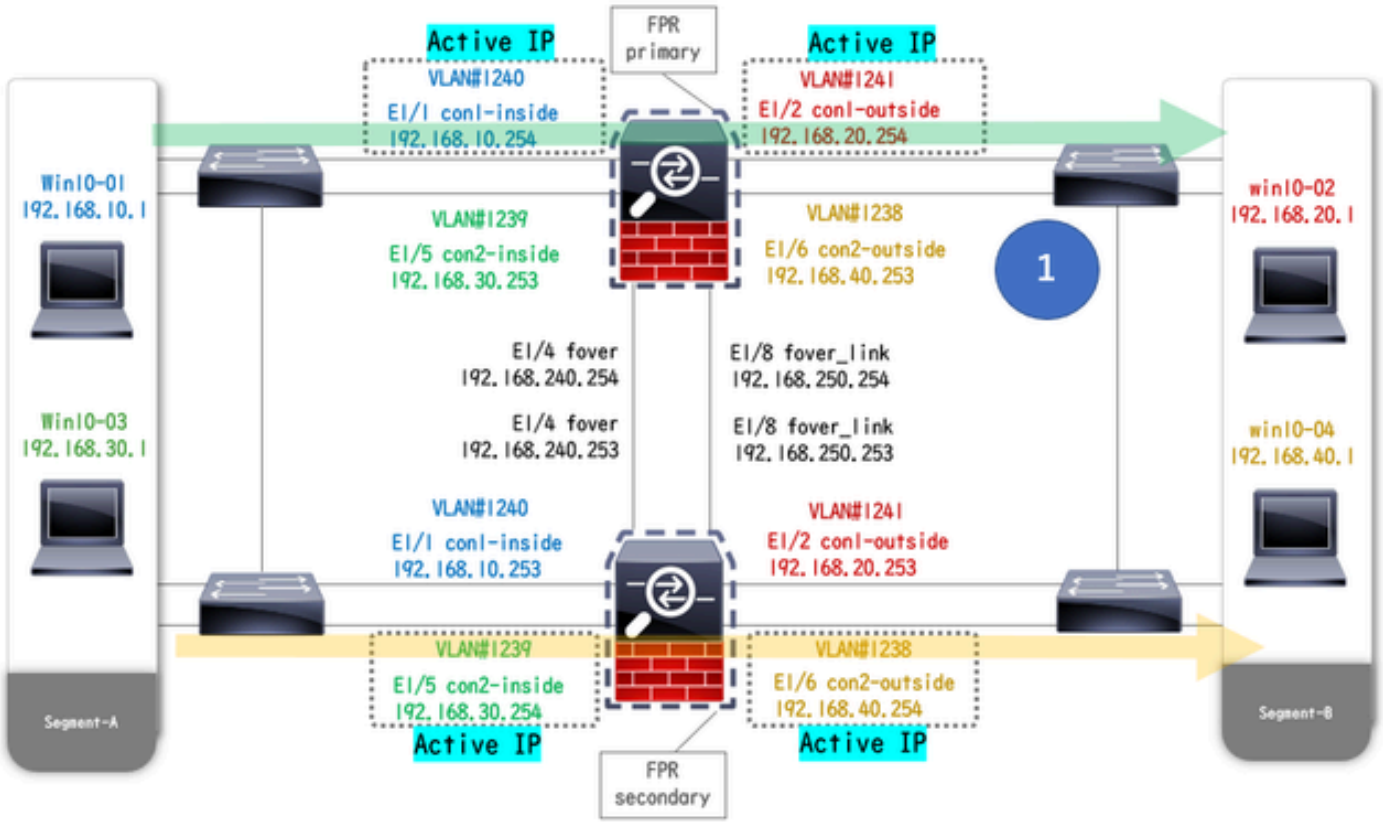
```
no failover active group 2
```



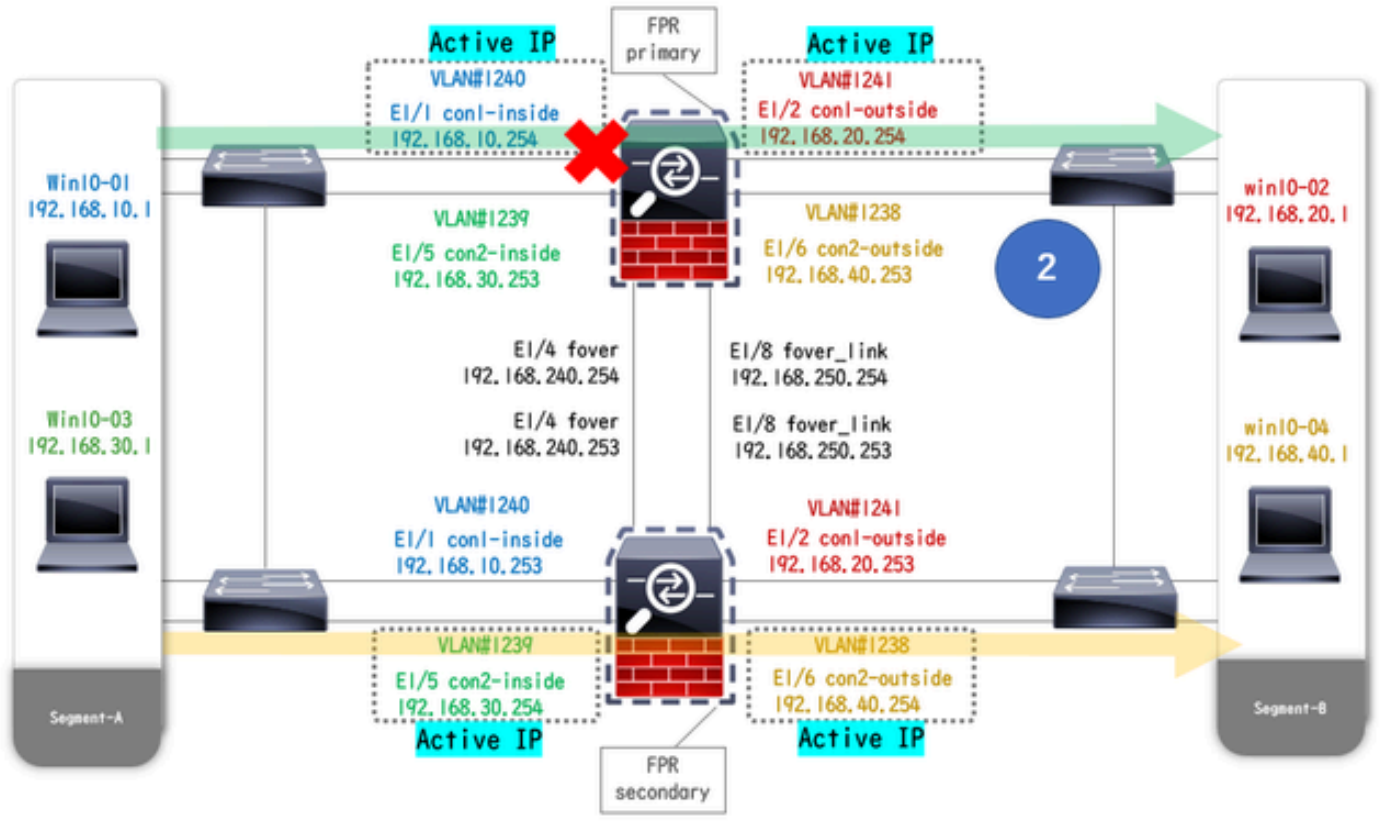
Observação: se você executar esse comando, o status do failover corresponderá à condição de fluxo de tráfego 1.

Verificar

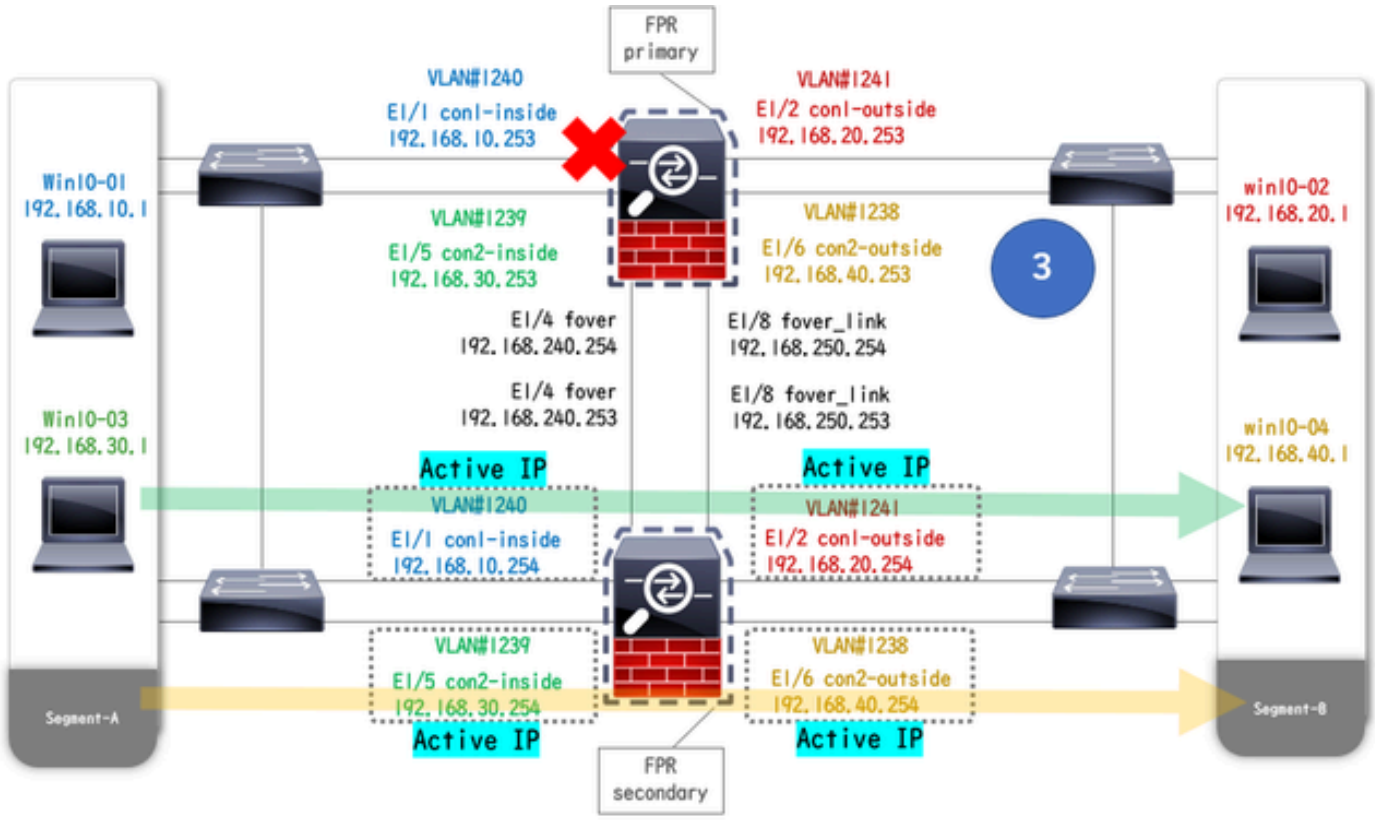
Quando E1/1 fica INATIVO, o failover do grupo 1 é acionado e as interfaces de dados no lado de Standby (Unidade Secundária) assumem o endereço IP e MAC da Interface Ativa original, garantindo que o tráfego (conexão FTP neste documento) seja transmitido continuamente pelos ASAs.



Antes do link



desativadoDurante o link desativado



Failover Acionado

Etapa 1. Iniciar Conexão FTP de Win10-01 para Win10-02

Etapa 2. Confirmar Conexão FTP Antes do Failover

Execute changeto context con1 para conectar o contexto con1 do contexto do sistema. Confirme se uma conexão FTP está estabelecida em ambas as unidades ASA.

<#root>

asa/act/pri/con1#

show conn

```
 5 in use, 11 most used
 ! --- Confirm the connection in Primary Unit TCP
```

con1-outside

192.168.20.1:21

con1-inside 192.168.10.1:49703

, idle 0:00:11, bytes 528, flags UIO asa/stby/sec/con1#

show conn

```
 5 in use, 11 most used
 ! --- Confirm the connection in Secondary Unit TCP
```

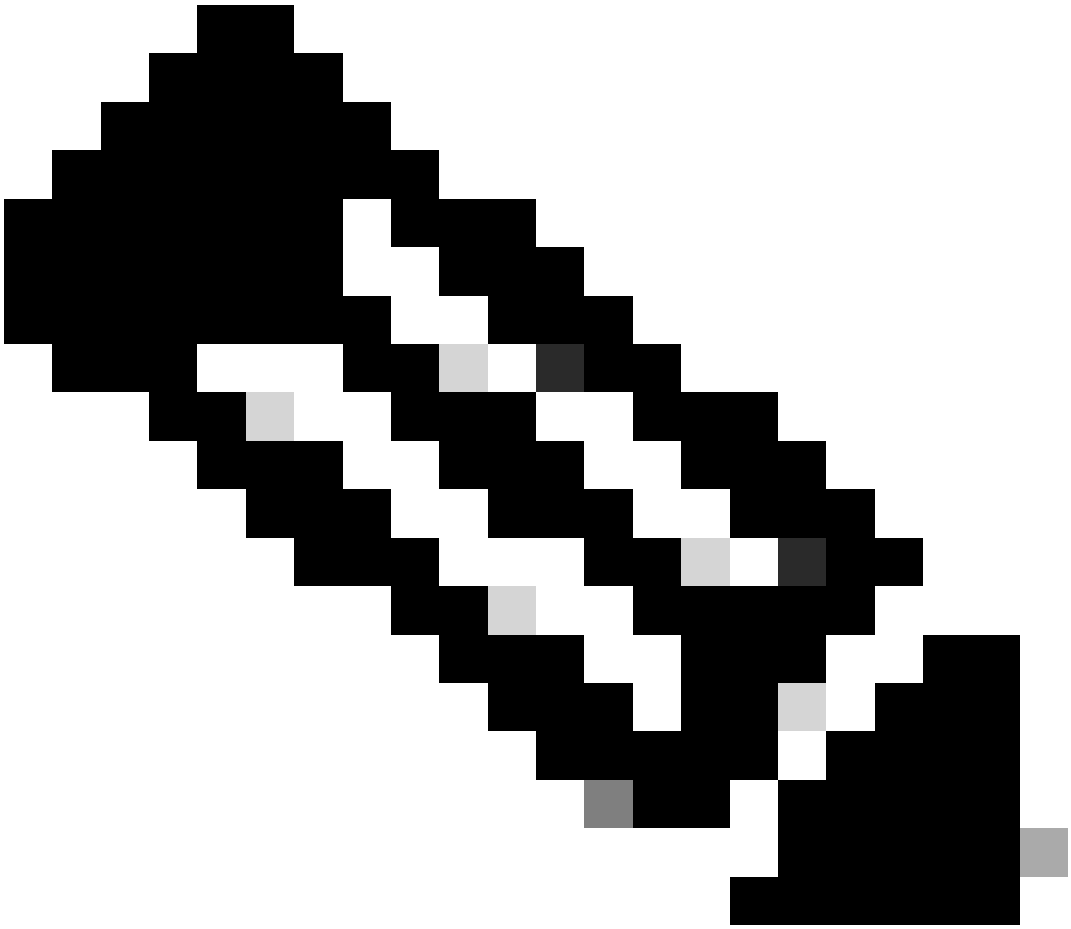
con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

, idle 0:00:14, bytes 528, flags UIO

Etapa 3. LinkDOWN E1/1 da unidade primária

Etapa 4. Confirmar Status de Failover

No contexto do sistema, confirme se o failover ocorre no grupo 1.



Observação: o status do failover corresponde à condição de fluxo de tráfego 4.

<#root>

asa/act/sec#

show failover

 Failover On Failover unit Secondary Failover LAN Interface: fover Ethernet1/4 (up) ..... Group 1 last

Secondary

 Group 1 State:

Active

<--- group 1 of Secondary Unit is Switching to Active Active time: 5 (sec) Group 2 State:

Active

 Active time: 10663 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Waiting) con1 Interface

Primary

 Group 1 State:

Failed

<--- group 1 of Primary Unit is Switching to Failed status Active time: 434 (sec) Group 2 State:

Standby Ready

 Active time: 117 (sec) con1 Interface con1-inside (192.168.10.253): Failed (Waiting) con1 Interface co

Etapa 5. Confirmar conexão FTP após failover

Execute changeto context con1 para conectar o contexto con1 do contexto do sistema, confirme se a conexão FTP não foi interrompida.

<#root>

asa/act/sec#

changeto context con1

 asa/act/sec/con1# show conn 11 in use, 11 most used
! --- Confirm the target FTP connection exists in group 1 of the Secondary Unit TCP

con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

, idle 0:00:09, bytes 529, flags UIO

Etapa 6. Confirmar comportamento do tempo de antecipação

LinkUP E1/1 da unidade primária e aguarde 30s (tempo de preferência), o estado de failover retorna ao estado original (fluxo de tráfego correspondente no padrão 1).

<#root>

asa/stby/pri#

Group 1 preempt mate

□□□□<--- Failover is triggered automatically, after the preempt time has passed asa/act/pri# show fail

Primary

Group 1 State:

Active

<--- group 1 of Primary Unit is switching to Active status Active time: 34 (sec) Group 2 State:

Standby Ready

Active time: 117 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface

Secondary

Group 1 State:

Standby Ready

□□<---- group 1 of Secondary Unit is switching to Standby status Active time: 125 (sec) Group 2 State:

Active

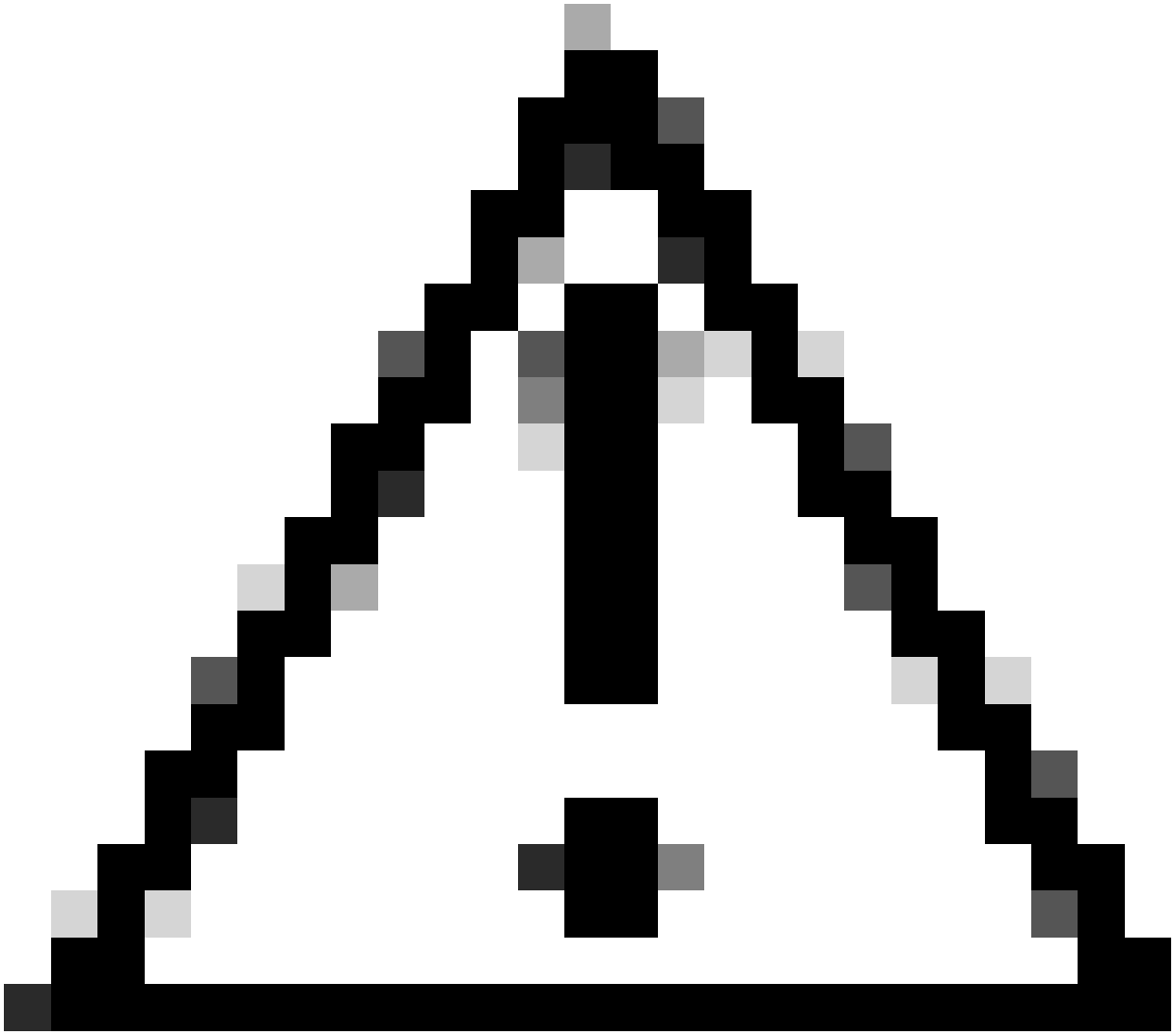
Active time: 10816 (sec) con1 Interface con1-inside (192.168.10.253): Normal (Monitored) con1 Interfac

Endereço MAC virtual

No Failover Ativo/Ativo, o endereço MAC virtual (valor definido manualmente, valor gerado automaticamente ou valor padrão) é sempre usado. O endereço MAC virtual ativo está associado à Interface ativa.

Configuração manual do endereço MAC virtual

Para definir manualmente o endereço MAC virtual para interfaces físicas, o comando mac address ou o mac-address comando (no modo de configuração I/F) pode ser usado. Este é um exemplo de configuração manual de um endereço MAC virtual para a interface física E1/1.



Cuidado: evite usar esses dois tipos de comandos no mesmo dispositivo.

<#root>

asa/act/pri(config)# failover group 1 asa/act/pri(config-fover-group)#

mac address E1/1 1234.1234.0001 1234.1234.0002

asa/act/pri(config-fover-group)# changeto context con1 asa/act/pri/con1(config)# show interface E1/1 |

1234.1234.0001

, MTU 1500 <--- Checking virtual MAC on the Primary Unit(con1) side asa/stby/sec# changeto context con1

1234.1234.0002

, MTU 1500 <--- Checking virtual MAC on the Secondary Unit(con1) side

OU

<#root>

asa/act/pri(config)# changeto context con1 asa/act/pri/con1(config)# int E1/1 asa/act/pri/con1(config-if)#

mac-addr

1234.1234.0001 standby 1234.1234.0002

asa/act/pri/con1(config)# show interface E1/1 | in MAC MAC address

1234.1234.0001

, MTU 1500 <--- Checking virtual MAC on the Primary Unit(con1) side asa/stby/sec# changeto context con1

1234.1234.0002

, MTU 1500<--- Checking virtual MAC on the Secondary Unit(con1) side

Configuração Automática de Endereço MAC Virtual

A geração automática de endereço MAC virtual também é suportada. Isso pode ser obtido usando o comando mac-address auto <prefix prefix> .
O formato do endereço MAC virtual é A2 xx.yyzz.zzzz, que está sendo gerado automaticamente.
A2 : valor fixo
xx.yy : gerado pelo <prefixo do prefixo> especificado na opção de comando (O prefixo é convertido em hexadecimal e, em seguida, inserido por ordem inversa).
zz.zzzz : gerado por um contador interno

Este é um exemplo sobre a geração de endereço MAC virtual por **mac-address auto** comando para a interface.

<#root>

asa/act/pri(config)#

mac-address auto

INFO: Converted to mac-address auto prefix 31

```
asa/act/pri(config)#
```

show run all context con1

```
 <--- Checking the virtual MAC addresses generated on con1 context
allocate-interface Ethernet1/1
mac-address auto Ethernet1/1 a21f.0000.0008 a21f.0000.0009
allocate-interface Ethernet1/2
mac-address auto Ethernet1/2 a21f.0000.000a a21f.0000.000b
config-url disk0:/con1.cfg
join-failover-group 1

asa/act/pri(config)#
```

show run all context con2

```
<--- Checking the virtual MAC addresses generated on con2 context
context con2
allocate-interface Ethernet1/5
mac-address auto Ethernet1/5 a21f.0000.000c a21f.0000.000d
allocate-interface Ethernet1/6
mac-address auto Ethernet1/6 a21f.0000.000e a21f.0000.000f
config-url disk0:/con2.cfg
join-failover-group 2
```

Configuração Padrão de Endereço MAC Virtual

Caso a geração automática ou manual de um endereço MAC virtual não esteja definida, o endereço MAC virtual padrão será usado.

Para obter mais informações sobre o endereço MAC virtual padrão, consulte Command Default of mac address no Guia de Referência de Comandos do Cisco Secure Firewall ASA Series.

Atualização

Você pode obter atualização zero de inatividade de um par de failover Ativo/Ativo usando CLI ou ASDM. Para obter mais informações, consulte Atualizar um par de failover ativo/ativo.

Informações Relacionadas

- Atualizar um par de failover ativo/ativo usando a CLI
- Endereço MAC
- Suporte técnico e downloads da Cisco

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.