Configuration du basculement actif/actif ASA dans Firepower 4100

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Mécanisme de basculement actif/actif ASA
- Flux de trafic
  - Condition de flux de trafic 1
  - Condition de flux de trafic 2
  - Condition de flux de trafic 3
  - Condition de flux de trafic 4
- Règles de sélection pour actif/veille
- Diagramme du réseau
- Configuration
  - Étape 1. Pré-configuration des interfaces
  - Étape 2. Configuration sur l'unité principale
  - Étape 3. Configuration sur l'unité secondaire
  - Étape 4 : confirmation de l'état de basculement après la synchronisation réussie
- Vérifier
  - Étape 1 : établissement d'une connexion FTP de Win10-01 à Win10-02
  - Étape 2 : confirmation de la connexion FTP avant le basculement
  - Étape 3. LinkDOWN E1/1 de l'unité principale
  - Étape 4. Confirmation du statut de basculement
  - Étape 5. Confirmation de la connexion FTP après le basculement
  - Étape 6. Confirmer le comportement de l'heure de préemption
- Adresse MAC virtuelle
  - Configuration manuelle de l'adresse MAC virtuelle
  - Configuration automatique de l'adresse MAC virtuelle
  - Paramètre par défaut de l'adresse MAC virtuelle
- Mise à niveau
- Informations connexes

Introduction

Ce document décrit comment configurer le basculement actif/actif dans le pare-feu de nouvelle génération Cisco Firepower 4145.

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance de ce sujet :

- Basculement actif/veille dans Cisco Adaptive Security Appliance (ASA).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de pare-feu de nouvelle génération Cisco Firepower 4145 (ASA) 9.18(3)56
- Système d'exploitation extensible Firepower (FXOS) 2.12(0.498)
- Windows 10

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

Le basculement actif/actif n'est disponible que pour les appliances de sécurité qui s'exécutent en mode de contexte multiple. Dans ce mode, l'ASA est logiquement divisé en plusieurs périphériques virtuels, appelés contextes. Chaque contexte fonctionne comme un périphérique indépendant, avec sa propre stratégie de sécurité, ses propres interfaces et ses propres administrateurs.

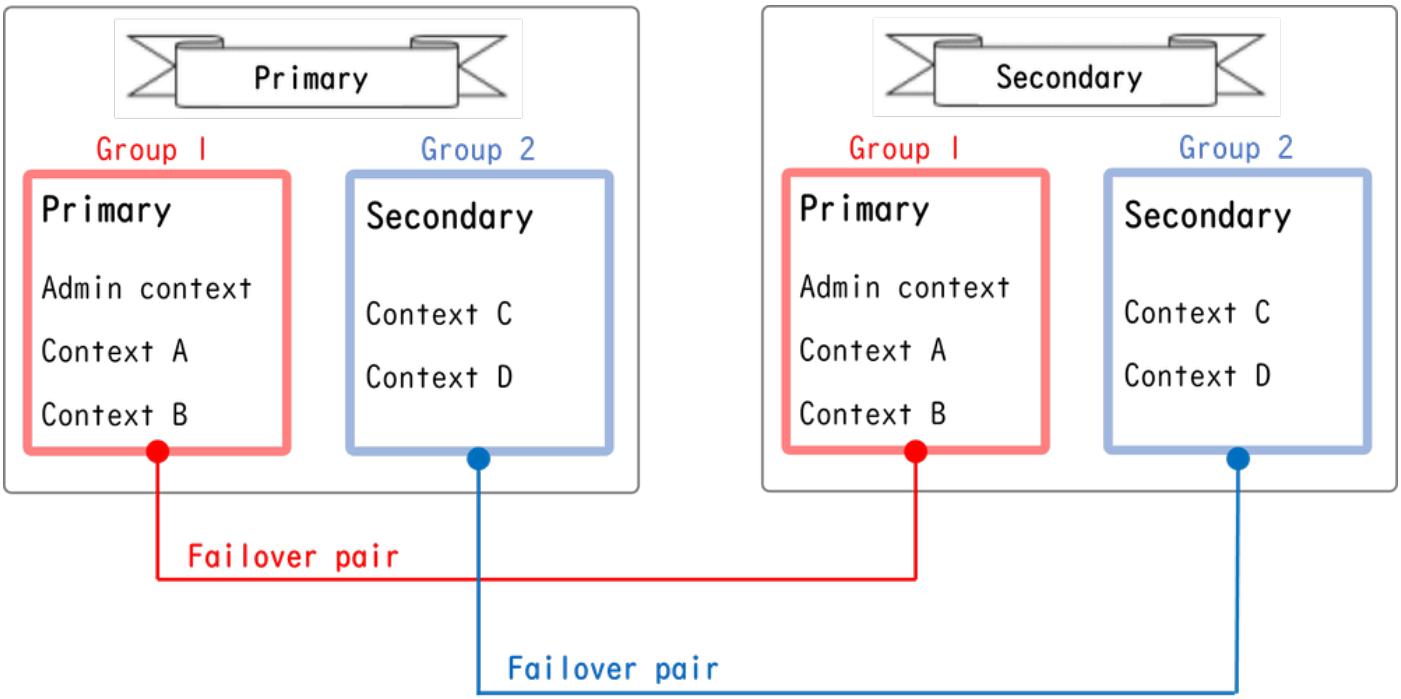
Le basculement actif/actif est une fonctionnalité de l'appareil de sécurité adaptatif (ASA) qui permet à deux périphériques Firepower de transmettre le trafic simultanément. Cette configuration est généralement utilisée pour un scénario d'équilibrage de charge dans lequel vous souhaitez répartir le trafic entre deux périphériques afin d'optimiser le débit. Il est également utilisé à des fins de redondance, de sorte que si un ASA tombe en panne, l'autre peut prendre le relais sans provoquer d'interruption de service.

Mécanisme de basculement actif/actif ASA

Chaque contexte du basculement actif/actif est affecté manuellement au groupe 1 ou au groupe 2. Le contexte Admin est affecté par défaut au groupe 1. Le même groupe (groupe1 ou groupe2) dans les deux châssis (unités) forme une paire de basculement qui réalise la fonction de redondance. Le comportement de chaque paire de basculement est fondamentalement identique à celui d'un basculement actif/veille. Pour plus de détails sur le basculement actif/veille, veuillez vous reporter à Configurer le basculement actif/veille. En cas de basculement actif/actif, en plus du rôle (principal ou secondaire) de chaque châssis, chaque groupe dispose également d'un rôle

(principal ou secondaire). Ces rôles sont prédéfinis manuellement par l'utilisateur et servent à déterminer l'état de haute disponibilité (HA) (actif ou en veille) pour chaque groupe de basculement.

Le contexte Admin est un contexte spécial qui gère les connexions de base du châssis (telles que SSH). Il s'agit d'une image de basculement actif/actif.



Paire de basculement dans le basculement actif/actif

Flux de trafic

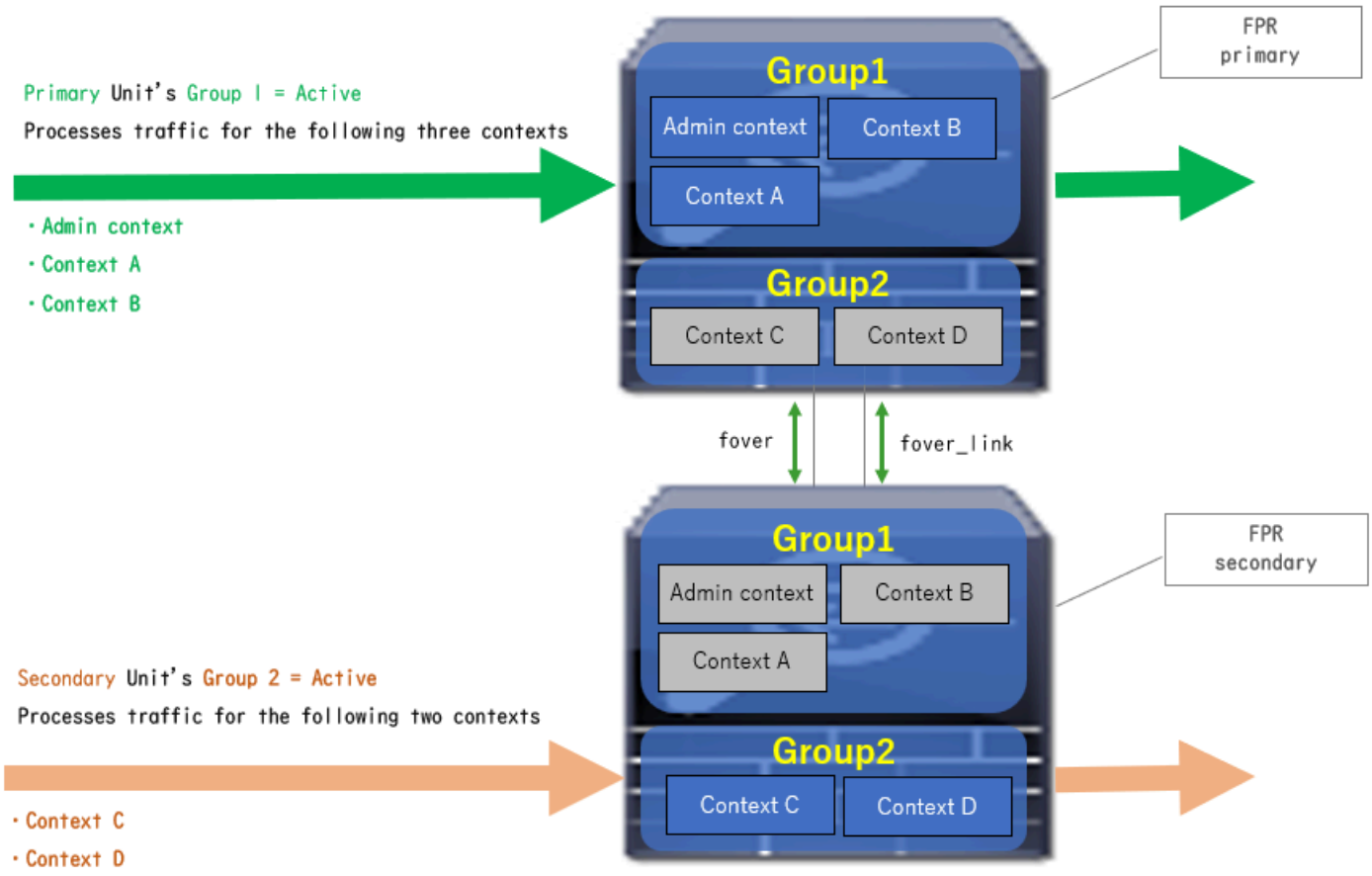
Dans le cas d'un basculement actif/actif, le trafic peut être géré selon les différents modèles présentés dans l'image suivante.

Group	Primary Unit	Secondary Unit	
Group 1	Active	Standby	Both of ASAs process traffic simultaneously
Group 2	Standby	Active	
Group 1	Active	Standby	Only the Primary Unit processes traffic
Group 2	Active	Standby	
Group 1	Standby	Active	Both of ASAs process traffic simultaneously
Group 2	Active	Standby	
Group 1	Standby	Active	Only the Secondary Unit processes traffic
Group 2	Standby	Active	

Flux de trafic

Condition de flux de trafic 1

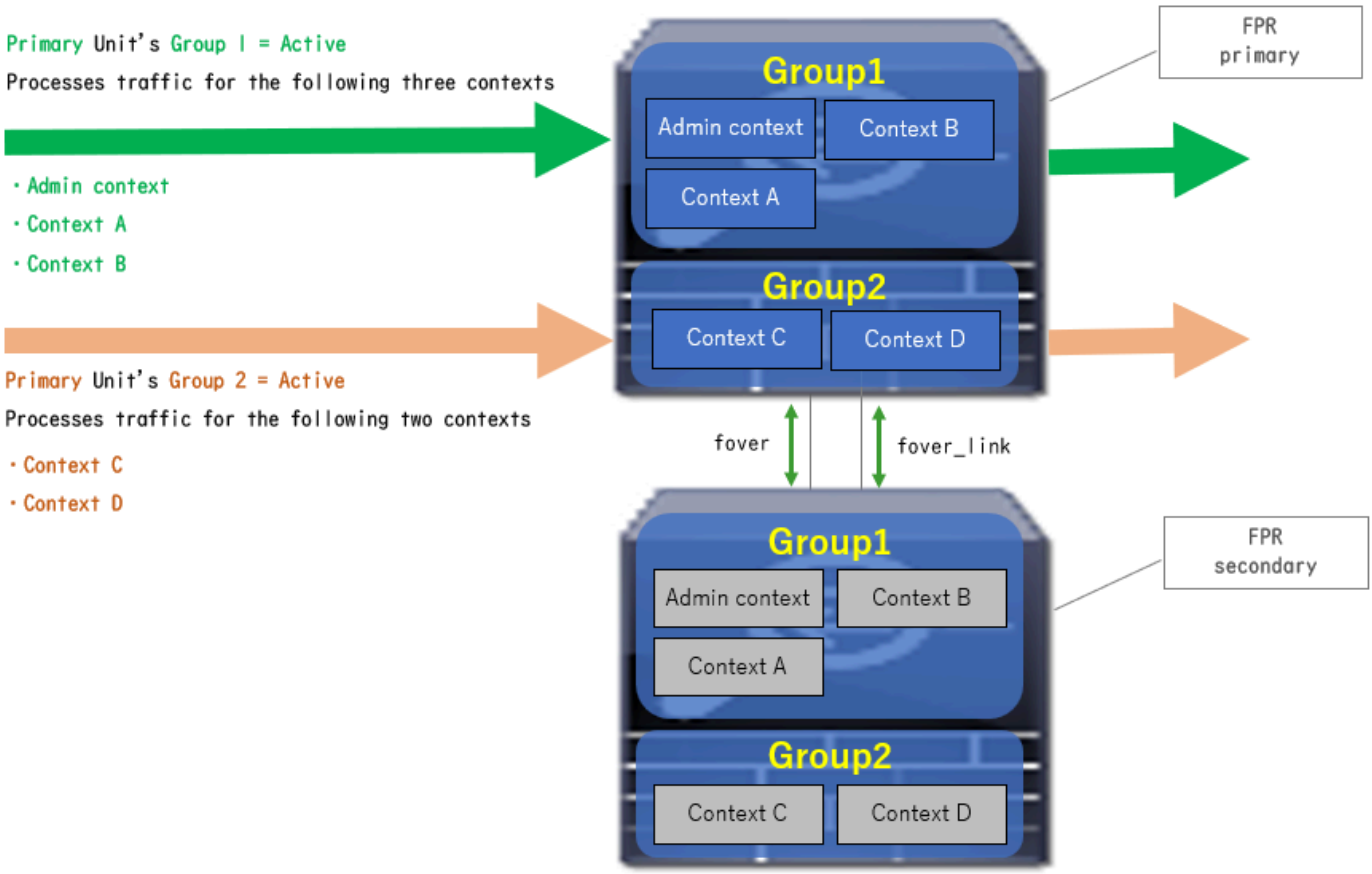
- Unité principale : Groupe 1 = Actif, Groupe 2 = En veille
- Unité secondaire : Groupe 1 = En veille, Groupe 2 = Actif



Condition de flux de trafic 1

Condition de flux de trafic 2

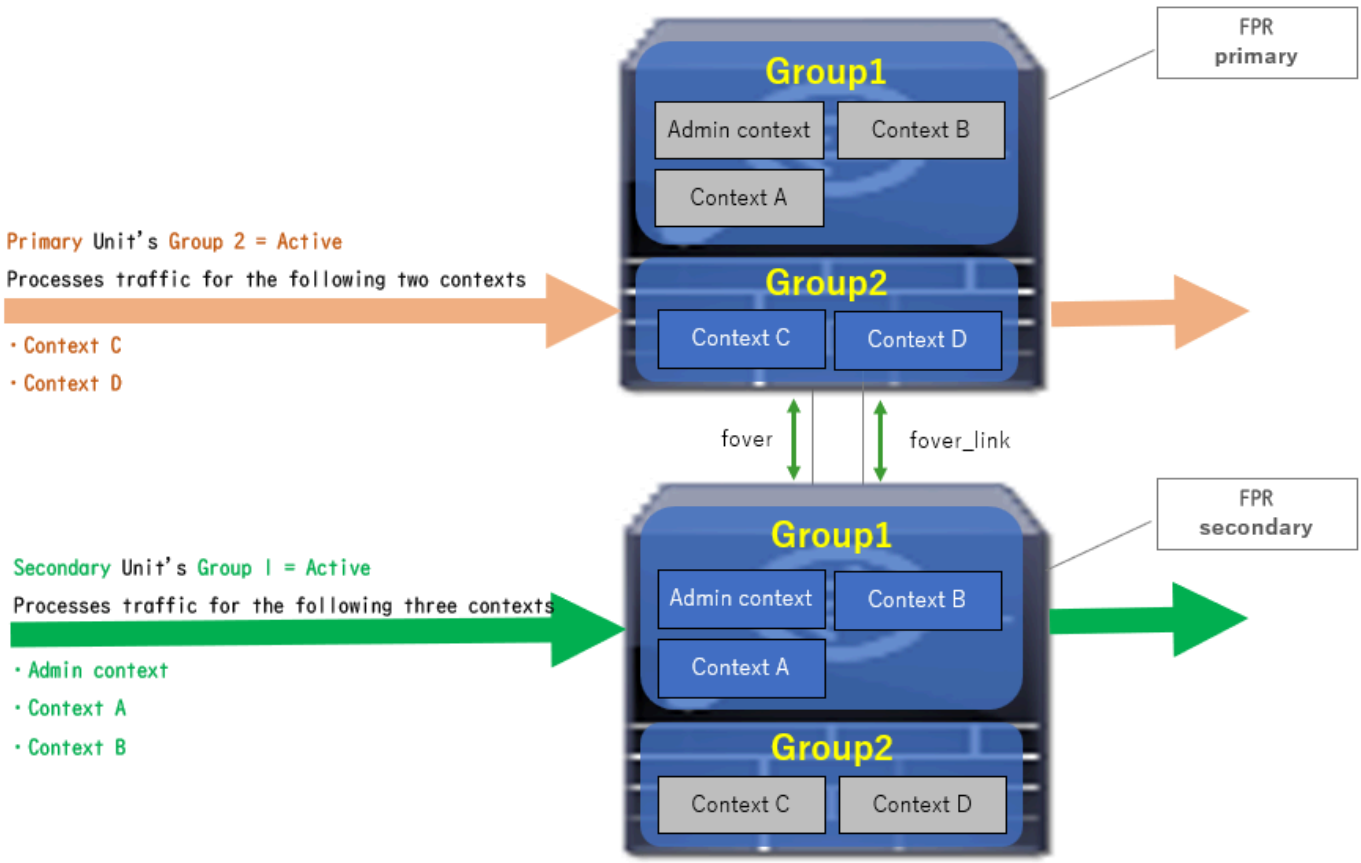
- Unité principale : Groupe 1 = actif, Groupe 2 = actif
- Unité secondaire : Groupe 1 = En veille, Groupe 2 = En veille



Condition de flux de trafic 2

Condition de flux de trafic 3

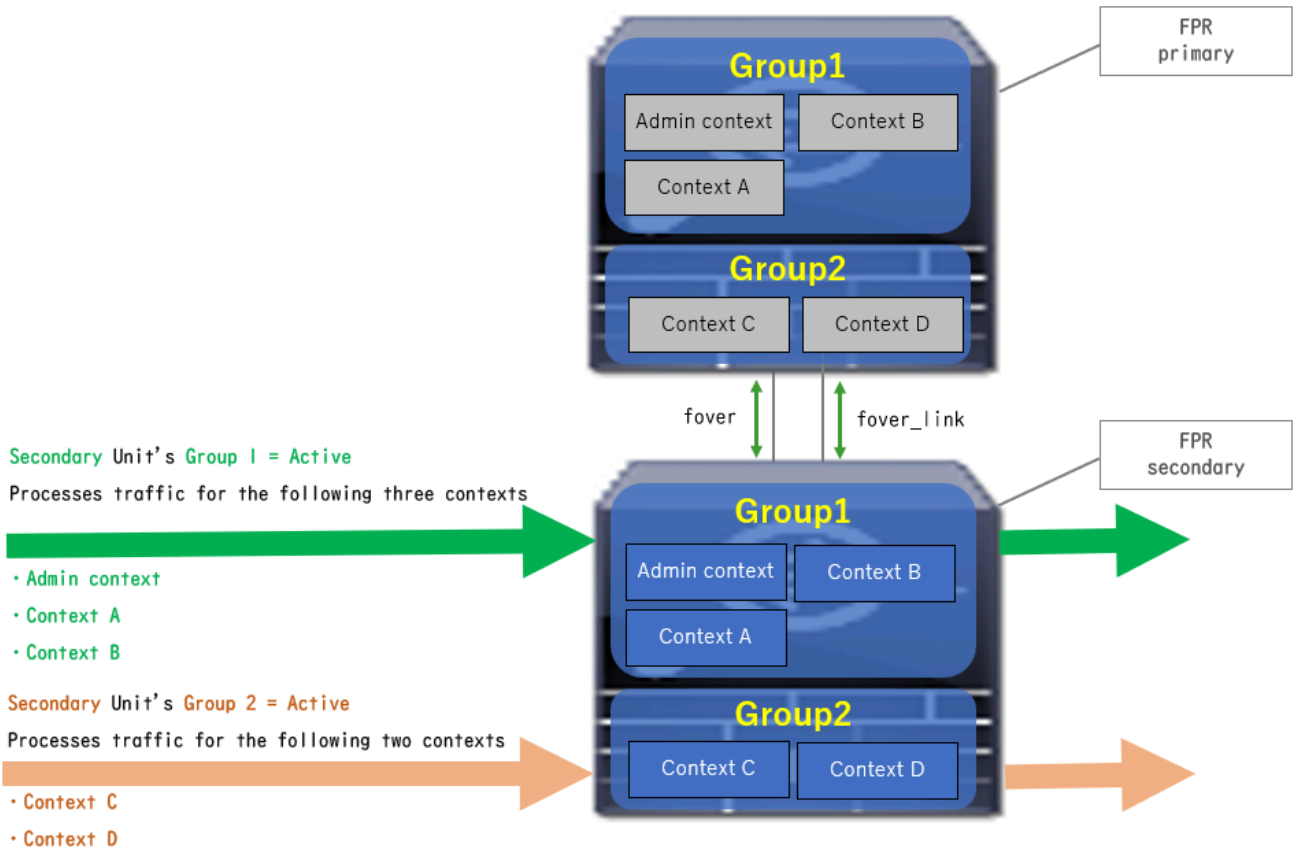
- Unité principale : Groupe 1 = En veille, Groupe 2 = Actif
- Unité secondaire : Groupe 1 = Actif, Groupe 2 = En veille



Condition de flux de trafic 3

Condition de flux de trafic 4

- Unité principale : Groupe 1 = En veille, Groupe 2 = En veille
- Unité secondaire : Groupe 1 = actif, Groupe 2 = actif



Condition de flux de trafic 4

Règles de sélection pour actif/veille

Dans le basculement actif/actif , l'état (actif/veille) de chaque groupe est déterminé par les règles suivantes :

- Supposons que 2 périphériques démarrent pratiquement en même temps, puis que l'une des unités (principale ou secondaire) devient active en premier.
- Une fois le délai de préemption écoulé, le groupe qui a le même rôle dans le châssis et le groupe devient actif.
- En cas d'événement de basculement (tel que l'interface DOWN), l'état du groupe change de la même manière qu'avec le basculement actif/veille.
- L'heure de préemption ne fonctionne pas après le basculement manuel.

Voici un exemple de changement d'état.

- Les deux périphériques démarrent pratiquement en même temps. État A →
- Temps de préemption écoulé. État B →
- Échec du périphérique principal (le basculement est déclenché). État C →
- Préempter le temps écoulé depuis la récupération de l'unité principale après une panne. État D →
- Déclencher manuellement le basculement. État E

Pour plus de détails sur les déclencheurs de basculement et la surveillance de l'état, veuillez vous reporter à Événements de basculement.

1. Les deux périphériques démarrent presque en même temps.

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

État A

2. Le délai de préemption (30 s dans ce document) est écoulé.

After 30 seconds (preempt time)	Active	Standby	Standby	Active

État B

3. Une défaillance (telle que Interface Down) s'est produite dans le groupe 1 de l'unité principale.

Failover event	Standby	Standby	Active	Active

État C

4. Temps de préemption (30 s dans ce document) écoulé depuis que le groupe 1 du périphérique principal a récupéré après une panne.

After 30 seconds since Primary Unit recovered	Active	Standby	Standby	Active

État D

5. Définissez manuellement le groupe 2 de l'unité principale sur Actif.

Manual failover	Active	Active	Standby	Standby

État E

Diagramme du réseau

Ce document présente la configuration et la vérification du basculement actif/actif sur la base de ce schéma.

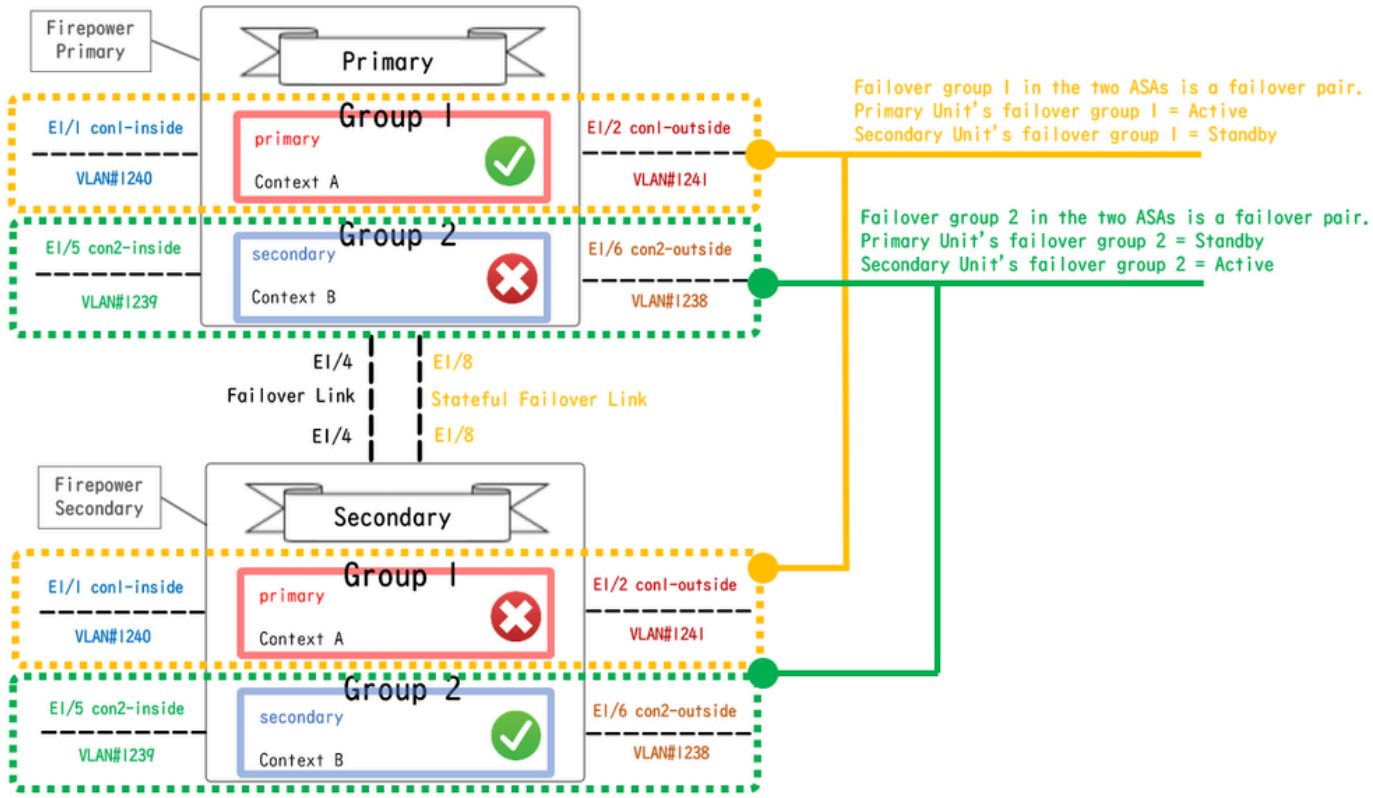


Diagramme de configuration logique

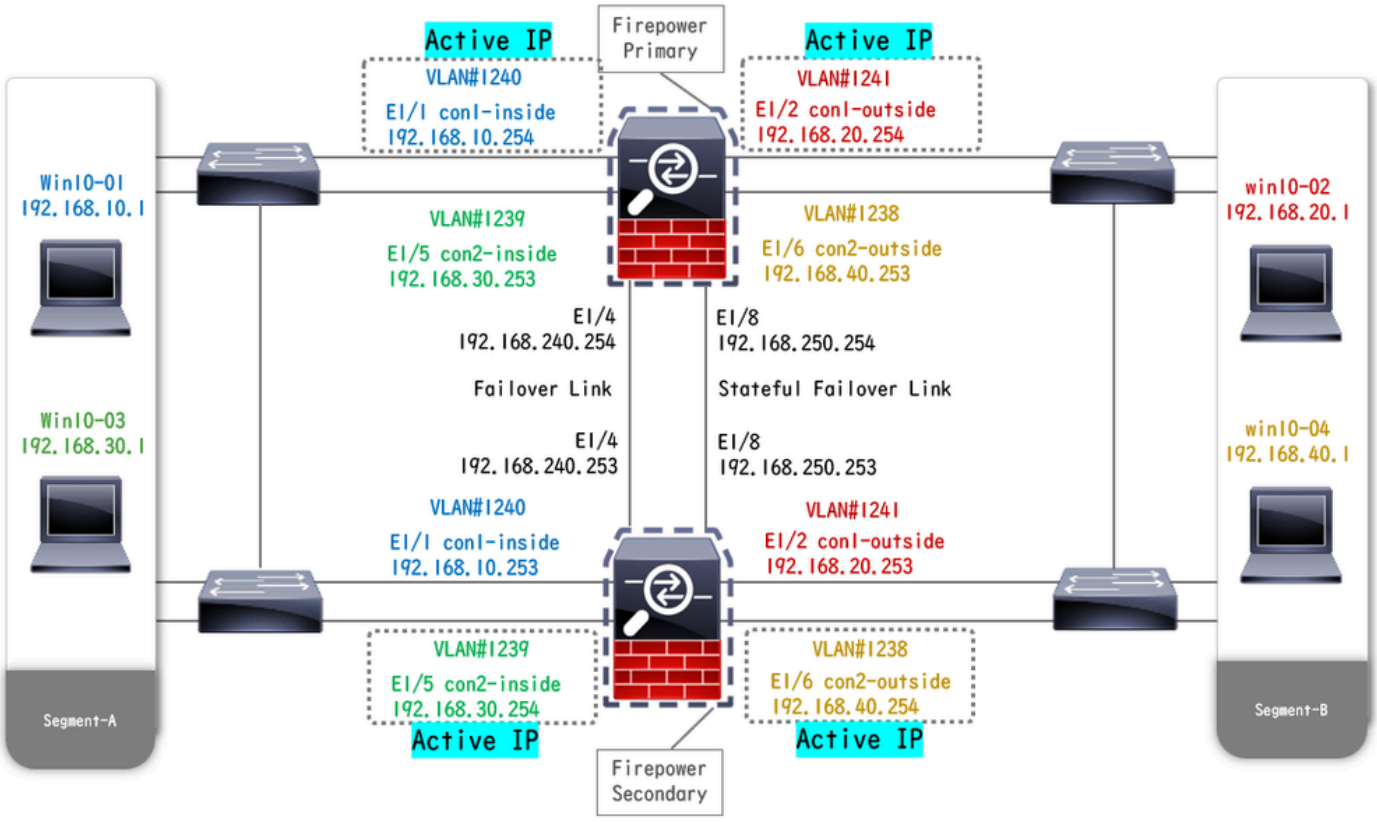
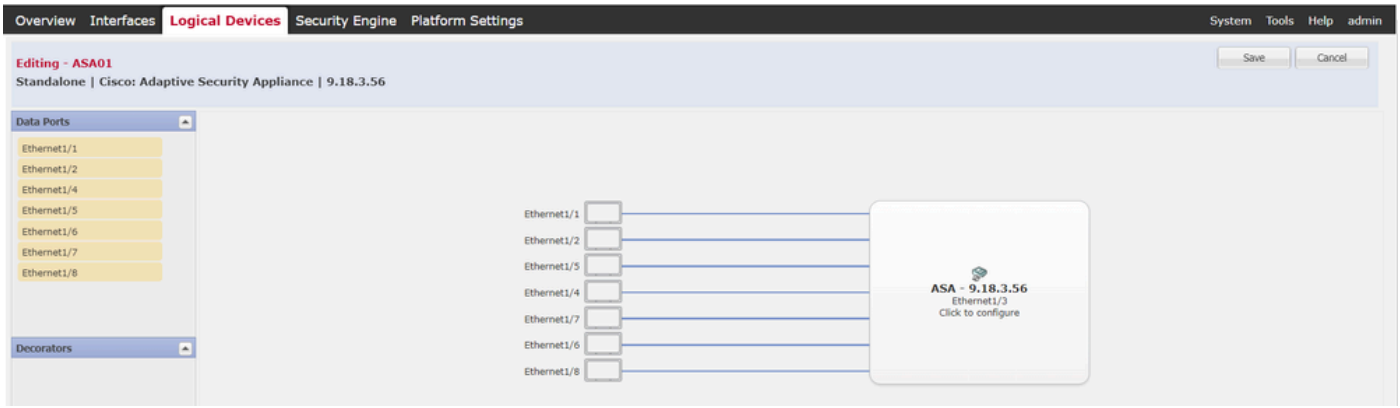


Schéma de configuration physique

Configuration

Étape 1. Pré-configuration des interfaces

Pour les deux Firepower, connectez-vous à l'interface utilisateur graphique FCM. Accédez à Logical Devices > Edit. Ajoutez une interface de données à ASA, comme illustré dans l'image.



Pré-configuration des interfaces

Étape 2. Configuration sur l'unité principale

Connectez-vous à la CLI FXOS principale via SSH ou la console. Exécutez **connect module 1 console** et connect asala commande pour accéder à l'interface de ligne de commande ASA.

a. Configurez le basculement sur l'unité principale (exécutez la commande dans le contexte système de l'unité principale).

```
<#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 192.168.240.253
failover interface ip fover_link 192.168.250.254 255.255.255.0 standby 192.168.250.253

failover group 1

□□□<--- group 1 is assigned to primary by default
preempt 30
failover group 2
secondary
preempt 30
failover
prompt hostname state priority context
```

b. Configurez le groupe de basculement pour le contexte (exécutez la commande dans le contexte système de l'unité principale).

```
<#root>

admin-context admin
```

```
context admin

         <--- admin context is assigned to group 1 by default
allocate-interface E1/3
config-url disk0:/admin.cfg

context con1
allocate-interface E1/1
allocate-interface E1/2
config-url disk0:/con1.cfg

join-failover-group 1

 <--- add con1 context to group 1
!
context con2
allocate-interface E1/5
allocate-interface E1/6
config-url disk0:/con2.cfg

join-failover-group 2

 <--- add con2 context to group 2
```

c. Exécutez changeto context con1pour connecter le contexte con1 à partir du contexte système . Configurez IP pour l'interface du contexte con1 (exécutez la commande dans le contexte con1 de l'unité principale).

```
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 con1-outside
ip address 192.168.20.254 255.255.255.0 standby 192.168.20.253
no shutdown
```

d. Exécutez changeto context con2pour connecter le contexte con2 à partir du contexte système . Configurez IP pour l'interface du contexte con2 (exécutez la commande dans le contexte con2 de l'unité principale).

```
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 con2-outside
ip address 192.168.40.254 255.255.255.0 standby 192.168.40.253
no shutdown
```

Étape 3. Configuration sur l’unité secondaire

a. Connectez-vous à l'interface de ligne de commande FXOS secondaire via SSH ou console. Configurez le basculement sur l'unité secondaire (exécutez la commande dans le contexte système de l'unité secondaire).

```
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 192.168.240.253
failover interface ip fover_link 192.168.250.254 255.255.255.0 standby 192.168.250.253
```

b. Exécutez la commande failover(exécutée dans le contexte système de l'unité secondaire).

```
failover
```

Étape 4 : confirmation de l’état de basculement après la synchronisation réussie

a. Exécutershow failoverdans le contexte système de l'unité secondaire.

```
<#root>

asa#

show failover


Failover On
Failover unit Secondary
Failover LAN Interface: fover Ethernet1/4 (up)
Version: Ours 9.18(3)56, Mate 9.18(3)56
Serial Number: Ours FCH23157YFY, Mate FCH23037U8R
Group 1 last failover at: 17:00:56 JST Jan 11 2024
Group 2 last failover at: 17:00:56 JST Jan 11 2024

This host:

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 con1-outside (192.168.20.253): Unknown (Waiting)
con2 Interface con2-inside (192.168.30.253): Unknown (Waiting)
con2 Interface con2-outside (192.168.40.253): Normal (Waiting)

Other host:

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)

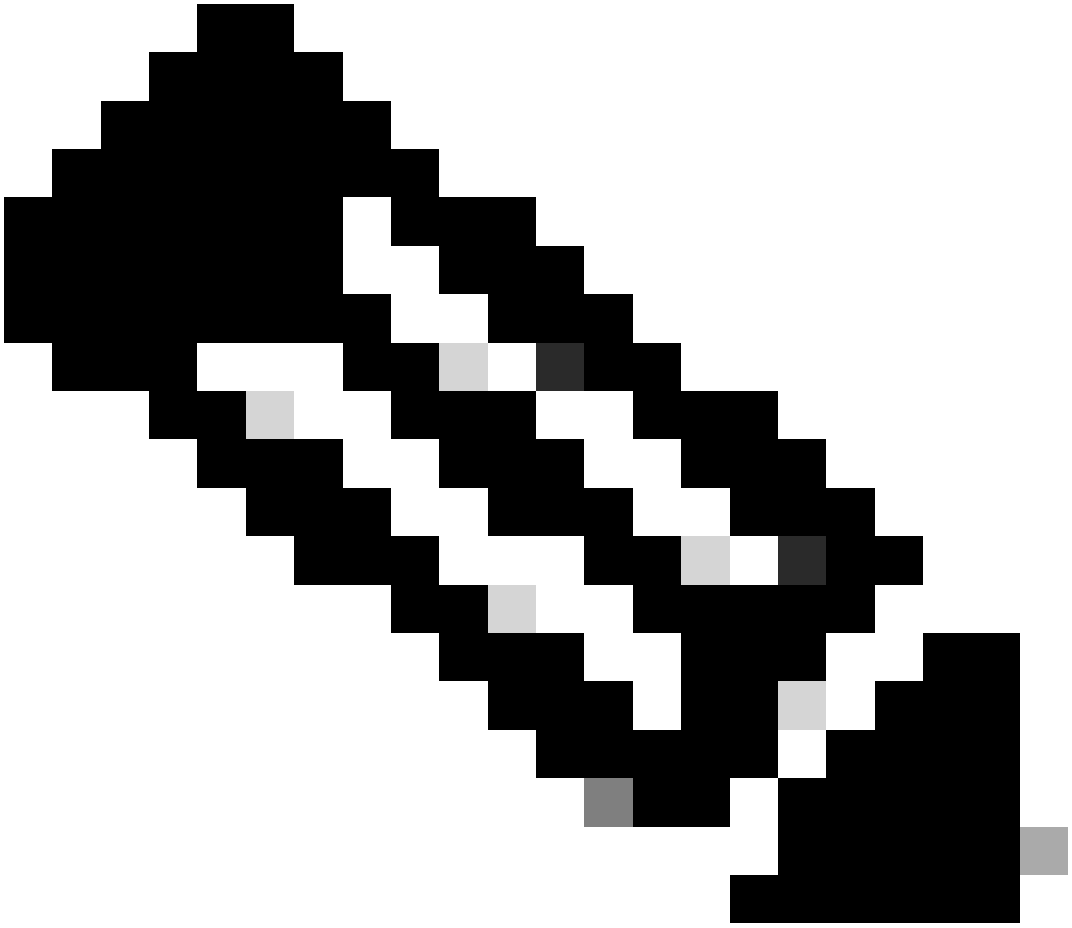
con1 Interface con1-inside (192.168.10.254): Normal (Monitored)
con1 Interface con1-outside (192.168.20.254): Normal (Monitored)
con2 Interface con2-inside (192.168.30.254): Normal (Waiting)
con2 Interface con2-outside (192.168.40.254): Normal (Waiting)

Stateful Failover Logical Update Statistics
Link : fover_link Ethernet1/8 (up)
```

b. (Facultatif) Exécutez **no failover active group 2** la commande pour basculer manuellement le groupe 2 de l'unité principale vers l'état Veille (exécuté dans le contexte système de l'unité principale). Cela peut équilibrer la charge du trafic via le pare-feu.

<#root>

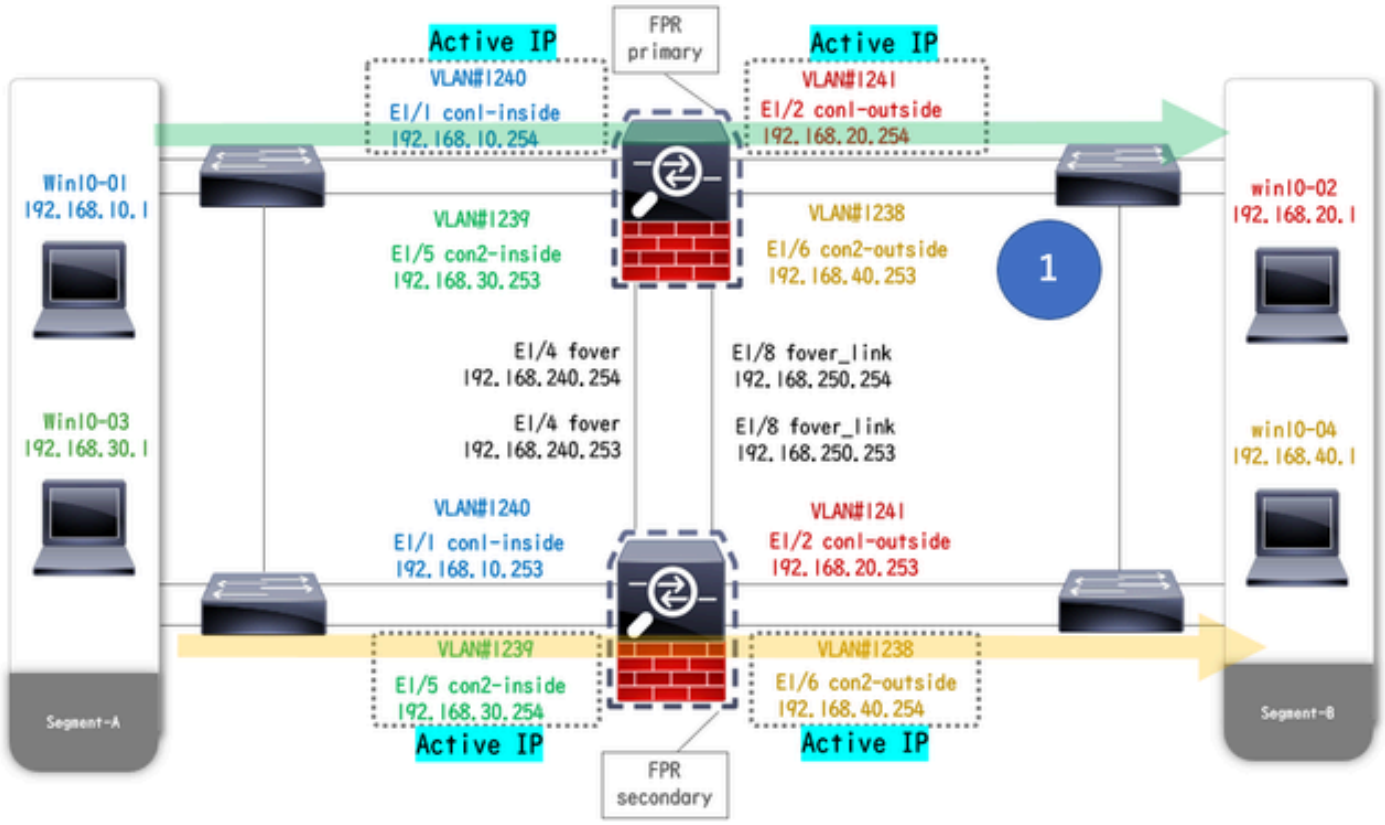
```
no failover active group 2
```



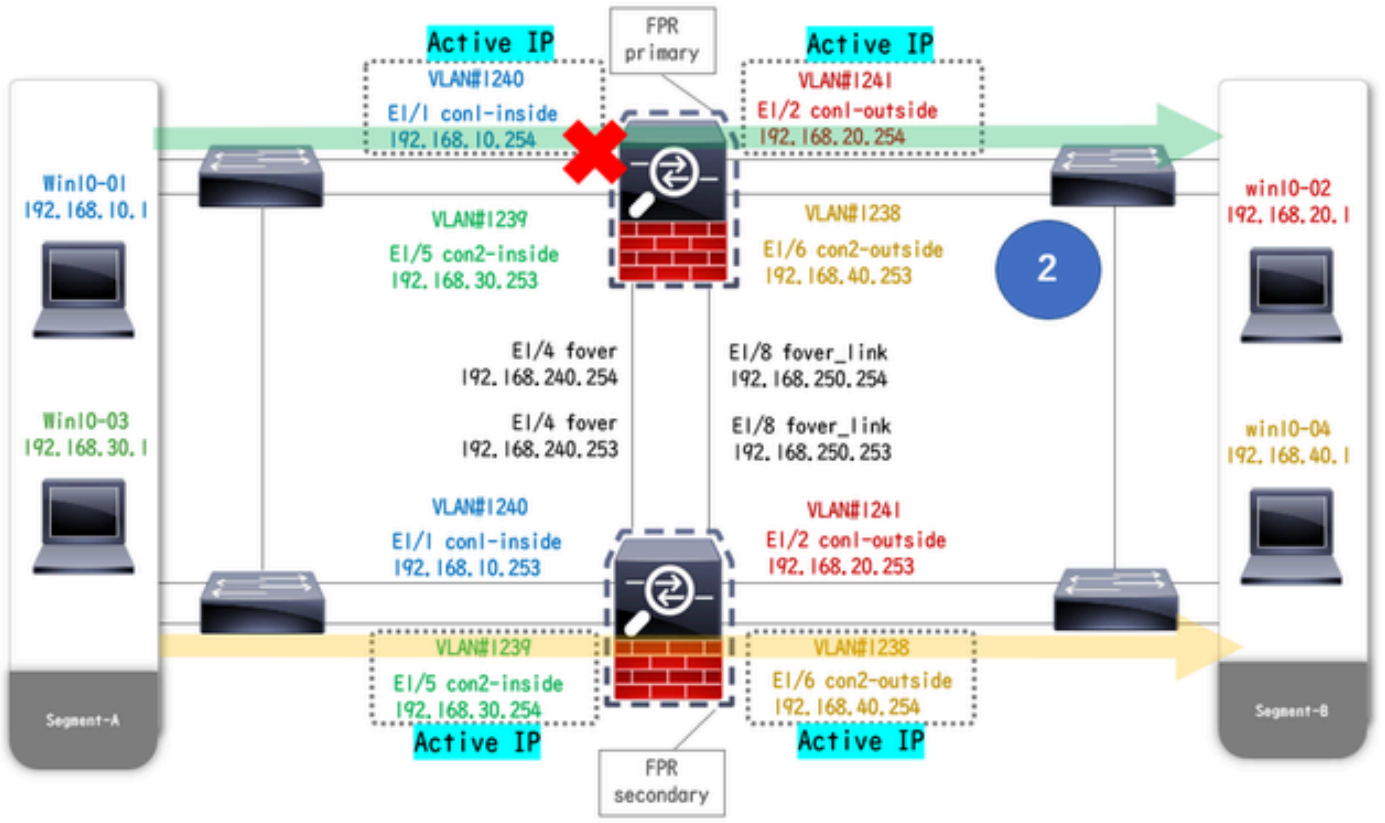
Remarque : Si vous exécutez cette commande, l'état du basculement correspond à la condition de flux de trafic 1.

Vérifier

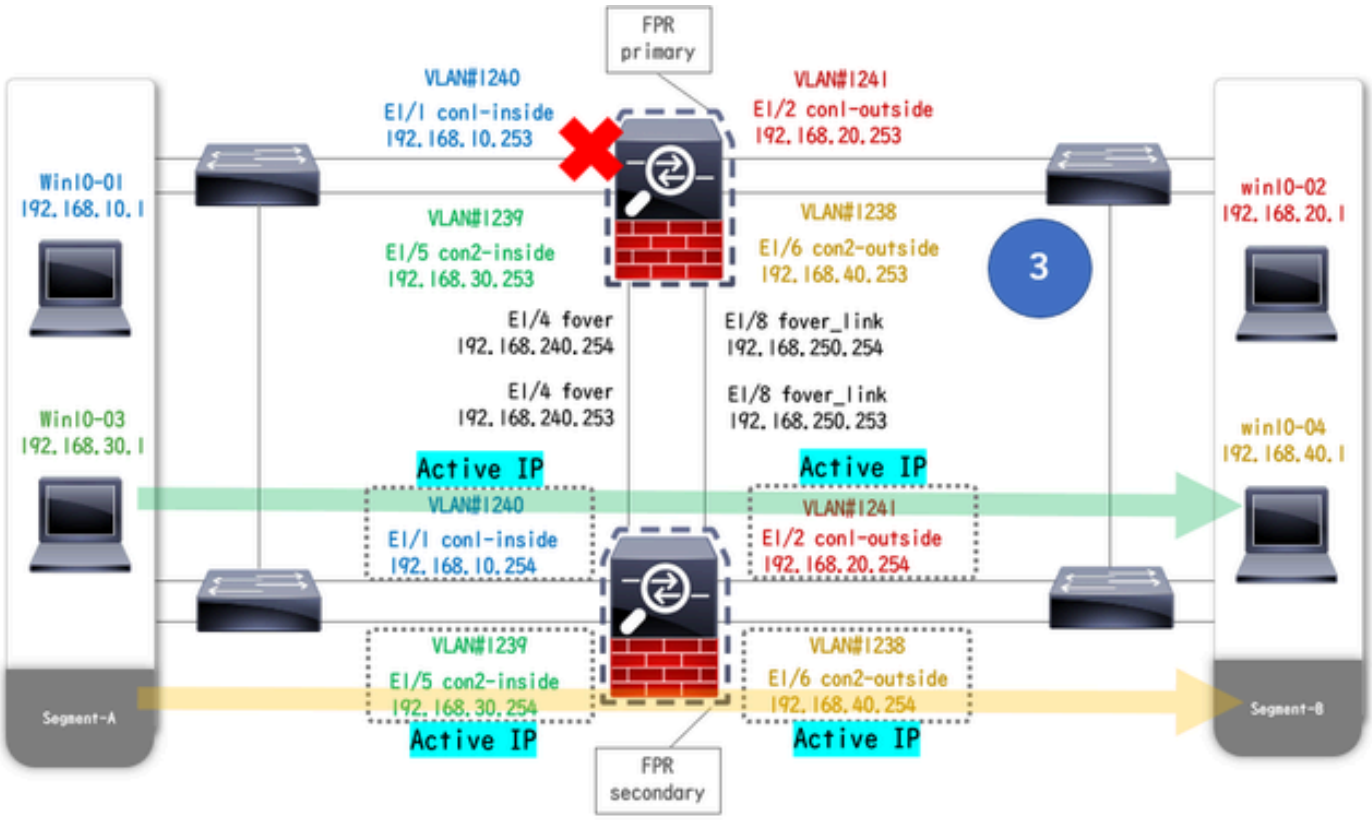
Lorsque E1/1 tombe en PANNE, le basculement du groupe 1 est déclenché et les interfaces de données côté veille (unité secondaire) prennent le relais des adresses IP et MAC de l'interface active d'origine, garantissant ainsi que le trafic (connexion FTP dans ce document) sera transmis en continu par les ASA.



Avant la désactivation de la liaison



Pendant la liaison désactivée



Basculement déclenché

Étape 1 : établissement d'une connexion FTP de Win10-01 à Win10-02

Étape 2 : confirmation de la connexion FTP avant le basculement

Exécutez changeto context con1pour connecter le contexte con1 à partir du contexte système. Vérifiez qu'une connexion FTP est établie dans les deux unités 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

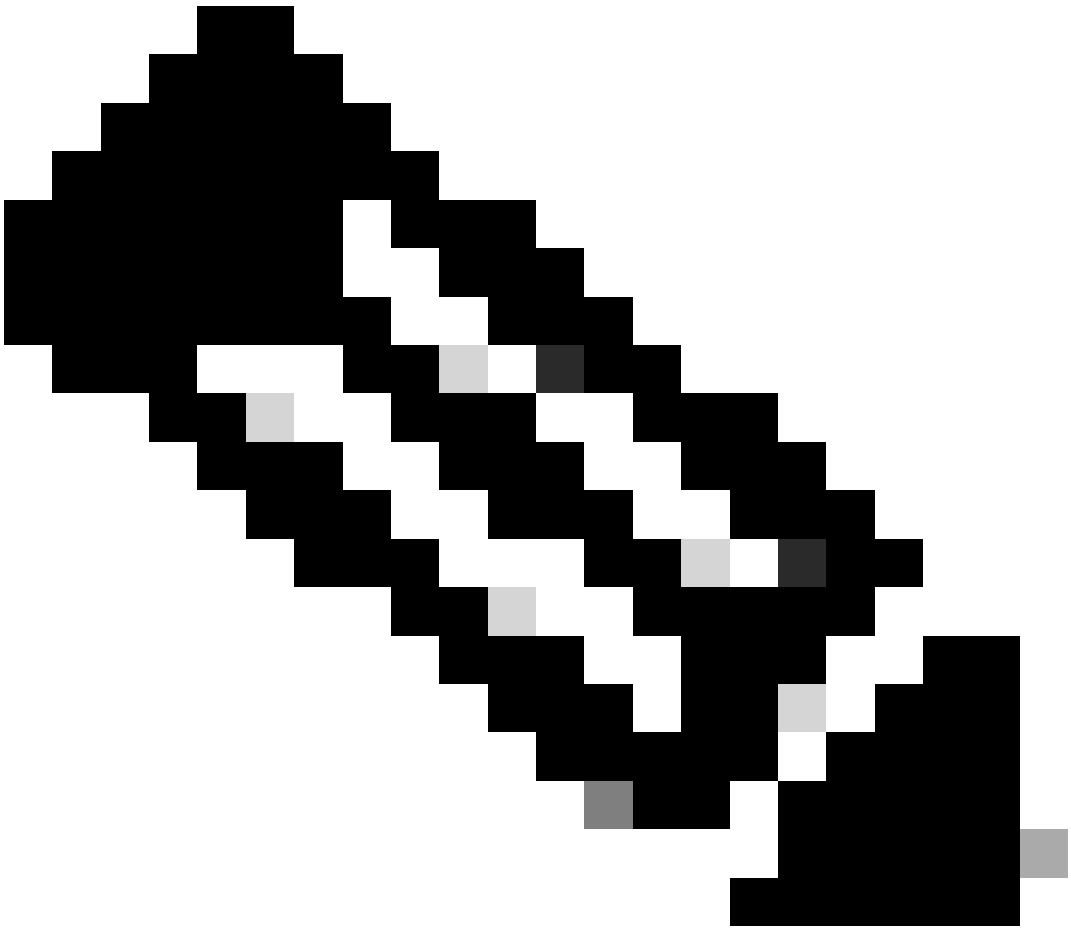
con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

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

Étape 3. LinkDOWN E1/1 de l’unité principale

Étape 4. Confirmation du statut de basculement

Dans le contexte du système, vérifiez que le basculement se produit dans le groupe 1.



Remarque : L'état du basculement correspond à la condition de flux de trafic 4.

<#root>

asa/act/sec#

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: fover Ethernet1/4 (up)
......
Group 1 last failover at: 20:00:16 JST Jan 11 2024
Group 2 last failover at: 17:02:33 JST Jan 11 2024

This host:
```

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 con1-outside (192.168.20.254): Normal (Waiting)
con2 Interface con2-inside (192.168.30.254): Normal (Monitored)
con2 Interface con2-outside (192.168.40.254): Normal (Monitored)

Other host:
```

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 con1-outside (192.168.20.253): Normal (Waiting)
con2 Interface con2-inside (192.168.30.253): Normal (Monitored)
con2 Interface con2-outside (192.168.40.253): Normal (Monitored)
```

Étape 5. Confirmation de la connexion FTP après le basculement

Exécutez changeto context con1pour connecter le contexte con1 à partir du contexte système, vérifiez que la connexion FTP n'est pas interrompue.

<#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
```

Étape 6. Confirmer le comportement de l'heure de préemption

LinkUP E1/1 de l'unité principale et attendre 30 secondes (temps de préemption), l'état de basculement revient à l'état d'origine (correspondance du flux de trafic dans le modèle 1).

<#root>

asa/stby/pri#

Group 1 preempt mate

```
□□□□<--- Failover is triggered automatically, after the preempt time has passed

asa/act/pri# show failover
Failover On
Failover unit Primary
Failover LAN Interface: fover Ethernet1/4 (up)
......
Group 1 last failover at: 11:02:33 UTC Jan 11 2024
Group 2 last failover at: 08:02:45 UTC Jan 11 2024

This host:
```

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 con1-outside (192.168.20.254): Normal (Monitored)
con2 Interface con2-inside (192.168.30.253): Normal (Monitored)
con2 Interface con2-outside (192.168.40.253): Normal (Monitored)

Other host:
```

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)

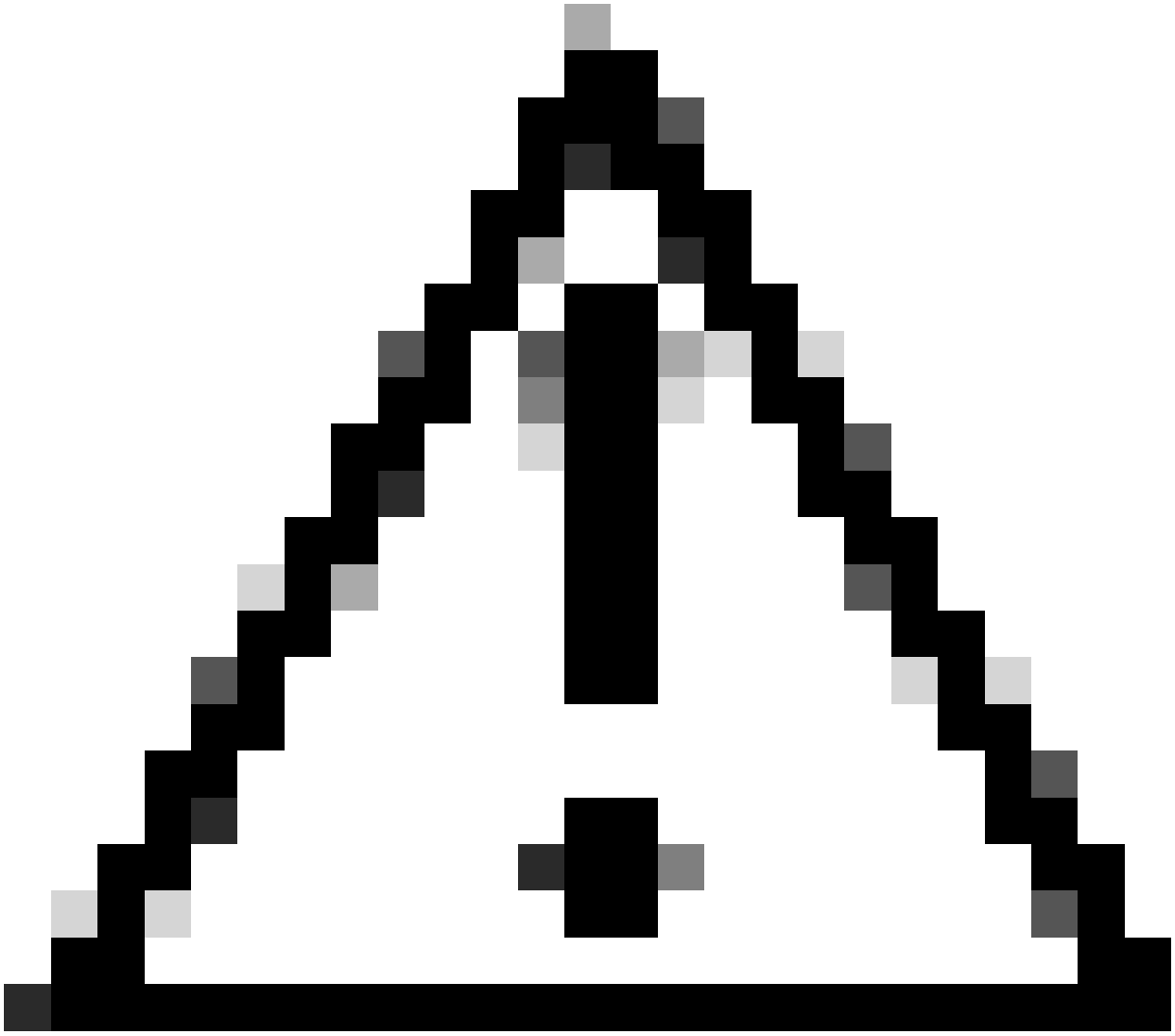
con1 Interface con1-inside (192.168.10.253): Normal (Monitored)
con1 Interface con1-outside (192.168.20.253): Normal (Monitored)
con2 Interface con2-inside (192.168.30.254): Normal (Monitored)
con2 Interface con2-outside (192.168.40.254): Normal (Monitored)
```

Adresse MAC virtuelle

Dans le cas d'un basculement actif/actif, l'adresse MAC virtuelle (valeur définie manuellement, valeur générée automatiquement ou valeur par défaut) est toujours utilisée. L'adresse MAC virtuelle active est associée à l'interface active.

Configuration manuelle de l'adresse MAC virtuelle

Afin de définir manuellement l'adresse MAC virtuelle pour les interfaces physiques, la `mac address`commande ou la commande `mac-address`(dans le mode de réglage l/F) peut être utilisée. Ceci est un exemple de configuration manuelle d'une adresse MAC virtuelle pour l'interface physique E1/1.



Mise en garde : Évitez d'utiliser ces deux types de commandes sur le même périphérique.

<#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 | in MAC
MAC address
```

1234.1234.0001

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

asa/stby/sec# changeto context con1
asa/stby/sec/con1# show interface E1/1 | in MAC
MAC address
```

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
asa/stby/sec/con1# show interface E1/1 | in MAC
MAC address
```

1234.1234.0002

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

Configuration automatique de l'adresse MAC virtuelle

La génération automatique d'adresses MAC virtuelles est également prise en charge. Vous pouvez y parvenir à l'aide de la commande mac-address auto
. Le format de l'adresse MAC virtuelle est A2 xx.yyzz.zzzz, qui est généré automatiquement.
A2 : valeur fixe
xx.yy : généré par le <préfixe préfixe> spécifié dans l'option de commande (le préfixe est converti au format hexadécimal, puis inséré par ordre inverse).
zz.zzzz : généré par un compteur interne

Ceci est un exemple de génération d'adresse MAC virtuelle par **mac-address auto** commande pour l'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
```

Paramètre par défaut de l'adresse MAC virtuelle

Si aucune génération automatique ou manuelle d'adresse MAC virtuelle n'est définie, l'adresse MAC virtuelle par défaut est utilisée.

Pour plus d'informations sur l'adresse MAC virtuelle par défaut, veuillez vous reporter à Command Default of mac address dans le Guide de référence des commandes de la gamme Cisco Secure Firewall ASA.

Mise à niveau

Vous pouvez obtenir une mise à niveau sans temps d'arrêt d'une paire de basculement actif/actif à l'aide de CLI ou ASDM. Pour plus d'informations, consultez Mise à niveau d'une paire de basculement actif/actif.

Informations connexes

- Mettre à niveau une paire basculement actif/actif à l'aide de la CLI
- Adresse MAC :
- Assistance technique de Cisco et téléchargements

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.