Firepower 4100シリーズでのASAアクティブ/アクティブフェールオーバーの設定

内容

はじめに

このドキュメントでは、Cisco Firepower 4145 NGFWアプライアンスでアクティブ/アクティブフェールオーバーを設定する方法について説明します。

前提条件

要件

次の項目に関する専門知識があることが推奨されます。

- Cisco適応型セキュリティアプライアンス(ASA)でのアクティブ/スタンバイフェールオーバー。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firepower 4145 NGFWアプライアンス(ASA)9.18(3)56
- Firepower eXtensibleオペレーティングシステム(FXOS)2.12(0.498)
- Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

アクティブ/アクティブフェールオーバーは、マルチコンテキストモードで実行されているセキュリティアプライアンスでのみ使用できます。このモードでは、ASAはコンテキストと呼ばれる複数の仮想デバイスに論理的に分割されます。各コンテキストは、独自のセキュリティポリシー、インターフェイス、および管理者を持つ独立したデバイスとして動作します。

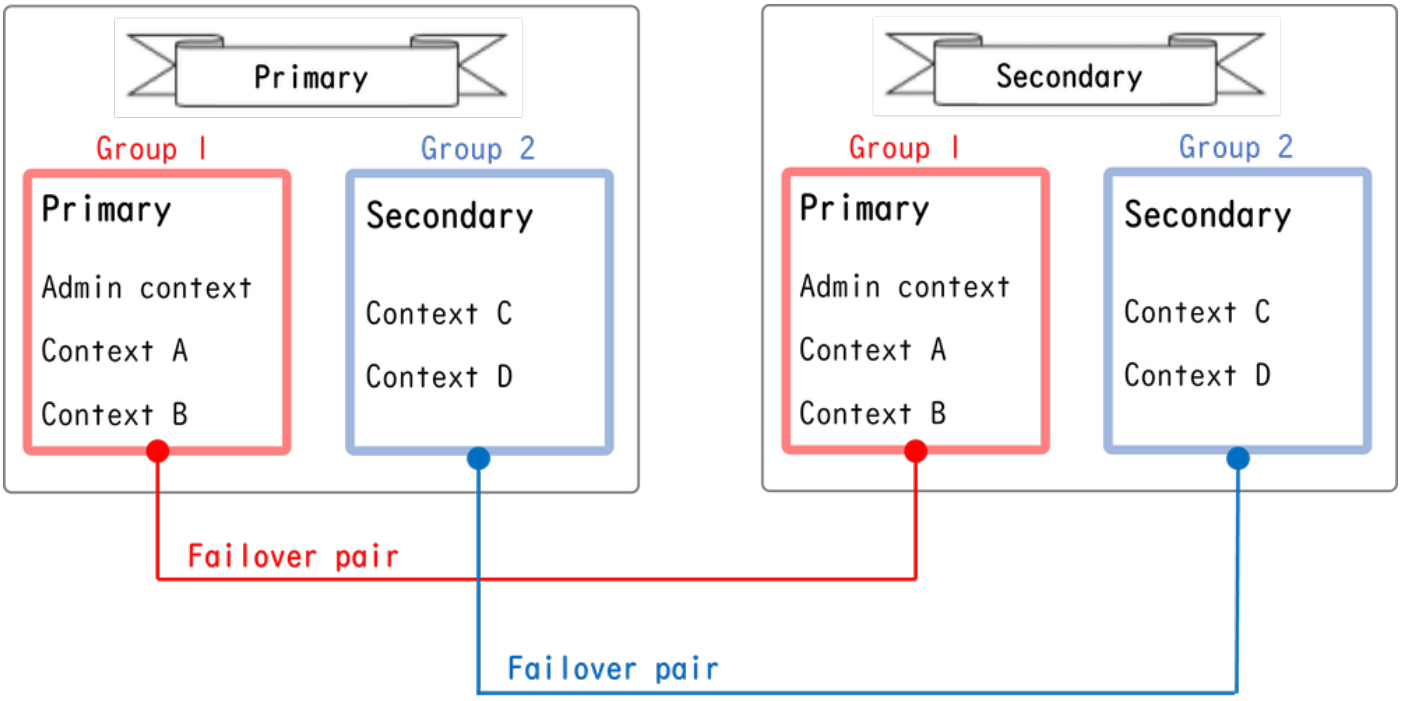
アクティブ/アクティブフェールオーバーは、2台のFirepowerデバイスがトラフィックを同時に通過できるようにする適応型セキュリティアプライアンス(ASA)の機能です。 この設定は、通常、スループットを最大化するために2つのデバイス間でトラフィックを分割するロードバランシングシナリオで使用されます。また、冗長性の目的でも使用されるため、一方のASAに障害が発生しても、他方のASAがサービスを中断せずに引き継ぐことができます。

ASAアクティブ/アクティブフェールオーバーのメカニズム

アクティブ/アクティブフェールオーバーの各コンテキストは、手動でグループ1またはグループ2に割り当てられます。管理コンテキストは、デフォルトでグループ1に割り当てられます。2台のシャーシ（ユニット）の同じグループ（グループ1またはグループ2）がフェールオーバーペアを形成し、冗長機能を実現します。各フェールオーバーペアの動作は、アクティブ/スタンバイフェールオーバーの動作と基本的に同じです。アクティブ/スタンバイフェールオーバーの詳細は、「アクティブ/スタンバイフェールオーバーの設定」を参照してください。アクティブ/アクティブフェールオーバーでは、各シャーシのロール（プライマリまたはセカンダリ）に加えて、各グループにはロール（プライマリまたはセカンダリ）もあります。これらのロールはユーザによって

手動で事前に設定され、各フェールオーバーグループのハイアベイラビリティ(HA)ステータス（アクティブまたはスタンバイ）を決定するために使用されます。

管理コンテキストは、基本的なシャーシ管理（SSHなど）接続を処理する特殊なコンテキストです。これはアクティブ/アクティブフェールオーバーのイメージです。



アクティブ/アクティブフェールオーバーでのフェールオーバーペア

Traffic flow

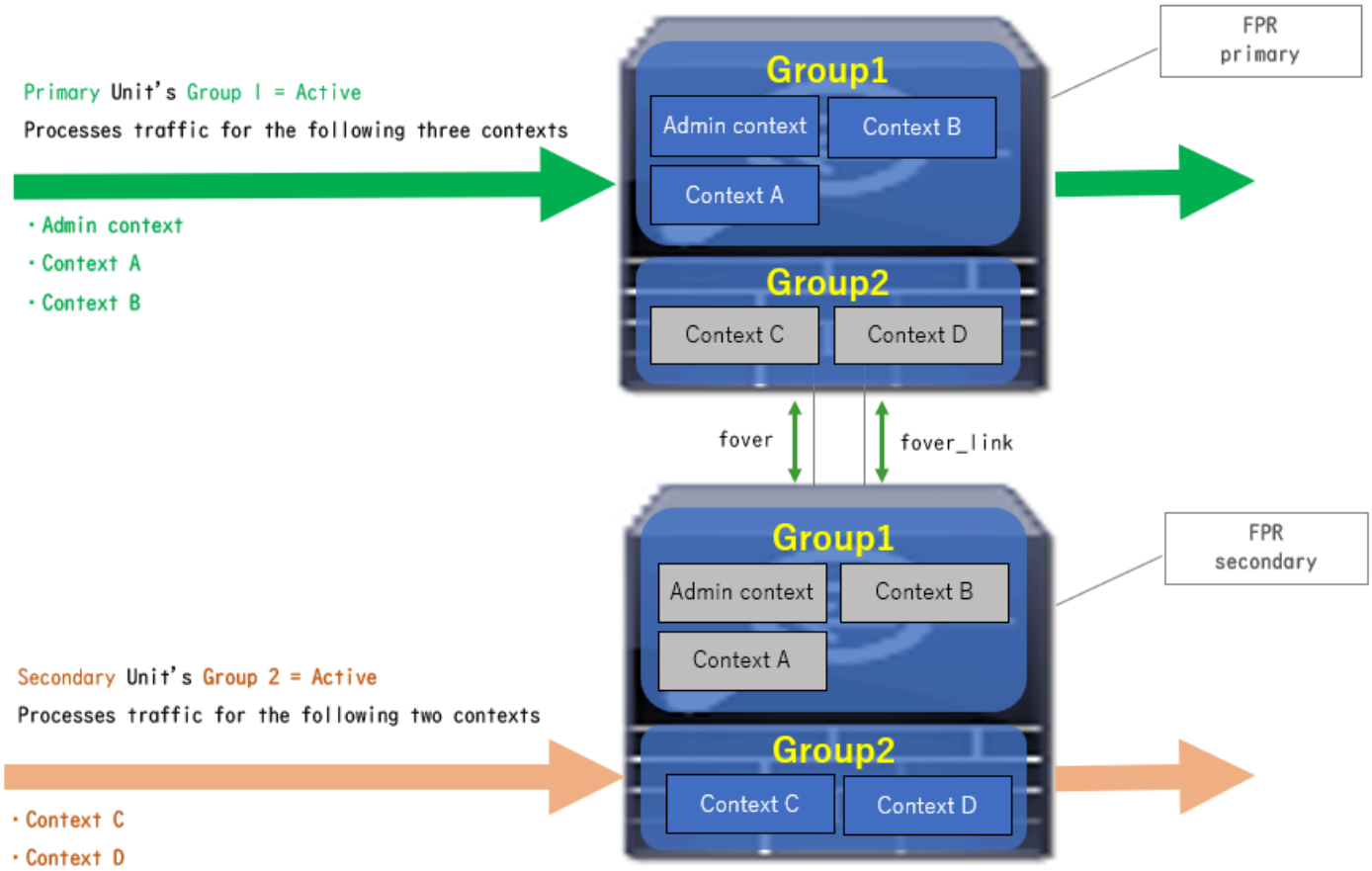
アクティブ/アクティブフェールオーバーでは、次の図に示すようにいくつかのパターンでトラフィックを処理できます。

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	

Traffic flow

トラフィックフロー条件1

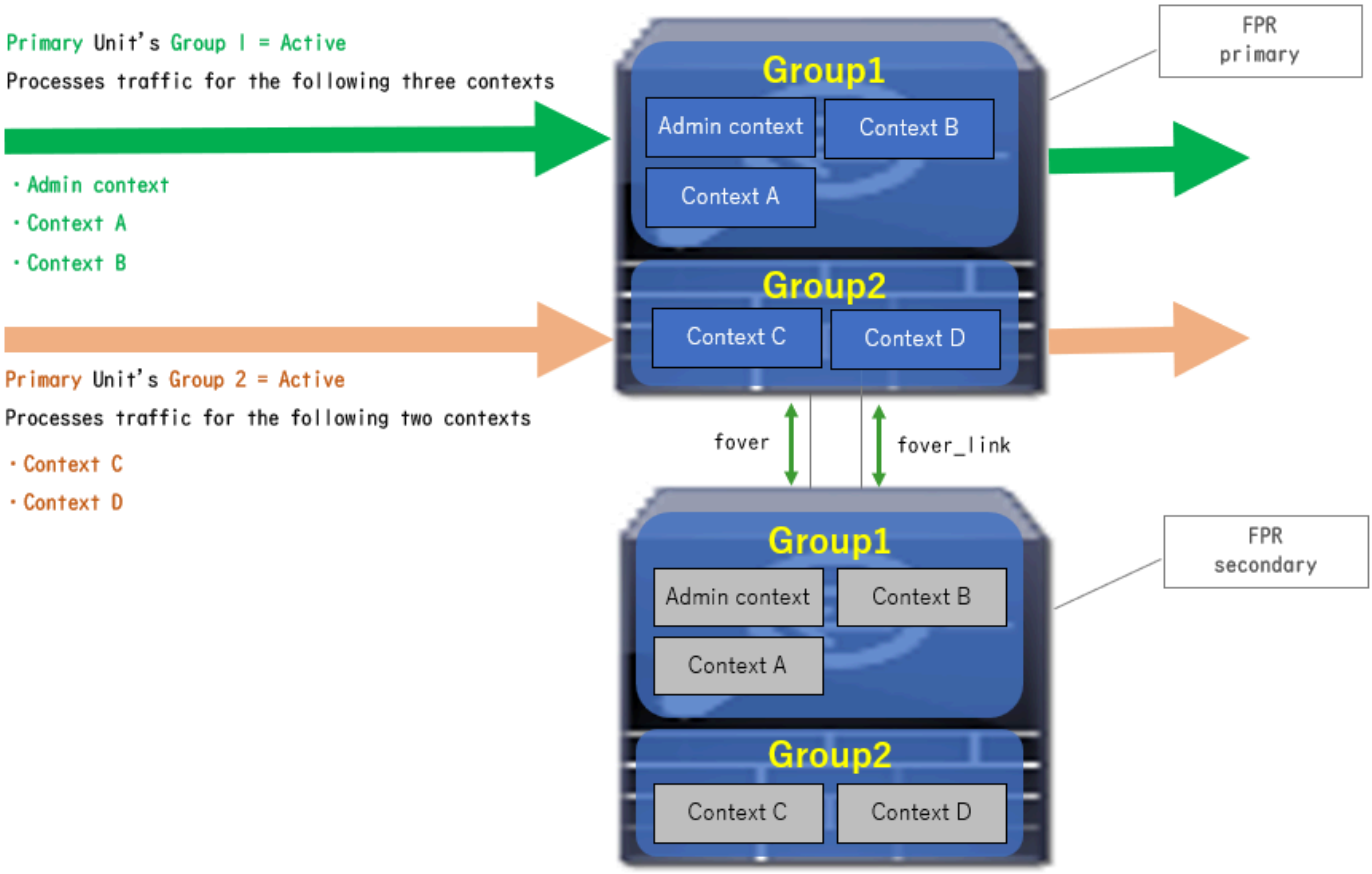
- プライマリユニット：グループ1 =アクティブ、グループ2 =スタンバイ
- セカンダリユニット：グループ1 =スタンバイ、グループ2 =アクティブ



トラフィックフロー条件1

トラフィックフロー条件2

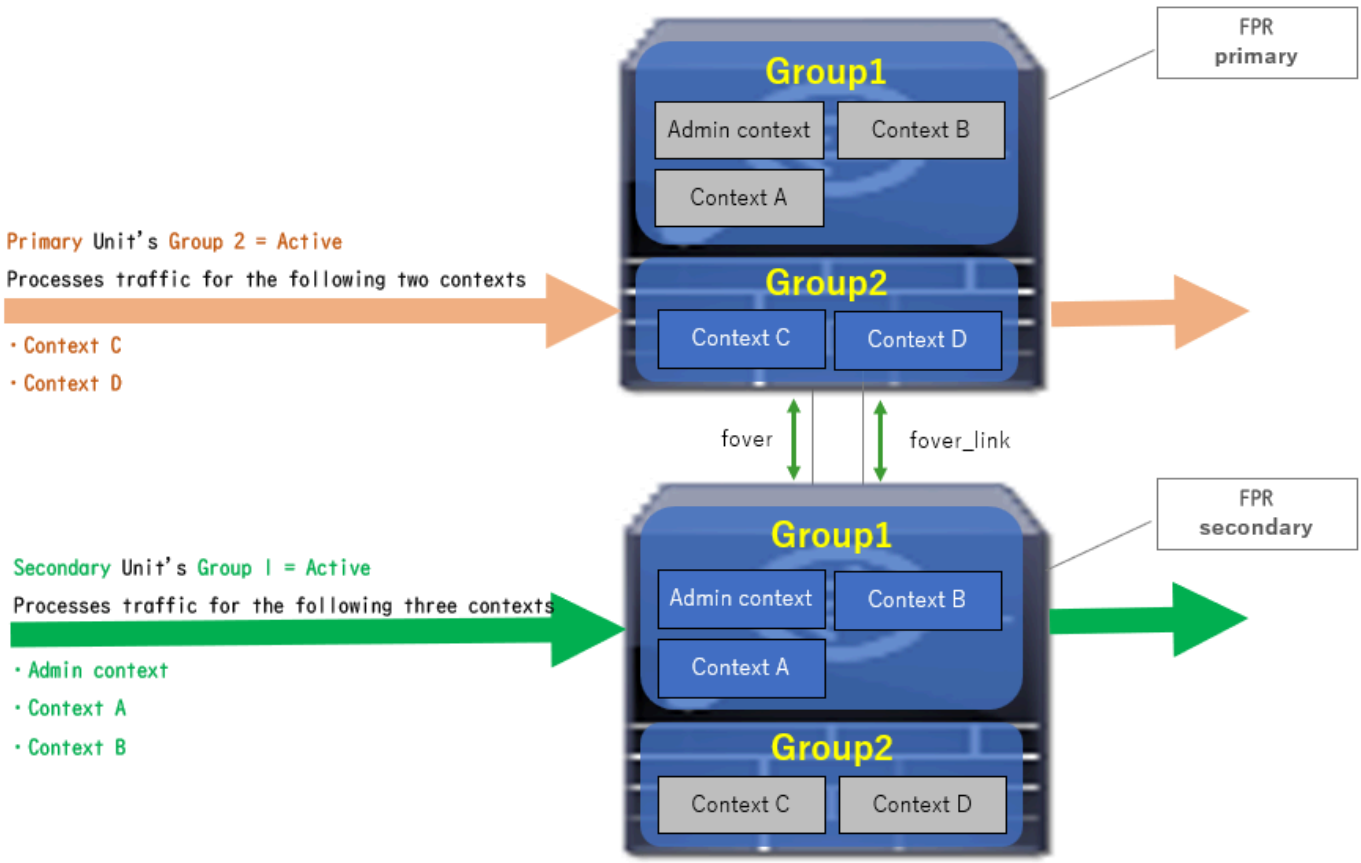
- プライマリユニット：グループ1 =アクティブ、グループ2 =アクティブ
- セカンダリユニット：グループ1 =スタンバイ、グループ2 =スタンバイ



トラフィックフロー条件2

トラフィックフロー条件3

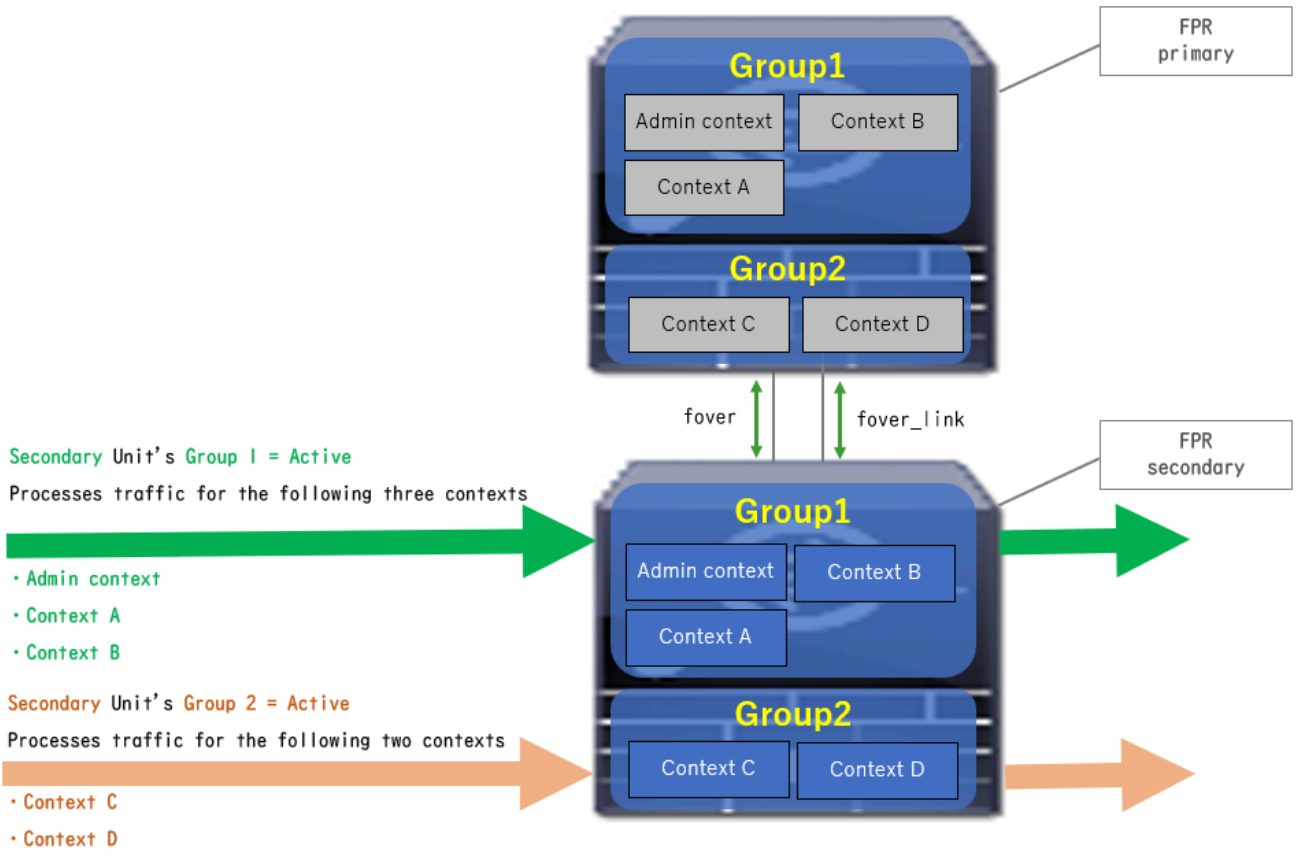
- プライマリユニット：グループ1 =スタンバイ、グループ2 =アクティブ
- セカンダリユニット：グループ1 =アクティブ、グループ2 =スタンバイ



トラフィックフロー条件3

トラフィックフロー状態4

- プライマリユニット：グループ1 =スタンバイ、グループ2 =スタンバイ
- セカンダリユニット：グループ1 =アクティブ、グループ2 =アクティブ



トラフィックフロー状態4

アクティブ/スタンバイの選択ルール

アクティブ/アクティブフェールオーバー（アクティブ/スタンバイ）では、各グループのステータス（アクティブ/スタンバイ）は次のルールによって決定されます。

- 2台のデバイスがほぼ同時に起動すると、最初にいずれかのユニット（プライマリまたはセカンダリ）がアクティブになります。
- プリエンプト時間が経過すると、シャーシとグループで同じロールを持つグループがアクティブになります。
- フェールオーバーイベント（インターフェイスのダウンなど）が発生すると、アクティブ/スタンバイフェールオーバーの場合と同様に、グループのステータスが変化します。
- 手動でフェールオーバーを実行した後、プリエンプション時間が機能しません。

ステータス変更の例を次に示します。

- 両方のデバイスがほぼ同時に起動します。ステータスA→
- プリエンプト時間が経過しました。ステータスB→
- プライマリデバイスの障害（フェールオーバーがトリガーされる）。ステータスC→
- プライマリデバイスが障害から回復してから経過したプリエンプト時間。ステータスD→
- フェールオーバーを手動でトリガーします。ステータスE

フェールオーバーのトリガーとヘルスモニタリングの詳細については、「フェールオーバーイベント」を参照してください。

1. 両方のデバイスがほぼ同時に起動している。

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

ステータスA

2. プリエンプト時間（このドキュメントでは30秒）が経過しました。

After 30 seconds (preempt time)	Active	Standby	Standby	Active

ステータスB

3. プライマリユニットのグループ1で障害（インターフェイスダウンなど）が発生しました。

Failover event	Standby	Standby	Active	Active

ステータスC

4. プライマリデバイスのグループ1が障害から回復してから経過したプリエンプト時間（このドキュメントでは30秒）です。

After 30 seconds since Primary Unit recovered	Active	Standby	Standby	Active

ステータスD

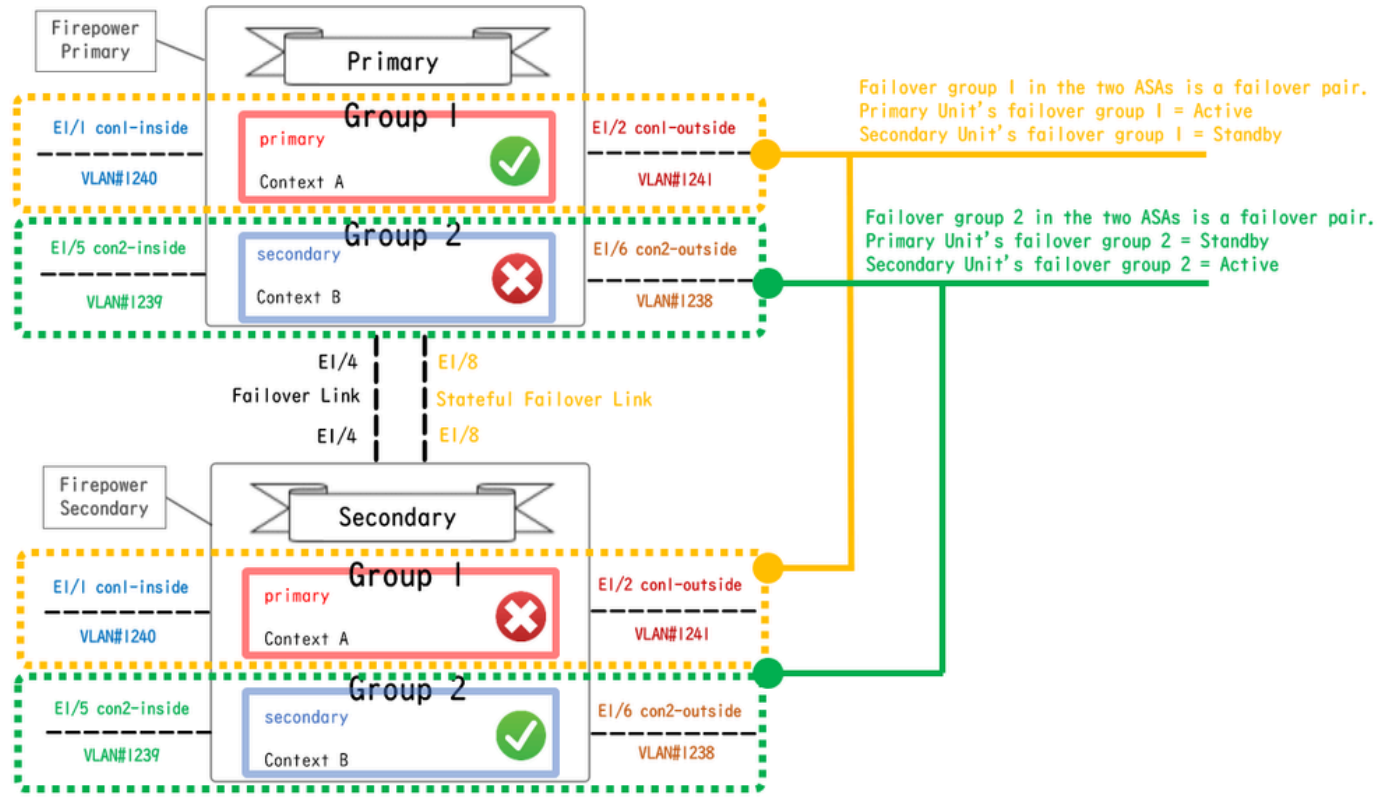
5. プライマリユニットのグループ2を手動でアクティブに設定します。

Manual failover	Active	Active	Standby	Standby

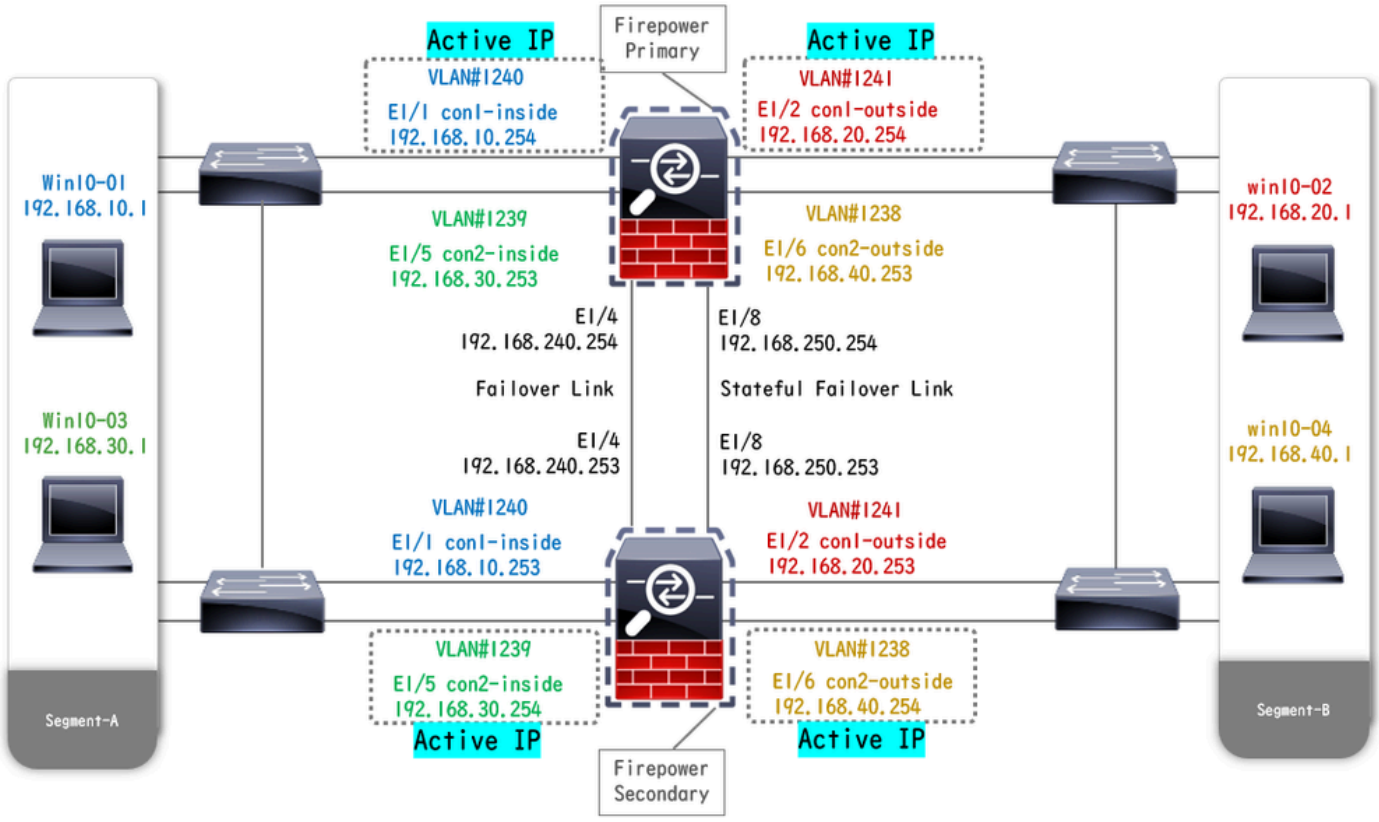
ステータスE

ネットワーク図

このドキュメントでは、次の図に基づくアクティブ/アクティブフェールオーバーの設定と検証について説明します。



論理構成図

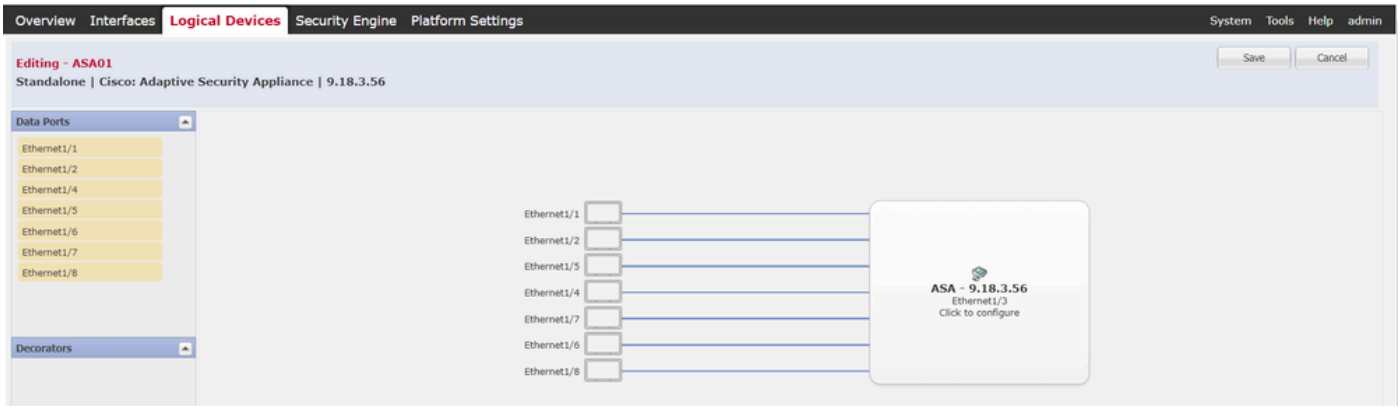


物理構成図

コンフィギュレーション

ステップ 1：インターフェイスの事前設定

両方のFirepowerに対して、FCM GUIでログインします。Logical Devices > Editの順に移動します。図に示すように、データインターフェイスをASAに追加します。



インターフェイスの事前設定

ステップ 2：プライマリユニットの設定

SSHまたはコンソールを介してプライマリFXOS CLIに接続します。 **connect module 1 console** および connect asaコマンドを実行して、ASA CLIに入ります。

a.プライマリユニットでフェールオーバーを設定します（プライマリユニットのシステムコンテキストでコマンドを実行）。

```
<#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 fail
```

b.コンテキストに応じてフェールオーバーグループを設定します（プライマリユニットのシステムコンテキストでコマンドを実行）。

```
<#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. changeto context con1を実行して、システムコンテキストからcon1コンテキストに接続します。con1コンテキストのインターフェイスのIPを設定します（プライマリユニットのcon1コンテキストでコマンドを実行）。

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. changeto context con2を実行して、システムコンテキストからcon2コンテキストに接続します。con2コンテキストのインターフェイスのIPを設定します（プライマリユニットのcon2コンテキストでコマンドを実行）。

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

ステップ 3：セカンダリユニットの設定

a. SSHまたはコンソールを使用して、セカンダリFXOS CLIに接続します。セカンダリユニットでフェールオーバーを設定します（セカンダリユニットのシステムコンテキストでコマンドを実行）。

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. failoverコマンドを実行します（セカンダリユニットのシステムコンテキストで実行）。

failover

ステップ 4：同期が正常に終了した後のフェールオーバーステータスの確認

a.セカンダリユニットのシステムコンテキストでshow failover実行します。

<#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:

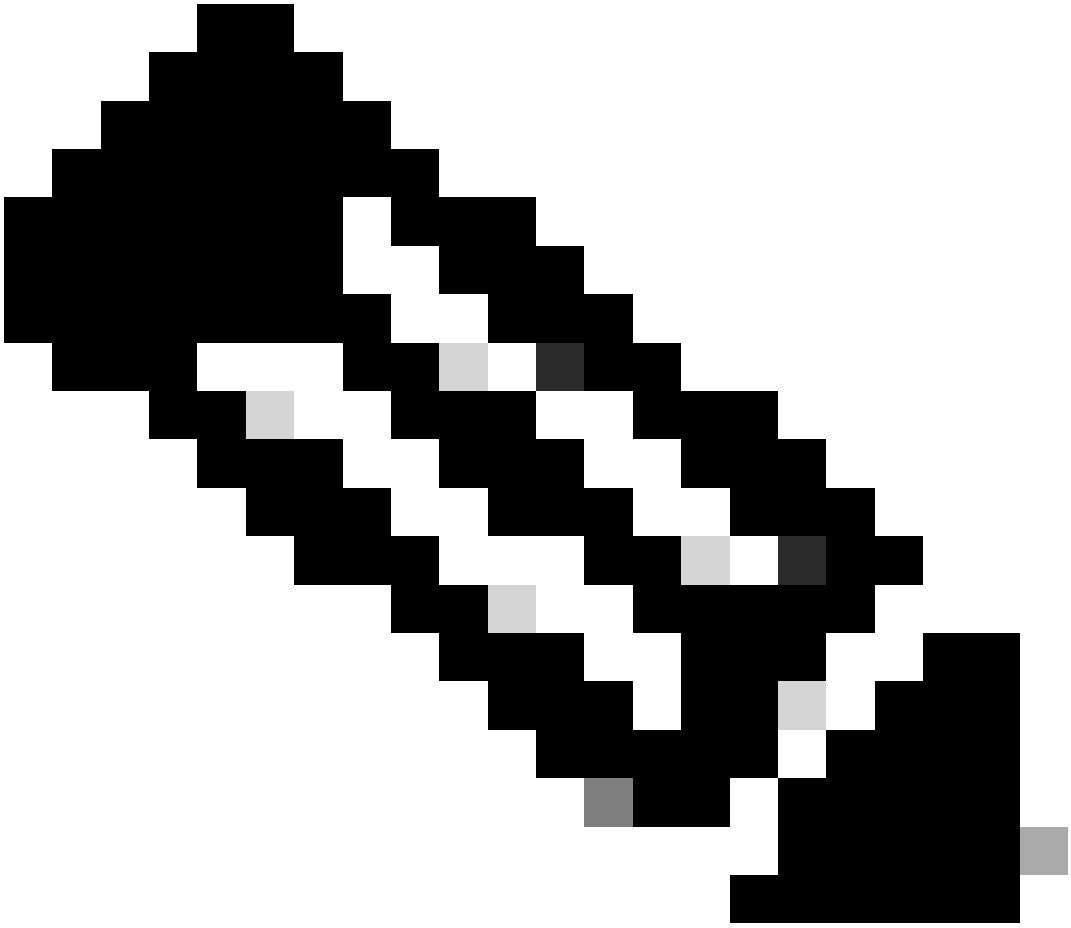
Active

Active time: 93 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface c

b.（オプション）**no failover active group 2** コマンドを実行して、プライマリユニットのグループ2を手動でスタンバイステータスに切り替えます（プライマリユニットのシステムコンテキストで実行）。これにより、ファイアウォールを通過するトラフィックの負荷を分散できます。

<#root>

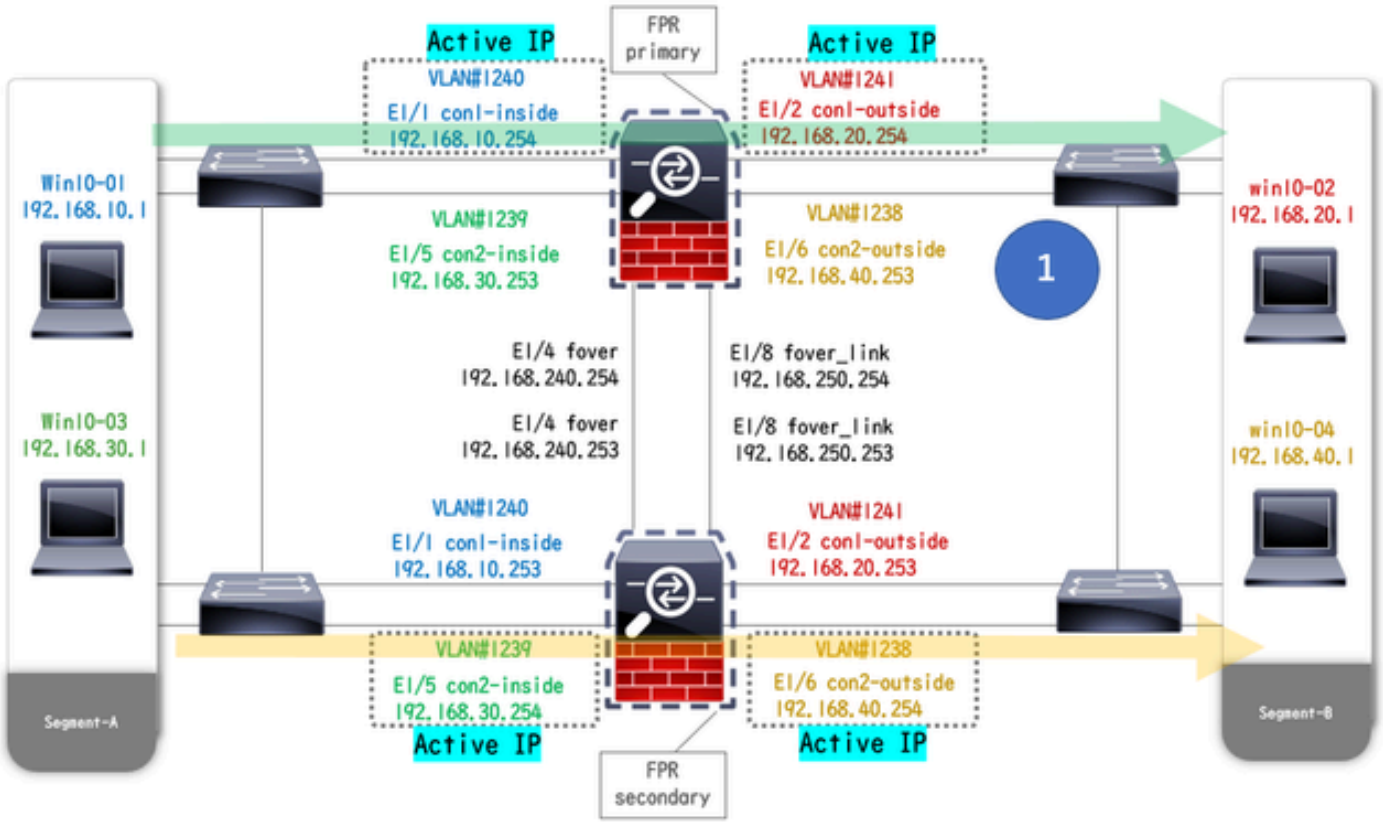
no failover active group 2



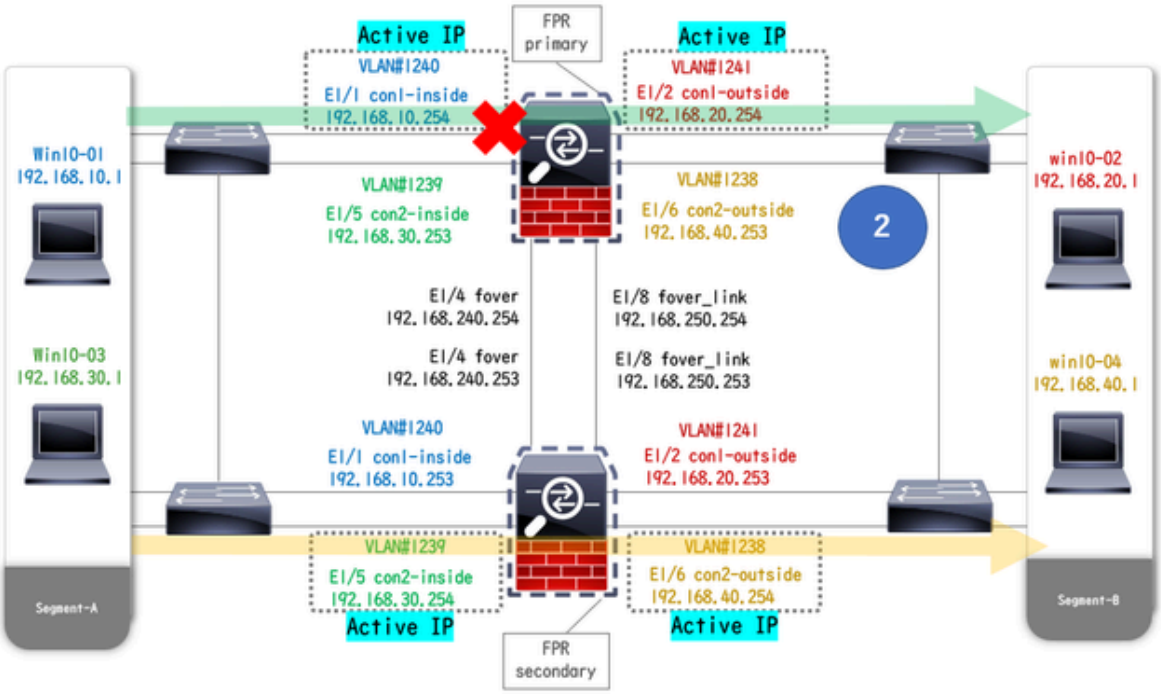
注：このコマンドを実行すると、フェールオーバーのステータスがトラフィックフロー条件1に一致します。

確認

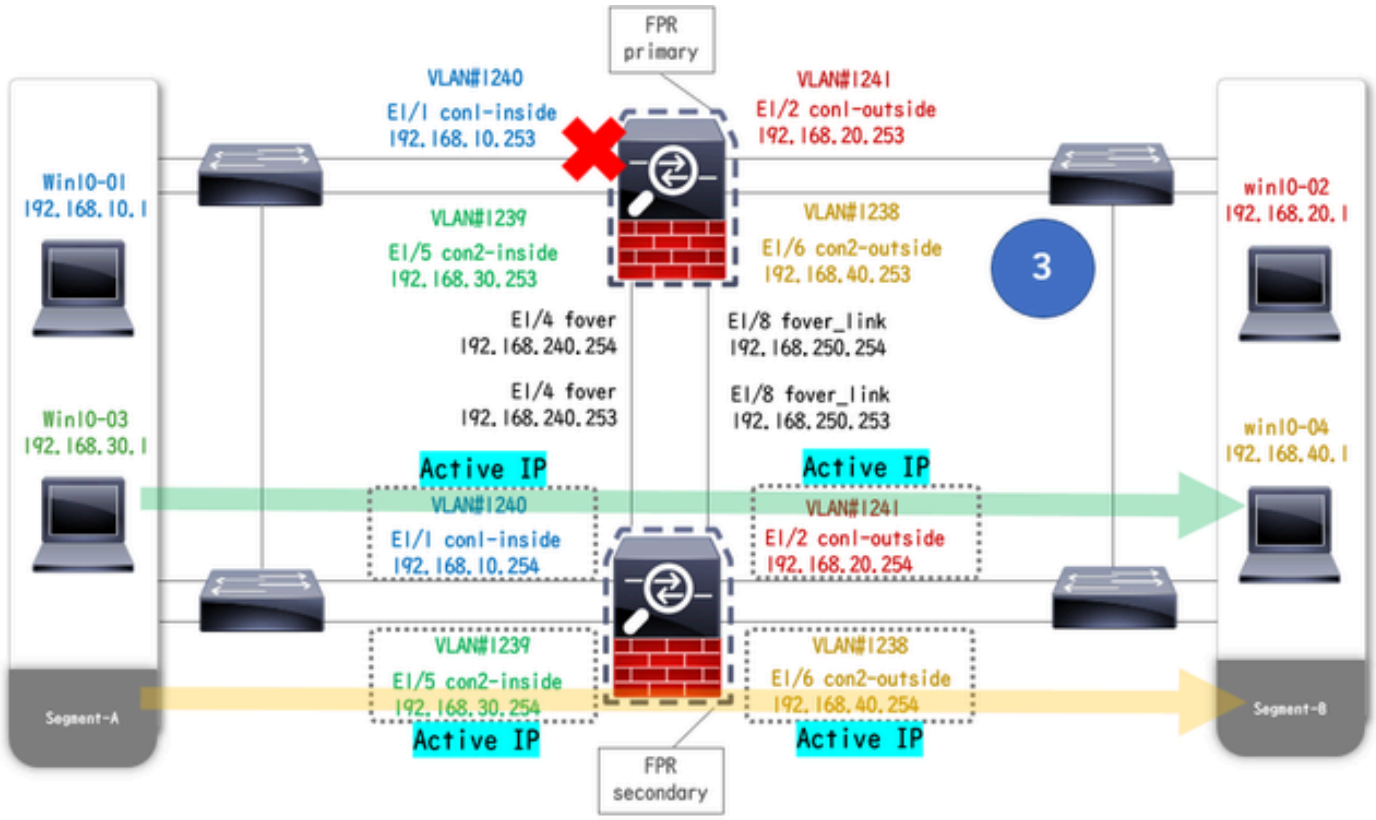
E1/1がダウンすると、グループ1のフェールオーバーがトリガーされ、スタンバイ側（セカンダリユニット）のデータインターフェイスが元のアクティブインターフェイスのIPアドレスとMACアドレスを引き継ぎ、トラフィック（このドキュメントではFTP接続）がASAによって継続的に渡されるようになります。



リンク



ダウン前リンクダウン中



トリガーされたフェールオーバー

ステップ 1：Win10-01からWin10-02へのFTP接続の開始

ステップ 2：フェールオーバー前のFTP接続の確認

システムコンテキストからcon1コンテキストに接続するために changeto context con1を実行します。両方のASAユニットでFTP接続が確立されていることを確認します。

<#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
```

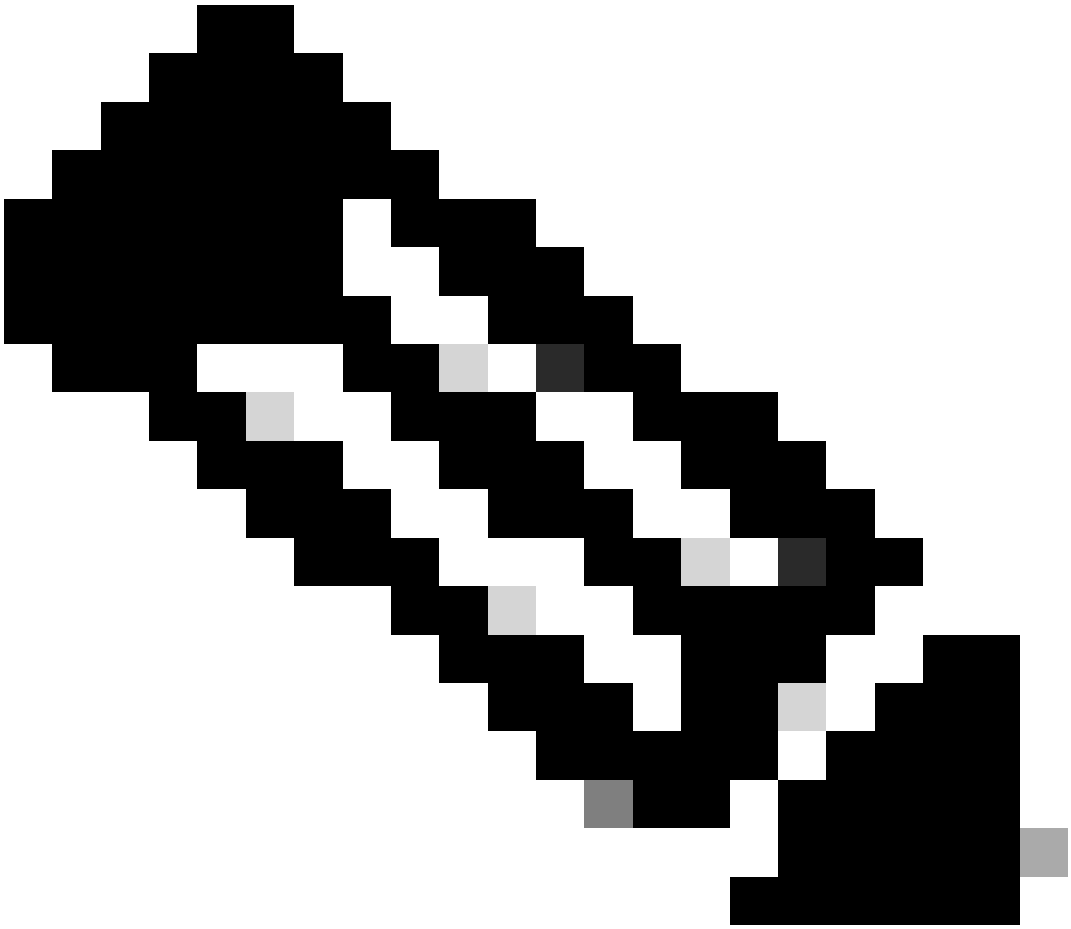
con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

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

ステップ 3：プライマリユニットのLinkDOWN E1/1

ステップ 4：フェールオーバーステータスの確認

システムコンテキストでは、フェールオーバーがグループ1で発生していることを確認します。



注：フェールオーバーのステータスは、トラフィックフロー条件4に一致します。

<#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

ステップ 5 : フェールオーバー後のFTP接続の確認

changeto context con1を実行して、システムコンテキストからcon1コンテキストに接続し、FTP接続が中断されていないことを確認します。

<#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

手順 6 : プリエンプト時間動作の確認

プライマリユニットのLinkUP E1/1を受信し、30秒間待機すると（プリエンプト時間）、フェールオーバー状態が元の状態に戻ります（パターン1のトラフィックフローに一致）。

<#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

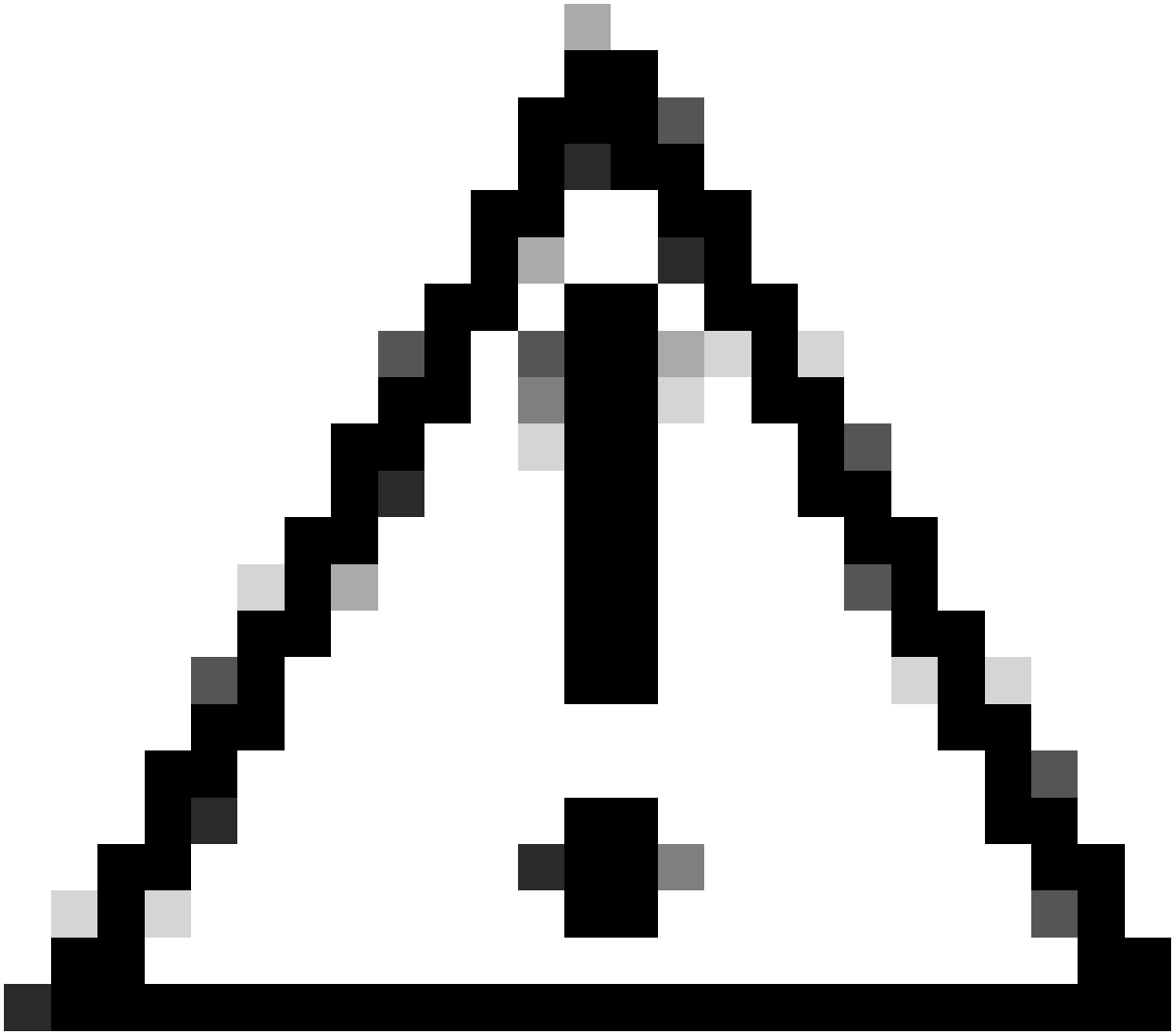
Active time: 10816 (sec) con1 Interface con1-inside (192.168.10.253): Normal (Monitored) con1 Interfac

仮想MACアドレス

アクティブ/アクティブフェールオーバーでは、仮想MACアドレス (手動で設定された値、自動生成された値、またはデフォルト値) が常に使用されます。アクティブな仮想MACアドレスは、アクティブインターフェイスに関連付けられます。

仮想MACアドレスの手動設定

物理インターフェイスの仮想MACアドレスを手動で設定するには、 mac addressコマンドまたは mac-addressコマンド (I/F設定モード内) を使用できます。これは、物理インターフェイスE1/1の仮想MACアドレスを手動で設定する例です。



注意：同じデバイス内では、これら2種類のコマンドの使用は避けてください。

<#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

または

<#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

仮想MACアドレスの自動設定

仮想MACアドレスの自動生成もサポートしています。これは、 mac-address auto <prefix prefix>コマンドを使用して実行できます。
仮想MACアドレスの形式は、自動生成されるA2 xx.yyzz.zzzzです。
A2：固定値
xx.yy：コマンドオプションで指定された<prefix prefix>によって生成されます (プレフィクスは16進数に変換されてから、逆順で挿入されます) 。
zz.zzzz ：内部カウンタにより生成

次に、インターフェイスに対する **mac-address auto** コマンドによる仮想MACアドレスの生成例を示します。

<#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
```

仮想MACアドレスのデフォルト設定

仮想MACアドレスの自動生成も手動生成も設定されていない場合は、デフォルトの仮想MACアドレスが使用されます。

デフォルト仮想MACアドレスの詳細については、『Cisco Secure Firewall ASAシリーズコマンドリファレンスガイド』の「MACア

ドレスのコマンドデフォルト」を参照してください。

アップグレード

CLIまたはASDMを使用して、アクティブ/アクティブフェールオーバーペアのアップグレードをダウンタイムなしで実行できます。詳細は、『アクティブ/アクティブフェールオーバーペアのアップグレード』を参照してください。

関連情報

- CLIを使用したアクティブ/アクティブフェールオーバーペアのアップグレード
- MAC アドレス
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。