firepower 4100 Series에서 ASA 액티브/액티브 장애 조치 구성

목차

소개

이 문서에서는 Cisco Firepower 4145 NGFW Appliance에서 액티브/액티브 장애 조치를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco ASA(Adaptive Security Appliance)의 액티브/스탠바이 장애 조치.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Firepower 4145 NGFW Appliance (ASA) 9.18(3)56
- Firepower eXtensible 운영 체제(FXOS) 2.12(0.498)
- Windows 10

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

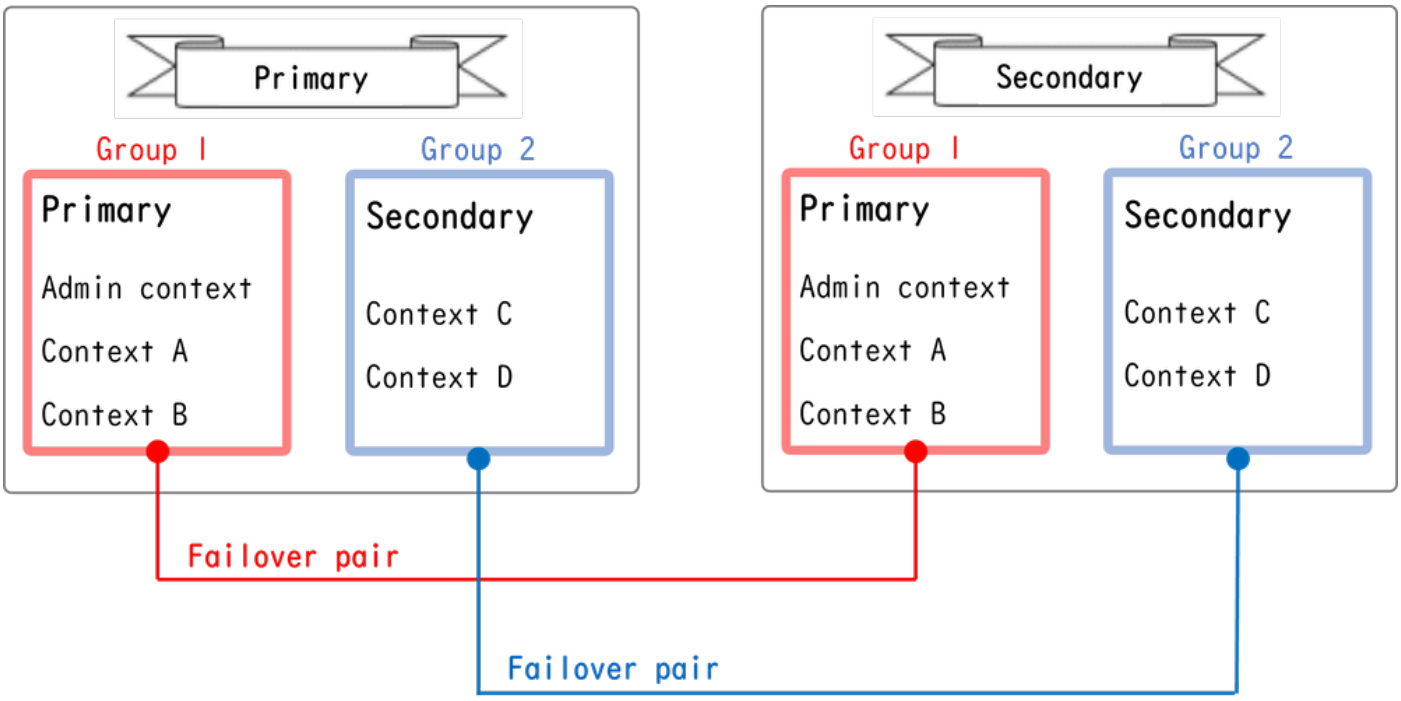
액티브/액티브 장애 조치는 다중 컨텍스트 모드에서 실행 중인 보안 어플라이언스에서만 사용할 수 있습니다. 이 모드에서는 ASA가 컨텍스트라고 하는 여러 가상 디바이스로 논리적으로 분할됩니다. 각 컨텍스트는 고유한 보안 정책, 인터페이스 및 관리자가 있는 독립적인 디바이스로 작동합니다.

액티브/액티브 장애 조치는 ASA(Adaptive Security Appliance)의 기능으로서 두 Firepower 디바이스가 동시에 트래픽을 전달할 수 있게 합니다. 이 컨피그레이션은 일반적으로 처리량을 최대화하기 위해 두 디바이스 간에 트래픽을 분할하려는 로드 밸런싱 시나리오에 사용됩니다. 이중화 목적으로도 사용되므로 한 ASA에서 장애가 발생하면 다른 ASA가 서비스 중단 없이 인계받을 수 있습니다.

ASA 액티브/액티브 장애 조치의 메커니즘

액티브/액티브 장애 조치의 각 컨텍스트는 그룹 1 또는 그룹 2에 수동으로 할당됩니다. 관리 컨텍스트는 기본적으로 그룹 1에 할당됩니다. 두 섀시(유닛)의 동일한 그룹(group1 또는 group2)이 장애 조치 쌍을 구성하며, 이는 이중화 기능을 실현합니다. 각 장애 조치 쌍의 동작은 기본적으로 액티브/스탠바이 장애 조치의 동작과 동일합니다. 액티브/스탠바이 장애 조치에 대한 자세한 내용은 액티브/스탠바이 장애 조치 구성을 참조하십시오. 액티브/액티브 장애 조치에서는 각 섀시의 역할(기본 또는 보조) 외에 각 그룹에도 역할(기본 또는 보조)이 있습니다. 이러한 역할은 사용자가 수동으로 미리 설정하며 각 장애 조치 그룹에 대한 HA(고가용성) 상태(액티브 또는 스탠바이)를 결정하는 데 사용됩니다.

관리 컨텍스트는 기본 섀시 관리(예: SSH) 연결을 처리하는 특수 컨텍스트입니다. 액티브/액티브 장애 조치 이미지입니다.



액티브/액티브 장애 조치의 장애 조치 쌍

트래픽 흐름

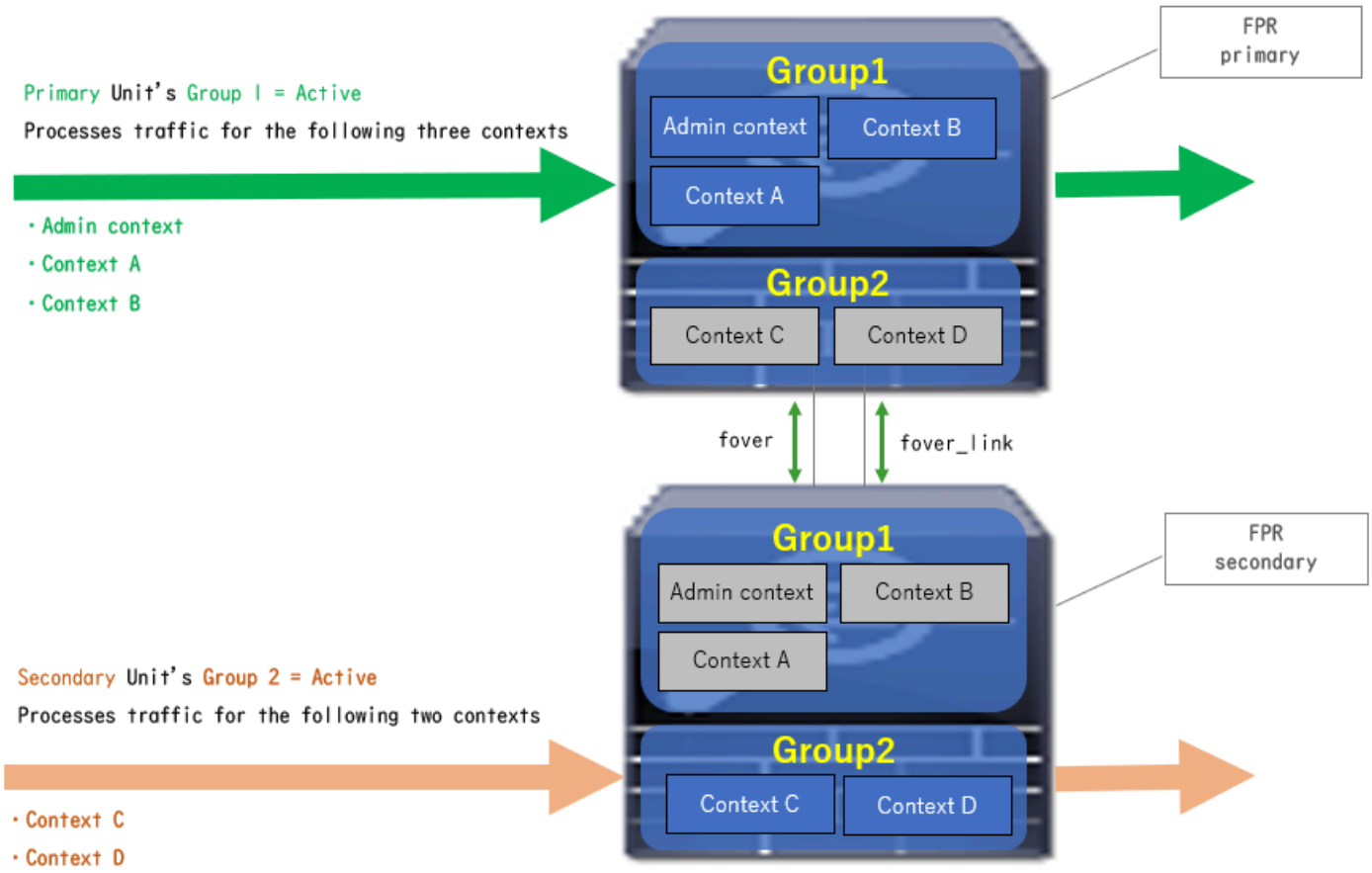
액티브/액티브 장애 조치에서는 다음 이미지와 같이 여러 패턴으로 트래픽을 처리할 수 있습니다.

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	

트래픽 흐름

트래픽 흐름 조건 1

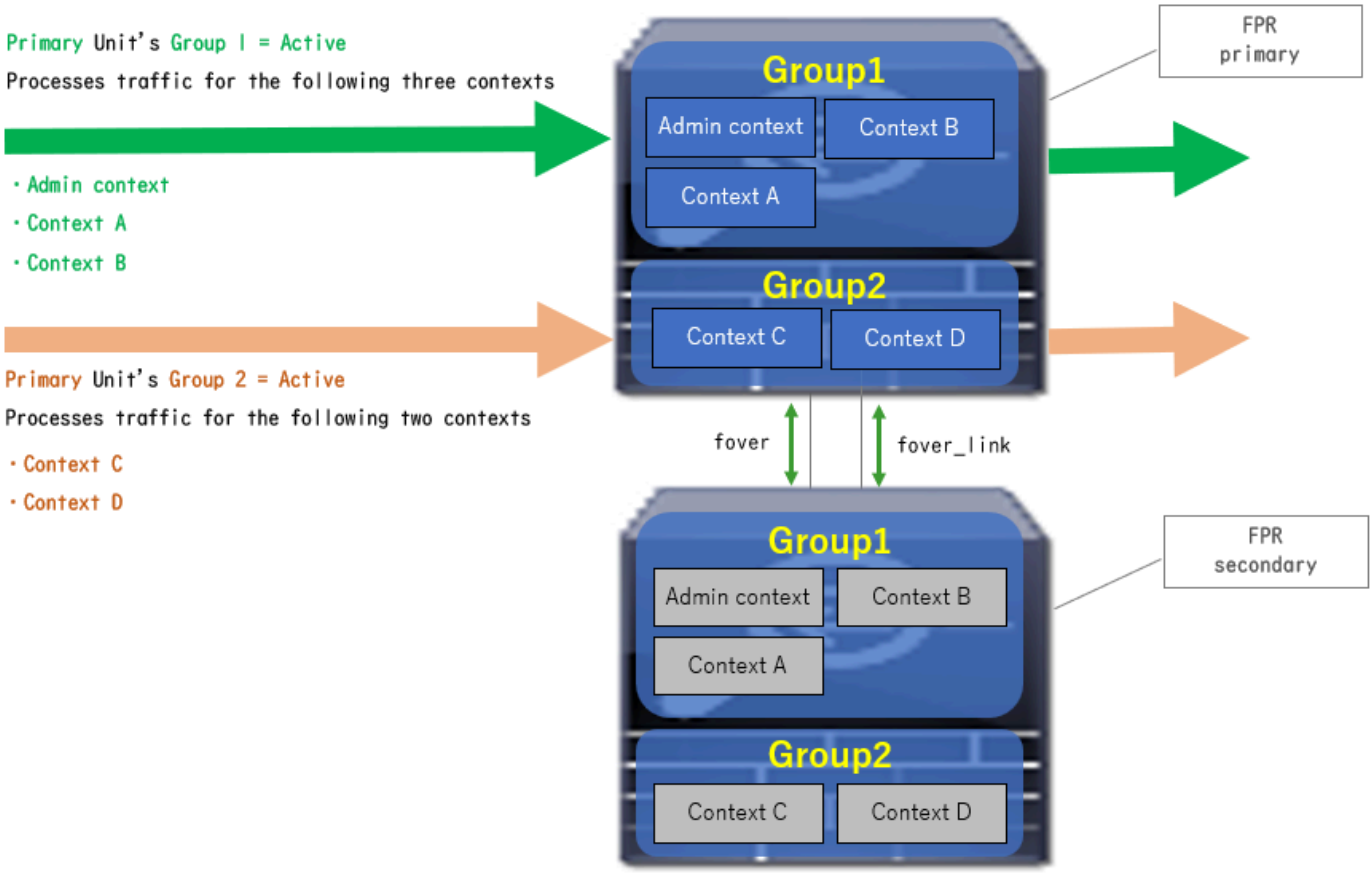
- 기본 단위: 그룹 1 = 활성, 그룹 2 = 대기
- 보조 유닛: 그룹 1 = 대기, 그룹 2 = 활성



트래픽 흐름 조건 1

트래픽 흐름 조건 2

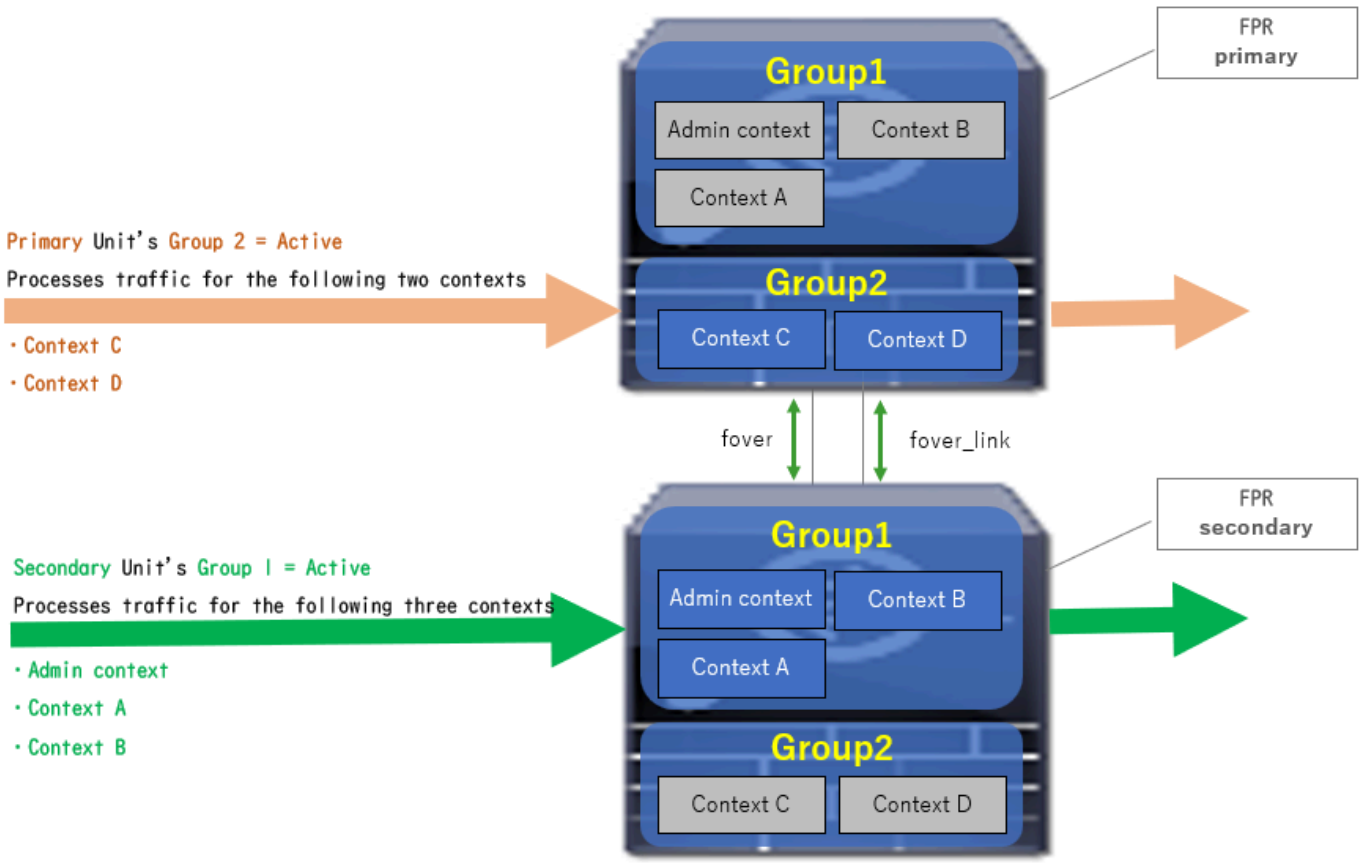
- 기본 단위: 그룹 1 = 활성, 그룹 2 = 활성
- 보조 유닛: 그룹 1 = 대기, 그룹 2 = 대기



트래픽 흐름 조건 2

트래픽 흐름 조건 3

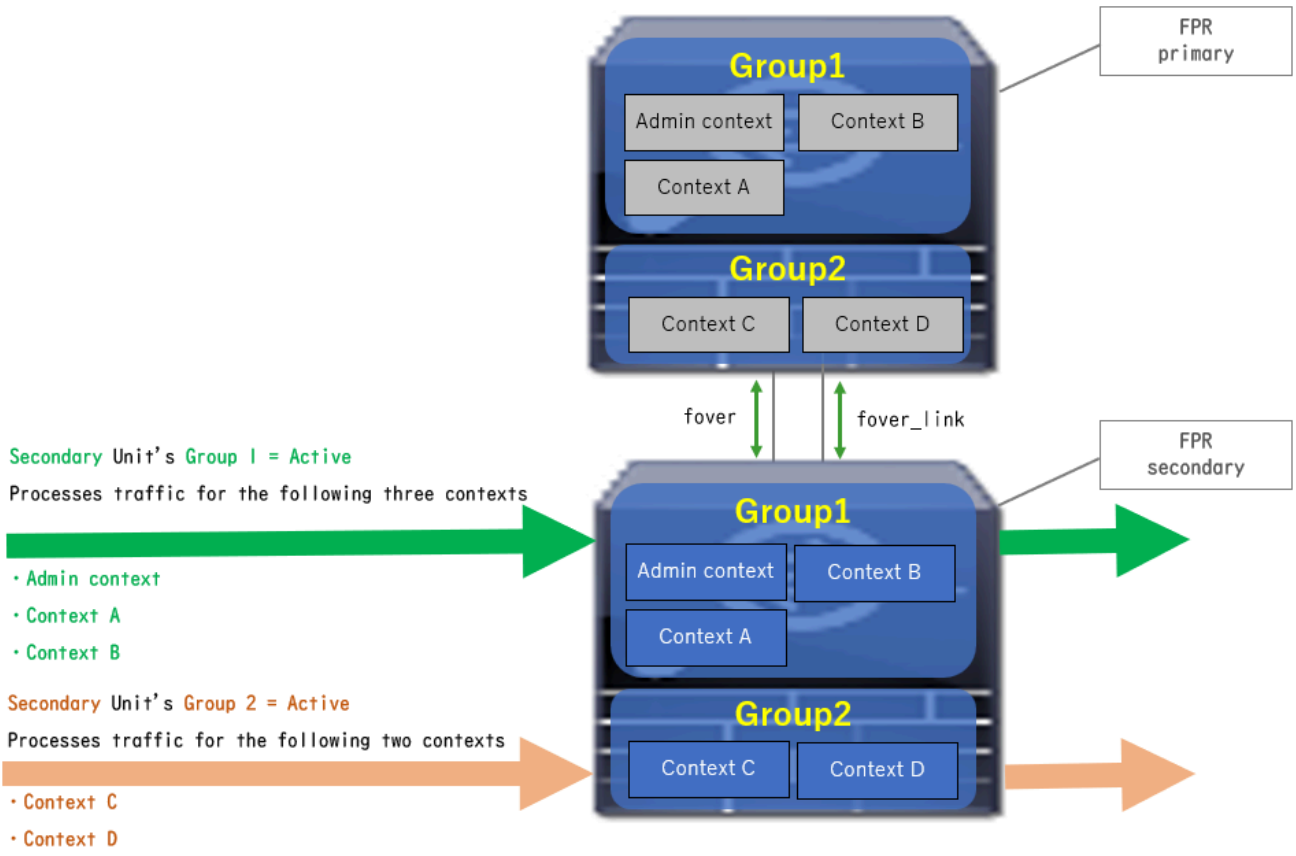
- 기본 유닛: 그룹 1 = 대기, 그룹 2 = 활성
- 보조 유닛: 그룹 1 = 액티브, 그룹 2 = 스탠바이



트래픽 흐름 조건 3

트래픽 흐름 조건 4

- 기본 유닛: 그룹 1 = 대기, 그룹 2 = 대기
- 보조 단위: 그룹 1 = 활성, 그룹 2 = 활성



트래픽 흐름 조건 4

액티브/스탠바이 선택 규칙

액티브/액티브 장애 조치에서 각 그룹의 상태(액티브/스탠바이)는 다음 규칙에 의해 결정됩니다.

- 두 개의 디바이스가 거의 동시에 부팅된다고 가정하면, 먼저 유닛 중 하나(기본 또는 보조)가 활성화됩니다.
- 선점 시간이 경과하면 섀시와 그룹에서 동일한 역할을 하는 그룹이 활성화됩니다.
- 장애 조치 이벤트(예: 인터페이스 DOWN)가 있는 경우, 그룹의 상태는 액티브/스탠바이 장애 조치와 동일한 방식으로 변경됩니다.
- 수동 장애 조치를 수행한 후에는 선점 시간이 작동하지 않습니다.

다음은 상태 변경의 예입니다.

- 두 장치 모두 거의 동시에 부팅되고 있습니다. 상태 A →
- 선점 시간이 지났습니다. 상태 B →
- 기본 디바이스 오류(장애 조치가 트리거됨). 상태 C →
- 기본 디바이스가 실패에서 복구된 이후 선점 시간이 경과했습니다. 상태 D →
- 장애 조치를 수동으로 트리거합니다. 상태 E

장애 조치 트리거 및 상태 모니터링에 대한 자세한 내용은 장애 조치 이벤트를 참조하십시오.

1. 두 장치가 거의 동시에 부팅되고 있습니다.

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

상태 A

2. 선점 시간(이 문서의 30초)이 경과되었습니다.

After 30 seconds (preempt time)	Active	Standby	Standby	Active

상태 B

3. 기본 유닛의 그룹 1에서 장애(인터페이스 다운 등)가 발생했습니다.

Failover event	Standby	Standby	Active	Active

상태 C

4. 운영 디바이스 그룹 1의 장애가 복구된 이후의 선점 시간(이 문서의 30초)입니다.

After 30 seconds since Primary Unit recovered	Active	Standby	Standby	Active

상태 D

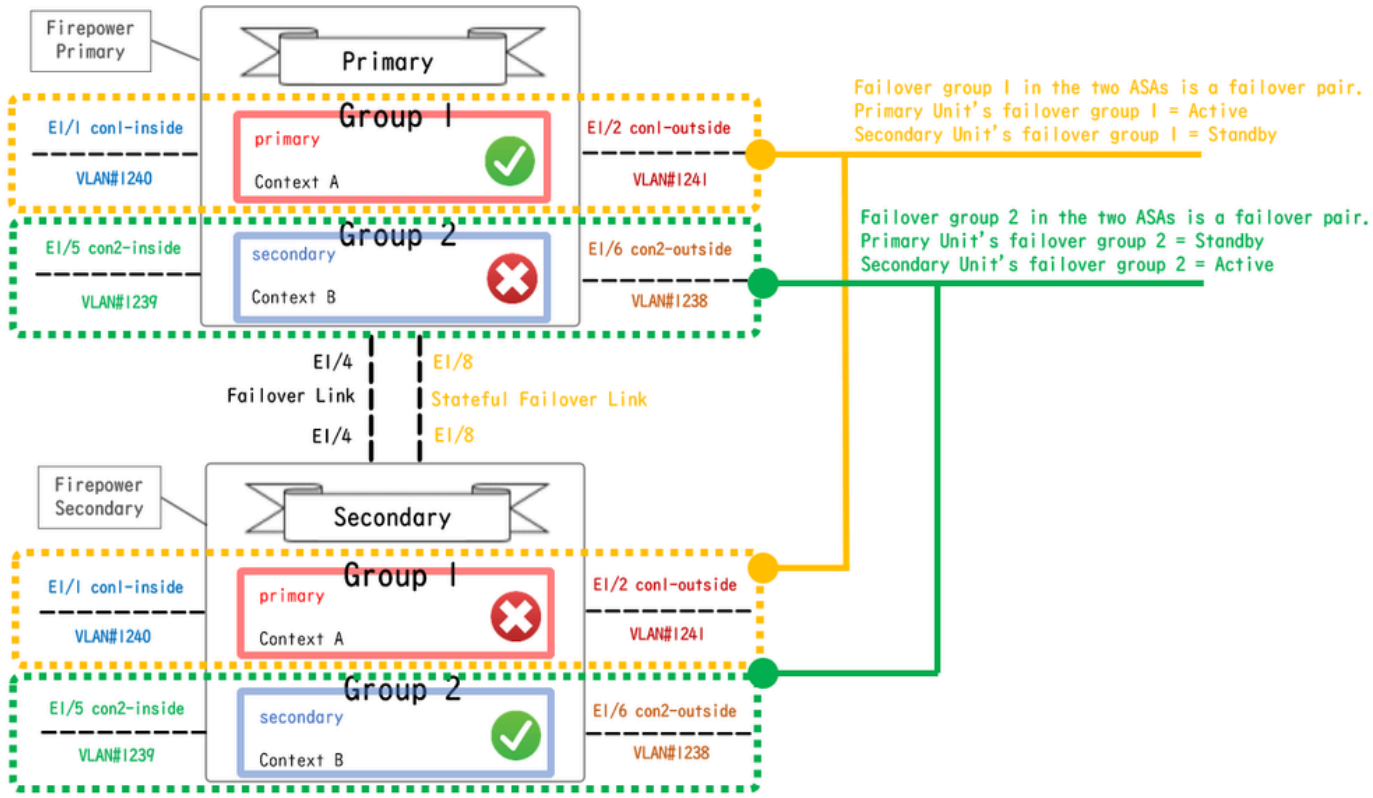
5. 수동으로 기본 유닛의 그룹 2를 활성으로 설정합니다.

Manual failover	Active	Active	Standby	Standby

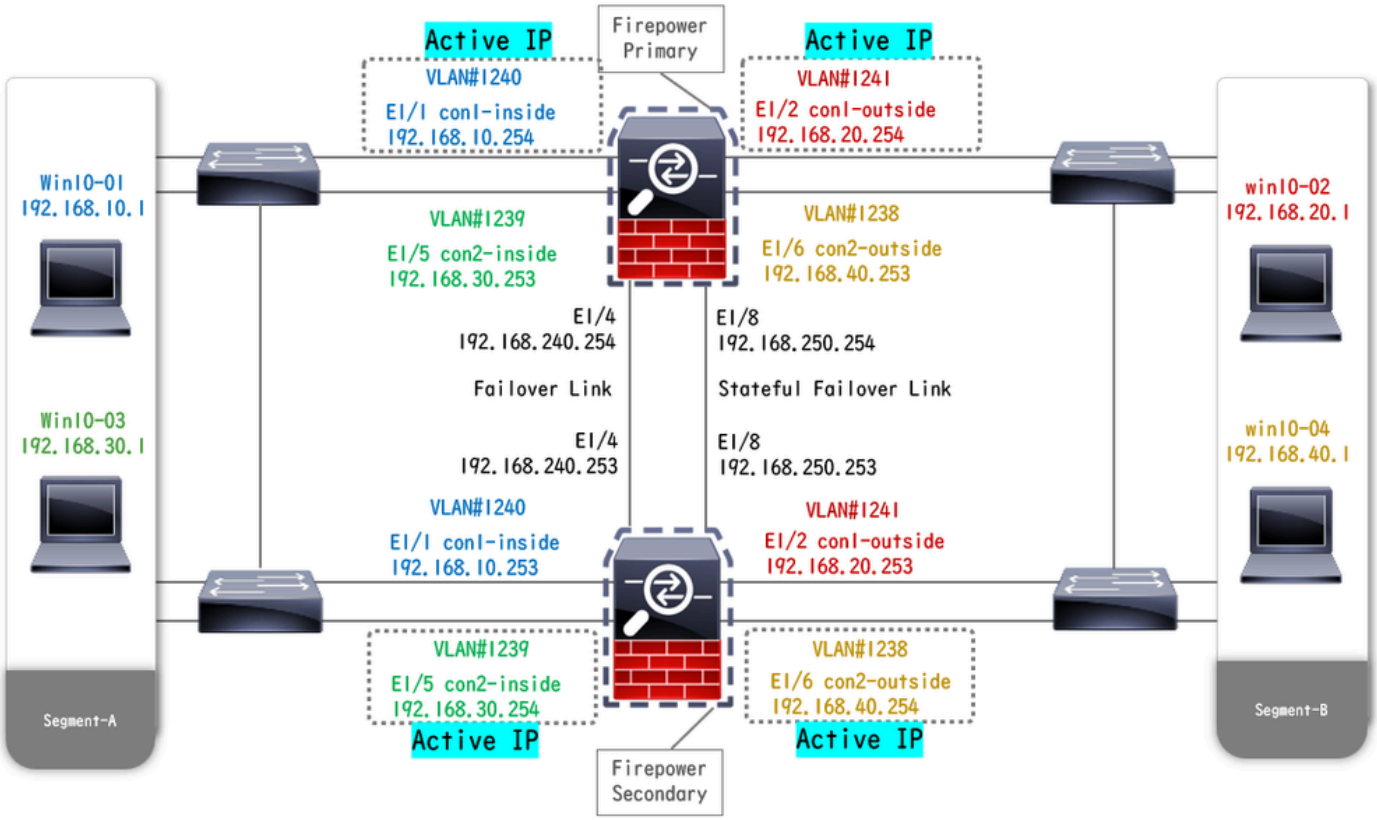
상태 E

네트워크 다이어그램

이 문서에서는 이 다이어그램을 기반으로 액티브/액티브 장애 조치를 구성하고 확인하는 방법을 소개합니다.



논리적 컨피그레이션 다이어그램

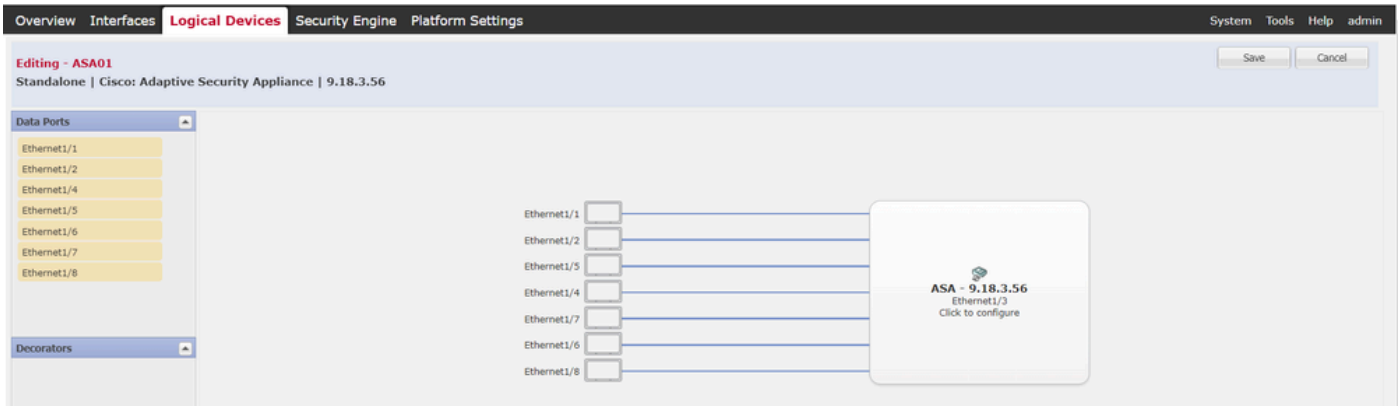


물리적 컨피그레이션 다이어그램

설정

1단계. 인터페이스 사전 구성

두 Firepower 모두에 대해 FCM GUI에 로그인합니다. Logical Devices(논리적 디바이스) > Edit(수정)로 이동합니다. 이미지에 표시된 대로 ASA에 데이터 인터페이스를 추가합니다.



인터페이스 사전 구성

2단계. 기본 유닛의 컨피그레이션

SSH 또는 콘솔을 통해 기본 FXOS CLI에 연결합니다. 실행 **connect module 1 console** 및 connect asa 명령을 사용하여 ASA CLI에 입력합니다.

a. 기본 유닛에서 장애 조치를 구성합니다(기본 유닛의 시스템 컨텍스트에서 명령 실행).

```
<#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. 컨텍스트에 대한 장애 조치 그룹을 구성합니다(기본 유닛의 시스템 컨텍스트에서 명령 실행).

```
<#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 con1시스템 컨텍스트에서 con1 컨텍스트를 연결하려면 를 실행합니다. con1 컨텍스트의 인터페이스에 대해 IP를 구성합니다(기본 유닛의 con1 컨텍스트에서 명령 실행).

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 con2시스템 컨텍스트에서 con2 컨텍스트를 연결하려면 를 실행합니다. con2 컨텍스트의 인터페이스에 대해 IP를 구성합니다(기본 유닛의 con2 컨텍스트에서 명령 실행).

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

3단계. 보조 유닛의 컨피그레이션

a. SSH 또는 콘솔을 통해 보조 FXOS CLI에 연결합니다. 보조 유닛에서 장애 조치를 구성합니다(보조 유닛의 시스템 컨텍스트에서 명령 실행).

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. failover명령 실행(보조 유닛의 시스템 컨텍스트에서 실행)

failover

4단계. 동기화가 완료된 후 장애 조치 상태 확인

a. 보조 show failover 유닛의 시스템 컨텍스트에서 실행합니다.

<#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:

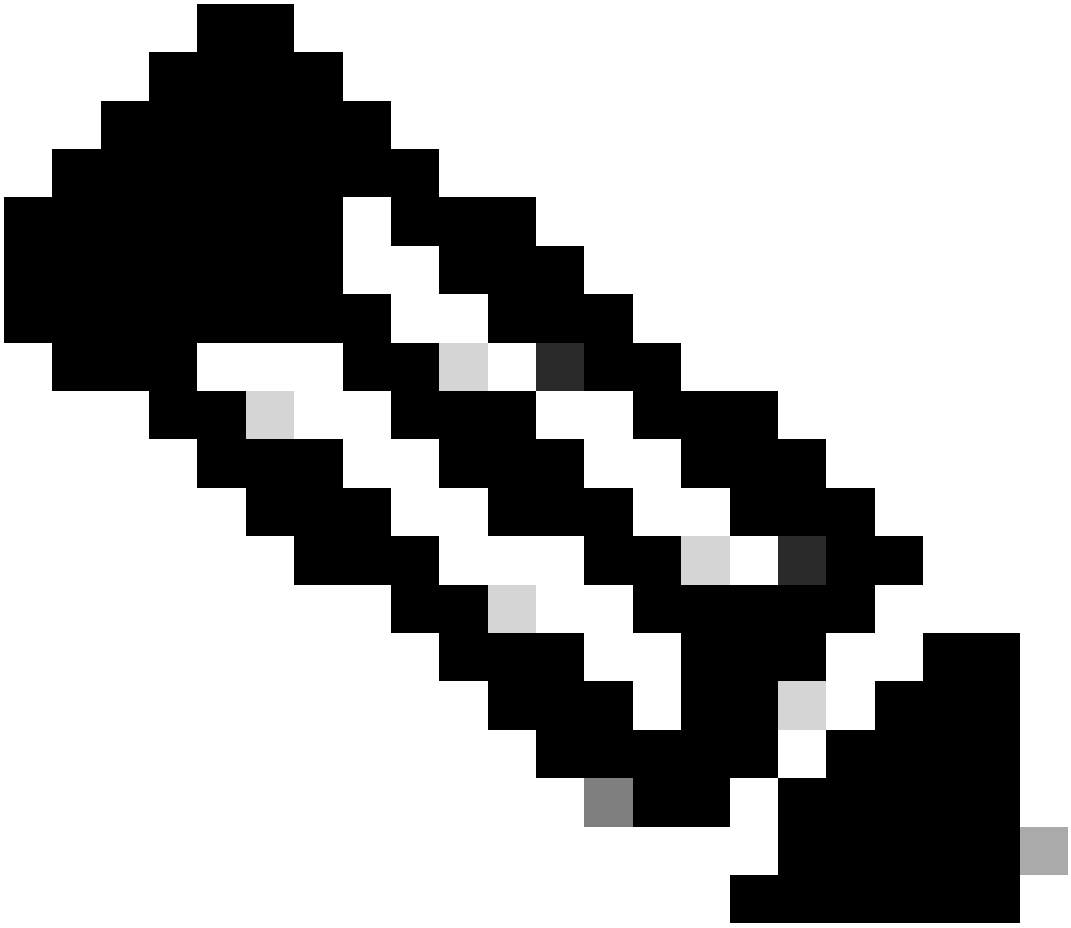
Active

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

b. (선택 사항) **no failover active group 2** 명령을 실행하여 기본 유닛의 그룹 2를 대기 상태로 수동으로 전환합니다(기본 유닛의 시스템 컨텍스트에서 실행). 이렇게 하면 방화벽을 통과하는 트래픽 로드의 균형을 맞출 수 있습니다.

<#root>

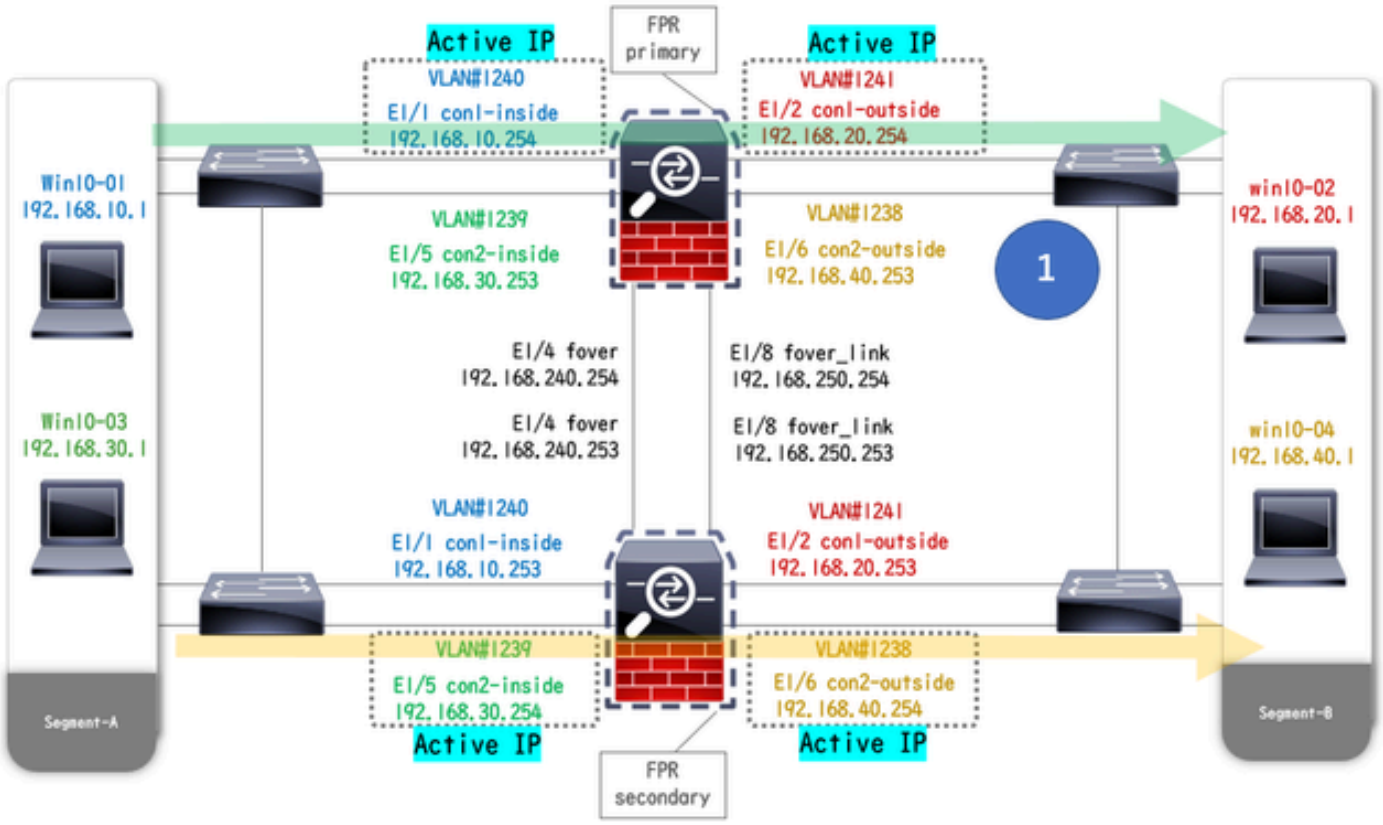
no failover active group 2



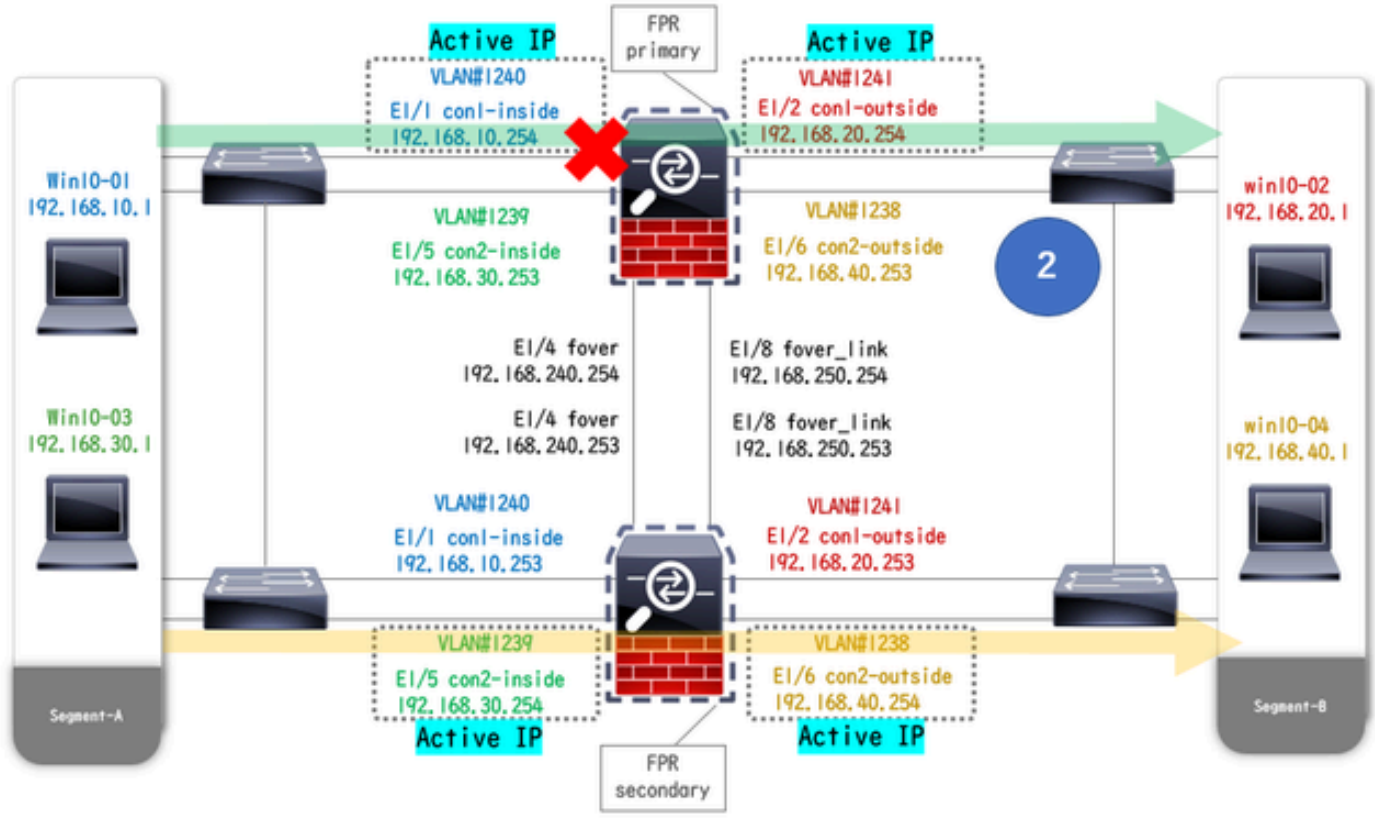
참고: 이 명령을 실행하면 장애 조치 상태가 트래픽 흐름 조건 1과 일치합니다.

다음을 확인합니다.

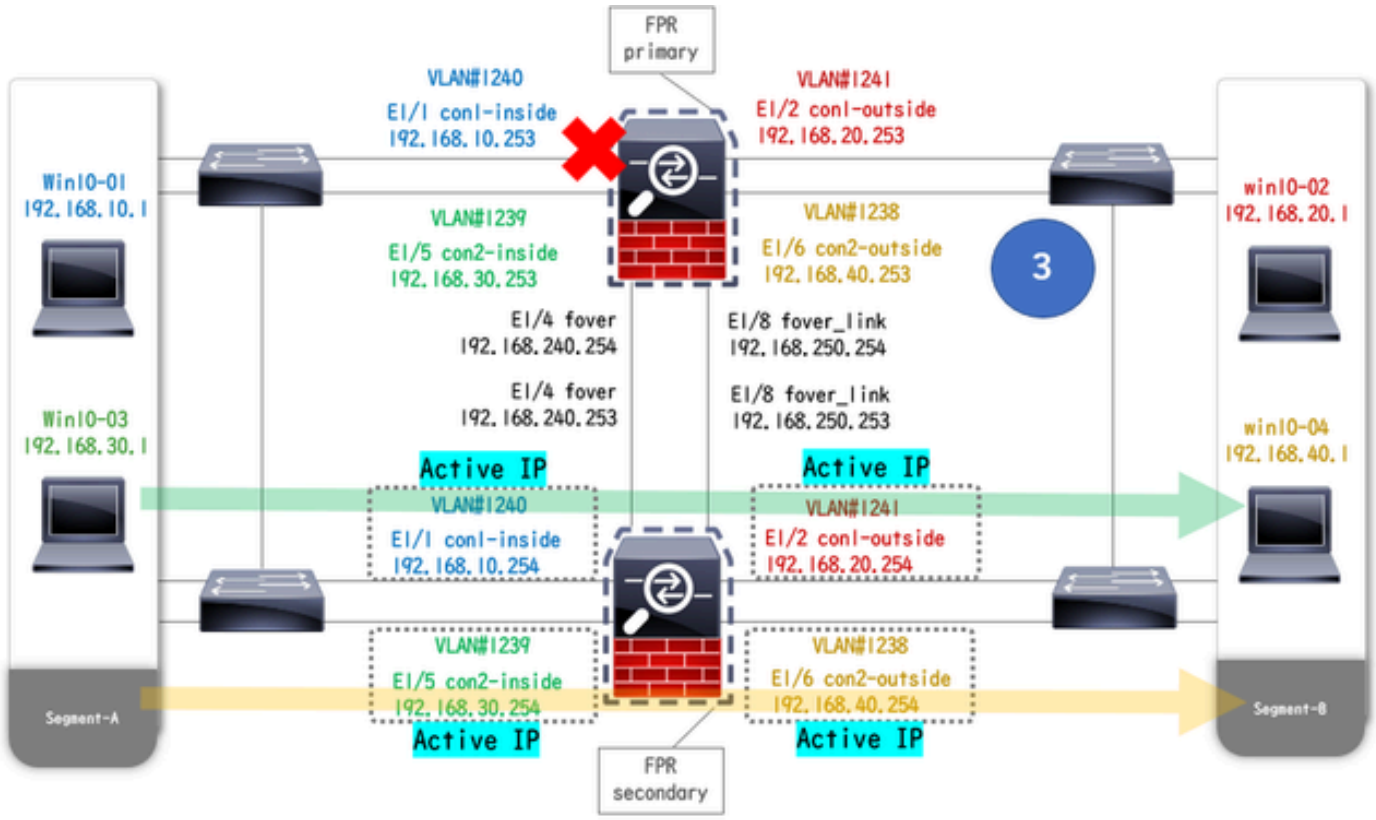
E1/1이 DOWN되면 그룹 1의 장애 조치가 트리거되고 스탠바이 측(보조 유닛)의 데이터 인터페이스가 원래 액티브 인터페이스의 IP 및 MAC 주소를 인수하여 트래픽(이 문서의 FTP 연결)이 ASA에서 지속적으로 전달되도록 합니다.


Active IP
FPR primary
Active IP
VLAN#1240
Et1/1 con1-inside
192.168.10.254
VLAN#1241
Et1/2 con1-outside
192.168.20.254
Win10-01
192.168.10.1
win10-02
192.168.20.1
VLAN#1239
Et1/5 con2-inside
192.168.30.253
VLAN#1238
Et1/6 con2-outside
192.168.40.253
1
Et1/4 fover
192.168.240.254
Et1/8 fover_link
192.168.250.254
Et1/4 fover
192.168.240.253
Et1/8 fover_link
192.168.250.253
Win10-03
192.168.30.1
win10-04
192.168.40.1
VLAN#1240
Et1/1 con1-inside
192.168.10.253
VLAN#1241
Et1/2 con1-outside
192.168.20.253
VLAN#1239
Et1/5 con2-inside
192.168.30.254
VLAN#1238
Et1/6 con2-outside
192.168.40.254
Segment-A
Segment-B
Active IP
FPR secondary
Active IP

링크


Active IP
FPR primary
Active IP
VLAN#1240
Et1/1 con1-inside
192.168.10.254
VLAN#1241
Et1/2 con1-outside
192.168.20.254
Win10-01
192.168.10.1
win10-02
192.168.20.1
VLAN#1239
Et1/5 con2-inside
192.168.30.253
VLAN#1238
Et1/6 con2-outside
192.168.40.253
2
Et1/4 fover
192.168.240.254
Et1/8 fover_link
192.168.250.254
Et1/4 fover
192.168.240.253
Et1/8 fover_link
192.168.250.253
Win10-03
192.168.30.1
win10-04
192.168.40.1
VLAN#1240
Et1/1 con1-inside
192.168.10.253
VLAN#1241
Et1/2 con1-outside
192.168.20.253
VLAN#1239
Et1/5 con2-inside
192.168.30.254
VLAN#1238
Et1/6 con2-outside
192.168.40.254
Segment-A
Segment-B
Active IP
FPR secondary
Active IP

중단 전링크 중단 중



장애 조치 트리거됨

1단계. Win10-01에서 Win10-02로의 FTP 연결 시작

2단계. 장애 조치 전에 FTP 연결 확인

시스템 컨텍스트에서 con1 컨텍스트를 연결하려면 를 실행합니다 changeto context con1. 두 ASA 유닛 모두에서 FTP 연결이 설정되었는지 확인합니다.

<#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
```

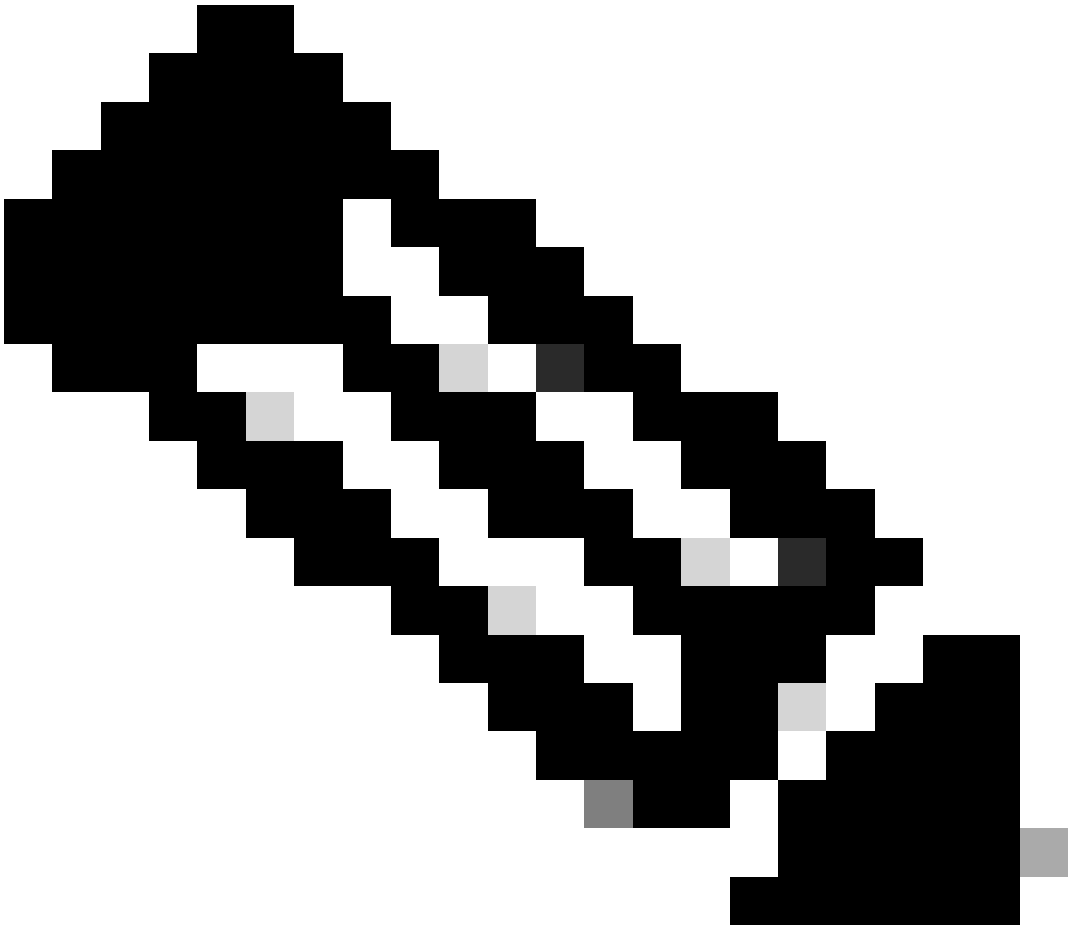
con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

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

3단계. 기본 유닛의 LinkDOWN E1/1

4단계. 장애 조치 상태 확인

시스템 컨텍스트에서 그룹 1에서 장애 조치가 발생하는지 확인합니다.



참고: 장애 조치의 상태는 트래픽 흐름 조건 4와 일치합니다.

<#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

5단계. 장애 조치 후 FTP 연결 확인

실행을 changeto context con1실행하여 시스템 컨텍스트에서 con1 컨텍스트를 연결하고 FTP 연결이 중단되지 않았는지 확인합니다.

<#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

6단계. 선점 시간 동작 확인

기본 유닛의 LinkUP E1/1에서 30초(선점 시간)를 기다리면 장애 조치 상태가 원래 상태(패턴 1의 트래픽 흐름 일치)로 돌아갑니다.

<#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

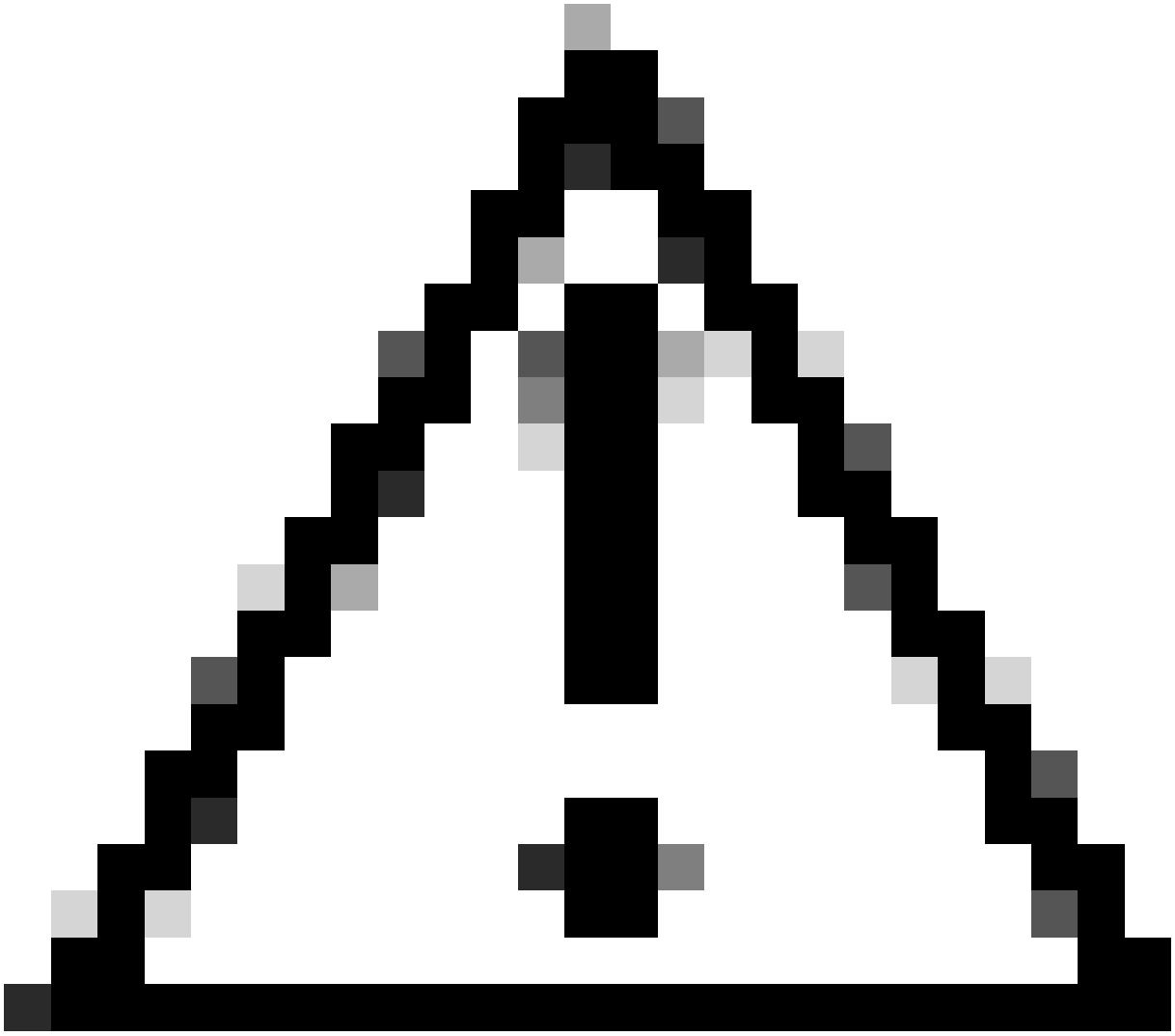
Active time: 10816 (sec) con1 Interface con1-inside (192.168.10.253): Normal (Monitored) con1 Interfac

가상 MAC 주소

액티브/액티브 장애 조치에서는 가상 MAC 주소(수동으로 값을 설정하거나 자동으로 생성된 값 또는 기본값)가 항상 사용됩니다. 액티브 가상 MAC 주소는 액티브 인터페이스와 연결됩니다.

수동으로 가상 MAC 주소 설정

물리적 인터페이스에 대한 가상 MAC 주소를 수동으로 설정하기 위해 I/F 설정 모드에서 mac address mac-address 명령 또는 명령을 사용할 수 있습니다. 이는 물리적 인터페이스 E1/1에 대한 가상 MAC 주소를 수동으로 설정하는 예입니다.



주의: 동일한 디바이스에서 이 두 가지 유형의 명령을 사용하지 마십시오.

<#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

또는

<#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

가상 MAC 주소의 자동 설정

가상 MAC 주소의 자동 생성도 지원됩니다. 이 명령은 명령을 사용하여 구현할 수 mac-address auto <prefix prefix> 있습니다. 가상 MAC 주소의 형식은 자동으로 생성되는 A2 xx.yyzz.zzzz입니다.
A2: 고정 값
xx.yy : 명령 옵션에 지정된 <prefix prefix>에 의해 생성됩니다(접두사는 16진수로 변환된 후 역순으로 삽입됨).
zz.zzzz : 내부 카운터에 의해 생성됩니다.

인터페이스에 대한 명령으로 가상 MAC 주소를 생성하 **mac-address auto** 는 예입니다.

<#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
```

가상 MAC 주소의 기본 설정

가상 MAC 주소의 자동 생성과 수동 생성 모두 설정되지 않은 경우 기본 가상 MAC 주소가 사용됩니다.

기본 가상 MAC 주소에 대한 자세한 내용은 Cisco Secure Firewall ASA Series 명령 참조 가이드에서 Command Default of mac address를 참조하십시오.

업그레이드

CLI 또는 ASDM을 사용하여 액티브/액티브 장애 조치 쌍의 다운타임 없이 업그레이드할 수 있습니다. 자세한 내용은 액티브/액티브 장애 조치 쌍 업그레이드를 참조하십시오.

관련 정보

- CLI를 사용하여 액티브/액티브 장애 조치 쌍 업그레이드
- MAC 주소
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.