

# Cisco FirePOWER 7000 및 8000 Series 디바이스의 클러스터링 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[클러스터 추가](#)

[클러스터 분리](#)

[상태 공유](#)

[문제 해결](#)

[장치가 올바르게 구성되지 않음](#)

[모든 HA 구성원에 최신 정책이 있어야 함](#)

[관련 문서](#)

## 소개

디바이스 클러스터링은 두 디바이스 또는 스택 간에 컨피그레이션 및 네트워킹 기능의 이중화를 제공합니다. 이 문서에서는 Cisco Firepower 7000 및 8000 Series 디바이스에서 클러스터링을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

클러스터를 설정하기 전에 클러스터링의 다양한 기능에 익숙해야 합니다. 자세한 내용은 FireSIGHT System 사용 설명서의 클러스터링 디바이스 섹션을 읽어 보시기 바랍니다.

## 요구 사항

두 디바이스 모두 다음과 같은 동일한 구성 요소가 있어야 합니다.

1. 동일한 하드웨어 모델  
**참고:** 클러스터에서 스택과 단일 디바이스를 구성할 수 없습니다. 동일한 유형 또는 두 개의 유사한 단일 디바이스 스택에 있어야 합니다.
2. 동일한 슬롯에 동일한 네트워크 모듈(Netmod)  
**참고:** 클러스터의 사전 요구 사항을 확인할 때 스택킹 네트워크는 고려되지 않습니다. 빈 슬롯과 같은 것으로 간주됩니다.
3. 동일한 라이선스와 정확히 동일해야 합니다. 한 디바이스에 추가 라이선스가 있으면 클러스터를 구성할 수 없습니다.
4. 동일한 소프트웨어 버전
5. 동일한 VDB 버전
6. 동일한 NAT 정책(구성된 경우)

## 사용되는 구성 요소

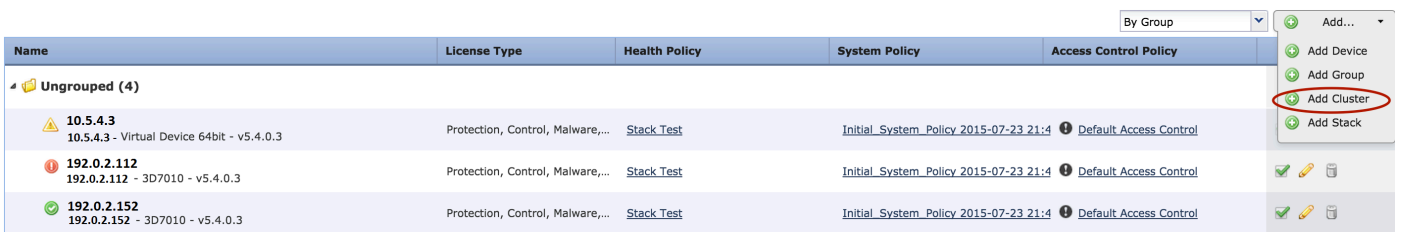
- 버전 5.4.0.4에서 Cisco Firepower 7010 2개
- FireSIGHT Management Center 5.4.1.3

**참고:** 이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

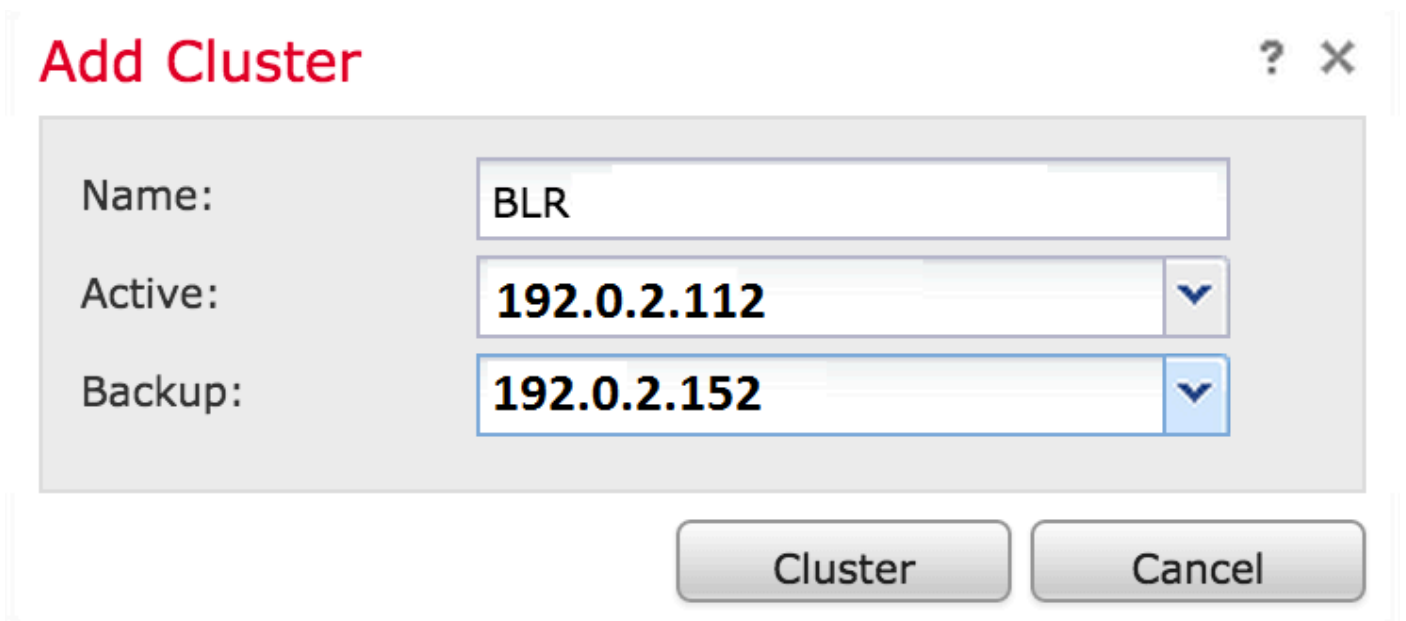
### 클러스터 추가

1. Device(디바이스) > Device Management(디바이스 관리)로 이동합니다.
2. 클러스터링할 디바이스를 선택합니다. 페이지 오른쪽 상단에서 Add 드롭다운 목록을 선택합니다.
3. 클러스터 추가를 선택합니다.



Name	License Type	Health Policy	System Policy	Access Control Policy
Ungrouped (4)				
10.5.4.3 10.5.4.3 - Virtual Device 64bit - v5.4.0.3	Protection, Control, Malware,...	Stack Test	Initial System Policy 2015-07-23 21:4	Default Access Control
192.0.2.112 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	Stack Test	Initial System Policy 2015-07-23 21:4	Default Access Control
192.0.2.152 192.0.2.152 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	Stack Test	Initial System Policy 2015-07-23 21:4	Default Access Control

4. Add Cluster 팝업 창이 나타납니다. 다음 화면이 표시됩니다. 액티브 및 백업 디바이스의 IP 주소를 제공합니다.



**Add Cluster** ? X

Name:

Active:  ▼

Backup:  ▼










5. Cluster 버튼을 클릭합니다. 모든 전제 조건이 충족되면 최대 10분 동안 Adding Cluster 상태 창이 표시됩니다.

# Please Wait...










## Adding cluster...



6. 클러스터가 성공적으로 생성되면 Device **Management** 페이지에서 업데이트된 디바이스를 찾습니다.










BLR-Cluster 3D7010 Cluster						  
	192.0.2.112 (active) 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>		
	192.0.2.152 192.0.2.152 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>		

7. 연필 아이콘 옆에 있는 회전 화살표를 클릭하여 클러스터에서 활성 피어를 전환할 수 있습니다.

BLR-Cluster 3D7010 Cluster						  
	192.0.2.112 (active) 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>		
	192.0.2.152 192.0.2.152 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>		

## 클러스터 분리

휴지통 아이콘 옆에 있는 Break cluster 옵션을 클릭하여 클러스터를 중단할 수 있습니다.

BLR-Cluster 3D7010 Cluster						  
	192.0.2.112 (active) 192.0.2.112 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>		
	192.0.2.152 192.0.2.152 - 3D7010 - v5.4.0.3	Protection, Control, Malware,...	<a href="#">Stack Test</a>	<a href="#">Initial_System_Policy 2015-07-23 21:4</a>		

휴지통 아이콘을 클릭하면 백업 디바이스에서 인터페이스 컨피그레이션을 제거하라는 메시지가 표시됩니다. 예 또는 아니오를 선택합니다.

## Confirm Break

Are you sure you want to break the cluster, "BLR-Cluster"?

Remove the interface configurations on **192.0.2.152**

Yes

No

또한 휴지통을 클릭하여 클러스터를 삭제하고 Management Center에서 디바이스 등록을 취소할 수 있습니다.

디바이스에서 Management Center에 대한 액세스 권한이 없는 경우 CLI에서 다음 명령을 사용하여 클러스터링을 중단할 수 있습니다.

> configure clustering disable

## 상태 공유

클러스터링된 상태 공유를 사용하면 클러스터링된 디바이스 또는 클러스터링된 스택이 상태를 동기화하여 디바이스 또는 스택 중 하나에 장애가 발생하면 다른 피어가 트래픽 플로우에 중단 없이 인계할 수 있습니다.

**참고:** 클러스터링된 상태 공유를 구성하기 전에 두 디바이스 또는 클러스터의 기본 스택킹된 디바이스에서 HA(고가용성) 링크 인터페이스를 구성하고 활성화해야 합니다.

**주의:** 상태 공유를 활성화하면 시스템 성능이 저하됩니다.

HA 링크에서 상태 공유를 활성화하려면 다음 단계를 수행하십시오.

1. **Devices > Device Management**로 이동합니다. 클러스터를 선택하고 편집합니다.
2. 인터페이스 탭을 선택합니다.
3. HA 링크로 만들 링크를 선택합니다.
4. 수정(연필 아이콘)을 클릭합니다. Edit **Interface** 창이 나타납니다.

### Edit Interface

? X

None Passive Inline Switched Routed HA Link

Enabled:

Mode: Autonegotiation

MDI/MDIX: Auto-MDIX

MTU: 9922

Save Cancel

5. 링크를 활성화하고 다른 옵션을 구성한 후 **저장**을 클릭합니다.
6. 이제 **Cluster** 탭으로 이동합니다. 페이지 오른쪽 섹션에 **상태 공유**라는 섹션이 표시됩니다.

## State Sharing



<b>Enabled:</b>	No
<b>Statistics:</b>	
<b>HA Link</b>	<input type="radio"/> (s1p3)
<b>Minimum Flow Lifetime:</b>	1000 ms
<b>Minimum Sync. Interval:</b>	100 ms
<b>Maximum HTTP URL Length:</b>	32

- 연필 아이콘을 클릭하여 상태 공유 옵션을 편집합니다.
- 사용가능 옵션이 선택되었는지 확인합니다.
- 플로우 수명, 동기화 간격 및 최대 HTTP URL 길이를 변경할 수도 있습니다.

이제 상태 공유가 활성화됩니다. Statistics 옆에 있는 돋보기 아이콘을 클릭하여 트래픽 통계를 확인할 수 있습니다. 아래 그림과 같이 두 디바이스에 대한 트래픽 통계가 표시됩니다.

### State Sharing Statistics



	Active Peer	Backup Peer
Device	10.122.144.203	10.122.144.204
Messages Received (Unicast)	0	0
Packets Received	0	0
Total Bytes Received	0	0
Protocol Bytes Received	0	0
Messages Sent	0	0
Packets Sent	0	0
Bytes Sent	0	0
TX Errors	0	0
TX Overruns	0	0
Recent Logs	<a href="#">View</a>	<a href="#">View</a>

Refresh

Close

State Sharing(상태 공유)이 활성화되고 Active(활성) 멤버의 인터페이스가 다운되면 모든 TCP 연결이 이제 Active(활성)가 된 Standby(대기) 디바이스로 전송됩니다.

## 문제 해결

## 장치가 올바르게 구성되지 않음

사전 요구 사항 중 하나가 충족되지 않으면 다음 오류 메시지가 나타납니다.

### Error



Device **192.0.2.152** is not properly configured to be a part of the cluster for **192.0.2.112** - check SW versions, HW, licensing, and applied NAT policy

OK

Management Center에서 **Devices > Device Management**로 이동하여 두 디바이스 모두 소프트웨어 버전, 하드웨어 모델, 라이선스 및 정책이 같은지 확인합니다.

또는 디바이스에서 다음 명령을 실행하여 적용된 액세스 제어 정책과 하드웨어 및 소프트웨어 버전을 확인할 수 있습니다.

```
> show summary
-----[ Device ]-----
Model                : Virtual Device 64bit (69) Version 5.4.0.4 (Build 55)
UUID                 : 4dfa9fca-30f4-11e5-9eb3-b150a60d4996
VDB version          : 252
-----
```

```
-----[ policy info ]-----
Access Control Policy : Default Access Control
Intrusion Policy      : Initial Inline Policy
.
```

*Output Truncated*

NAT 정책을 확인하려면 디바이스에서 다음 명령을 실행합니다.

```
> show nat config
```

**참고:** 라이선스는 Management Center에만 저장되므로 Management Center에서만 확인할 수 있습니다.

모든 HA 구성원에 최신 정책이 있어야 함

다음과 같은 오류가 발생할 수 있습니다.

## Error



All members of an HA config must have up-to-date policies deployed to them. The following devices are out of date: **192.0.2.112**

OK

이 오류는 액세스 제어 정책이 최신 상태가 아닐 때 발생합니다. 정책을 다시 적용하고 클러스터 컨피그레이션을 다시 시도합니다.

## 관련 문서

- [클러스터링 디바이스 - FireSIGHT System 사용 설명서](#)