

ZBFW 고가용성 구성 및 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기규칙](#)

[구성](#)

[예 1: 라우터 1 컨피그레이션 조각\(호스트 이름 ZBFW1\)](#)

[예 2: 라우터 2 컨피그레이션 코드 조각\(호스트 이름 ZBFW2\)](#)

[문제 해결](#)

[디바이스가 서로 통신할 수 있는지 확인](#)

[예 3: 피어 상태 감지](#)

[예 4: 세분화된 출력](#)

[예 5: 역할 상태 및 우선 순위](#)

[예 6: RII 그룹 ID가 할당되었는지 확인](#)

[연결이 피어 라우터에 복제되는지 확인합니다.](#)

[예 7: 처리된 연결](#)

[디버그 출력 수집](#)

[일반적인 문제](#)

[제어 및 데이터 인터페이스 선택](#)

[RII 그룹 없음](#)

[자동 장애 조치](#)

[비대칭 라우팅](#)

[예 11: 비대칭 라우팅 컨피그레이션](#)

[관련 정보](#)

소개

이 설명서에서는 액티브/스탠바이 설정에 대한 HA(Zone Firewall High Availability)의 기본 컨피그레이션, 트러블슈팅 명령 및 이 기능에 나타난 일반적인 문제를 설명합니다.

Cisco IOS[®] ZBFW(Zone-Based Firewall)는 액티브/스탠바이 또는 액티브/액티브 설정에서 두 Cisco IOS 라우터를 구성할 수 있도록 HA를 지원합니다. 따라서 단일 장애 지점을 방지하기 위해 이중화가 가능합니다.

사전 요구 사항

요구 사항

Cisco IOS Software Release 15.2(3)T 이후 릴리스가 있어야 합니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

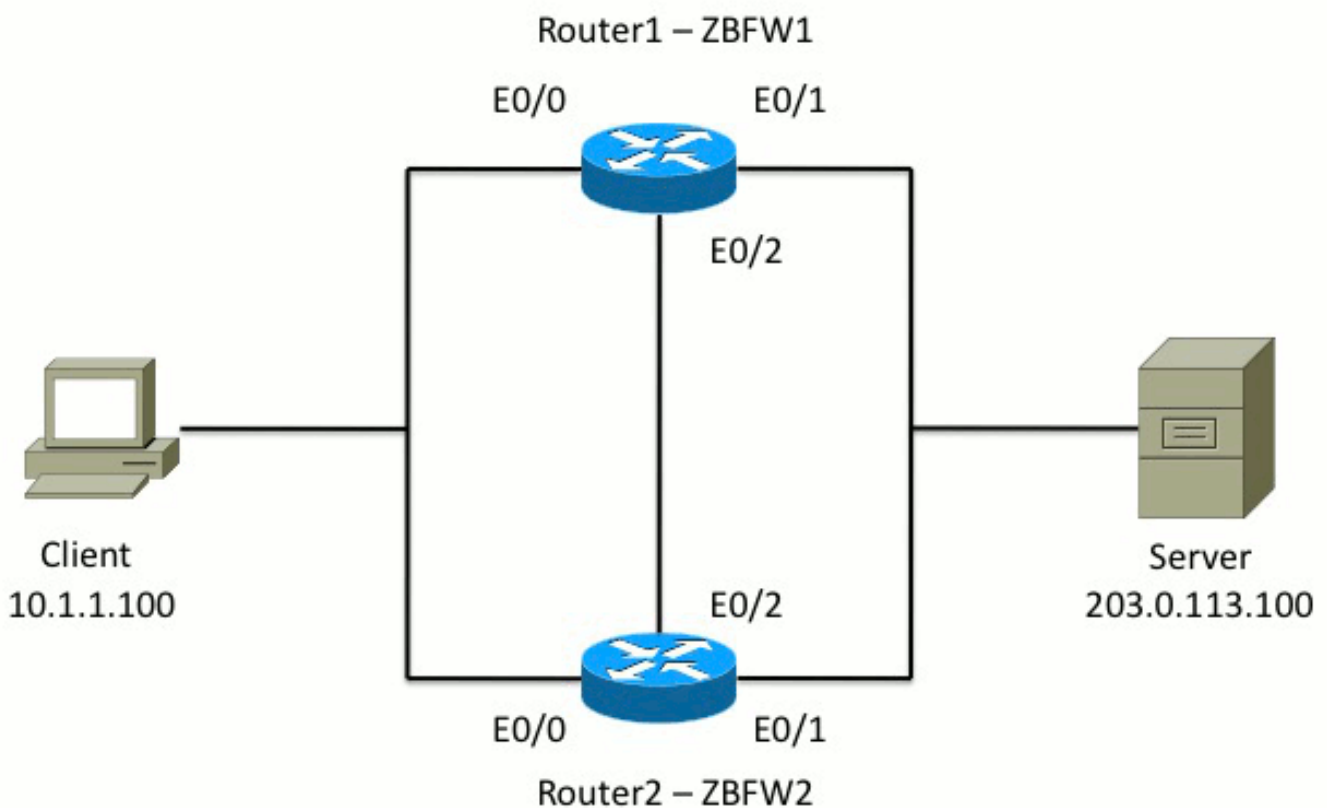
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

구성

이 다이어그램은 컨피그레이션 예에 사용된 토폴로지를 보여줍니다.



예 1에 표시된 컨피그레이션에서는 내부에서 외부로 TCP, UDP 및 ICMP(Internet Control Message Protocol) 트래픽을 검사하도록 ZBFW가 구성됩니다. 굵게 표시된 컨피그레이션은 HA 기능을 설정합니다. Cisco IOS 라우터에서 HA는 redundancy subconfig 명령을 통해 구성됩니다. 이중화를 구성하려면 먼저 글로벌 검사 매개변수 맵에서 이중화를 활성화합니다.

이중화를 활성화한 후 **애플리케이션 이중화** 하위 컨피그레이션을 입력하고 **제어 및 데이터**에 사용되는 인터페이스를 선택합니다. 제어 인터페이스는 각 라우터의 상태에 대한 정보를 교환하기 위해 사용됩니다. 데이터 인터페이스는 복제해야 하는 연결에 대한 정보를 교환하기 위해 사용됩니다.

예 2에서 **priority** 명령은 라우터 1과 라우터 2가 모두 작동하는 경우 라우터 1을 쌍에서 액티브 유닛으로 설정하도록 설정됩니다. **preempt** 명령(이 문서에서 자세히 설명됨)은 우선 순위가 변경되면 오류가 발생하는지 확인하는 데 사용됩니다.

마지막 단계는 각 인터페이스에 **RII(Redundant Interface Identifier)** 및 **RG(Redundancy Group)**를 할당하는 것입니다. RII 그룹 번호는 각 인터페이스에 대해 고유해야 하지만 동일한 서브넷에 있는 인터페이스에 대해 디바이스 간에 일치해야 합니다. RII는 두 라우터가 컨피그레이션을 동기화할 때 대량 동기화 프로세스에만 사용됩니다. 두 라우터가 이중화 인터페이스를 동기화하는 방법입니다. RG는 해당 인터페이스를 통한 연결이 HA 연결 테이블에 복제됨을 나타내는 데 사용됩니다.

예 2에서 **redundancy group 1** 명령은 내부 인터페이스에서 VIP(가상 IP) 주소를 생성하기 위해 사용됩니다. 이는 모든 내부 사용자가 활성 유닛이 처리하는 VIP와 통신하기 때문에 HA가 보장됩니다.

외부 인터페이스에는 WAN 인터페이스이므로 RG 컨피그레이션이 없습니다. 라우터 1과 라우터 2의 외부 인터페이스는 동일한 ISP(인터넷 서비스 공급자)에 속하지 않습니다. 외부 인터페이스에서 트래픽이 올바른 디바이스로 전달되도록 하려면 동적 라우팅 프로토콜이 필요합니다.

예 1: 라우터 1 컨피그레이션 조각(호스트 이름 ZBFW1)

```
parameter-map type inspect global
redundancy
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
zone security INSIDE
zone security OUTSIDE
```

```

zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
zone-member security INSIDE
redundancy rii 100
redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
ip address 203.0.113.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
zone-member security OUTSIDE
redundancy rii 200

```

예 2: 라우터 2 컨피그레이션 코드 조각(호스트 이름 ZBFW2)

```

parameter-map type inspect global
redundancy
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
ip address 10.1.1.2 255.255.255.0
ip nat inside
ip virtual-reassembly in
zone-member security INSIDE
redundancy rii 100

```

```
redundancy group 1 ip 10.1.1.3 exclusive
!  
interface Ethernet0/1  
ip address 203.0.113.2 255.255.255.0  
ip nat outside  
ip virtual-reassembly in  
zone-member security OUTSIDE  
redundancy rii 200
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

디바이스가 서로 통신할 수 있는지 확인

디바이스가 서로를 볼 수 있는지 확인하려면 이중화 애플리케이션 그룹의 작동 상태가 작동 중인지 확인해야 합니다. 그런 다음 각 디바이스가 올바른 역할을 수행했는지 확인하고 올바른 역할에서 해당 피어를 볼 수 있는지 확인합니다. 예 3에서 ZBFW1은 활성 상태이며 해당 피어를 대기 상태로 탐지합니다. 이는 ZBFW2에서 반전됩니다. 두 디바이스 모두 작동 상태가 가동 중이고 해당 피어 상태가 탐지되면 두 라우터가 제어 링크 전체에서 성공적으로 통신할 수 있습니다.

예 3: 피어 상태 감지

```
ZBFW1# show redundancy application group 1  
Group ID:1  
Group Name:ZBFW_HA  
  
Administrative State: No Shutdown  
Aggregate operational state : Up  
My Role: ACTIVE  
Peer Role: STANDBY  
Peer Presence: Yes  
Peer Comm: Yes  
Peer Progression Started: Yes  
  
RF Domain: btob-one  
RF state: ACTIVE  
Peer RF state: STANDBY COLD-BULK  
!  
ZBFW2# show redundancy application group 1  
Group ID:1  
Group Name:ZBFW_HA  
  
Administrative State: No Shutdown  
Aggregate operational state : Up  
My Role: STANDBY  
Peer Role: ACTIVE  
Peer Presence: Yes  
Peer Comm: Yes  
Peer Progression Started: Yes  
  
RF Domain: btob-one  
RF state: STANDBY COLD-BULK  
Peer RF state: ACTIVE
```

예 4의 출력은 두 라우터의 제어 인터페이스에 대한 보다 세분화된 출력을 보여줍니다. 출력은 제어

트래픽에 사용되는 물리적 인터페이스를 확인하고 피어의 IP 주소를 확인합니다.

예 4: 세분화된 출력

```
ZBFW1# show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.60.1.2 Standby RGs: 1 BFD handle: 0
```

```
ZBFW1# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
!
```

```
ZBFW2# show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.60.1.1 Active RGs: 1 BFD handle: 0
```

```
ZBFW2# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
```

통신이 설정되면 Example 5의 명령을 사용하여 각 디바이스가 특정 역할에 속해 있는 이유를 이해할 수 있습니다. ZBFW1은 피어보다 우선순위가 높으므로 활성 상태입니다. ZBFW1의 우선 순위는 200이고, ZBFW2의 우선 순위는 150입니다. 이 출력이 굵게 강조 표시됩니다.

예 5: 역할 상태 및 우선 순위

```
ZBFW1# show redundancy application protocol group 1

RG Protocol RG 1
Role: Active
Negotiation: Enabled
Priority: 200
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 10.60.1.2, priority 150, intf Et0/2
Log counters:
role change to active: 1
role change to standby: 0
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0

RG Media Context for RG 1
-----
Ctx State: Active
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
```

```
Pkts 249, Bytes 15438, HA Seq 0, Seq Number 249, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Standby Peer: Present. Hold Timer: 10000
Pkts 237, Bytes 8058, HA Seq 0, Seq Number 252, Pkt Loss 0
```

```
!
ZBFW2# show redundancy application protocol group 1
```

```
RG Protocol RG 1
-----
Role: Standby
Negotiation: Enabled
Priority: 150
Protocol state: Standby-cold
Ctrl Intf(s) state: Up
Active Peer: address 10.60.1.1, priority 200, intf Et0/2
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0
```

```
RG Media Context for RG 1
-----
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 232, Bytes 14384, HA Seq 0, Seq Number 232, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 220, Bytes 7480, HA Seq 0, Seq Number 229, Pkt Loss 0
```

마지막 확인은 RII 그룹 ID가 각 인터페이스에 할당되었는지 확인하는 것입니다. 두 라우터에서 이 명령을 입력할 경우, 디바이스 간 동일한 서브넷에 있는 인터페이스 쌍에 동일한 RII ID가 할당되도록 두 번 체크인합니다. 동일한 고유 RII ID로 구성되지 않은 경우 두 디바이스 간에 연결이 복제되지 않습니다. 예 6을 참조하십시오.

예 6: RII 그룹 ID가 할당되었는지 확인

```
ZBFW1# show redundancy rii
No. of RIIs in database: 2
Interface RII Id decrement
Ethernet0/1 : 200      0
Ethernet0/0 : 100      0
!
ZBFW2# show redundancy rii
No. of RIIs in database: 2
```

```
Interface RII Id decrement
Ethernet0/1 : 200      0
Ethernet0/0 : 100      0
```

연결이 피어 라우터에 복제되는지 확인합니다.

예 7에서 ZBFW1은 연결을 위해 트래픽을 능동적으로 전달합니다. 연결이 대기 장치 ZBFW2에 성공적으로 복제되었습니다. 영역 방화벽에서 처리된 연결을 보려면 **show policy-firewall session** 명령을 사용하십시오.

예 7: 처리된 연결

```
ZBFW1#show policy-firewall session
Session B2704178 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
SIS_OPEN/TCP_ESTAB
Created 00:00:31, Last heard 00:00:30
Bytes sent (initiator:responder) [37:79]
HA State: ACTIVE, RG ID: 1
Established Sessions = 1
```

```
ZBFW2#show policy-firewall session
Session B2601288 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
SIS_OPEN/TCP_ESTAB
Created 00:00:51, Last heard never
Bytes sent (initiator:responder) [0:0]
HA State: STANDBY, RG ID: 1
Established Sessions = 1
```

연결이 복제되지만 전송된 바이트는 업데이트되지 않습니다. 장애 조치 이벤트가 발생할 경우 트래픽이 영향을 받지 않도록 데이터 인터페이스를 통해 연결 상태(TCP 정보)가 정기적으로 업데이트됩니다.

보다 세부적인 출력을 보려면 **show policy-firewall session zone-pair <ZP> ha** 명령을 입력합니다. Example 7과 유사한 출력을 제공하지만 사용자가 지정된 영역 쌍으로만 출력을 제한할 수 있습니다.

디버그 출력 수집

이 섹션에서는 이 기능의 문제를 해결하기 위해 관련 출력을 생성하는 debug 명령을 보여 줍니다.

디버그 활성화는 사용 중인 라우터에서 매우 까다로울 수 있습니다. 따라서, 이를 활성화하기 전에 영향을 이해해야 합니다.

• 디버그 리던던시 응용 프로그램 그룹 라이브 이벤트

이 명령은 연결이 올바른 RII 그룹과 일치하여 올바르게 복제되도록 하기 위해 사용됩니다. 트래픽이 ZBFW에 도착하면 소스 및 대상 인터페이스에서 RII 그룹 ID를 확인합니다. 그런 다음 데이터 링크를 통해 피어에 이 정보가 전달됩니다. 대기 피어의 RII 그룹이 활성 유닛과 정렬되면 Example 8의 syslog가 생성되고 연결을 복제하는 데 사용되는 RII 그룹 ID를 확인합니다.

예 8: Syslog


```
debug redundancy application group rii event
debug redundancy application group rii error
!
*Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:100
*Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:200
```

• 디버그 이중화 애플리케이션 그룹 프로토콜 모두

이 명령은 두 피어가 서로를 볼 수 있는지 확인하는 데 사용됩니다. 피어 IP 주소가 디버그에서 확인됩니다. 예 9에서 볼 수 있듯이 ZBFW1은 IP 주소가 **10.60.1.2**인 대기 상태의 피어를 확인합니다. ZBFW2의 경우 역방향이 적용됩니다.

예 9: 디버그의 피어 IP 확인

```
debug redundancy application group protocol all
!
ZBFW1#
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Standby,
addr=10.60.1.2, present=exist, reload=0, intf=Et0/2, priority=150.
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] set peer_status 0.
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] priority_event
'media: low priority from standby', role_event 'no event'.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] select fsm event,
priority_event=media: low priority from standby, role_event=no event.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] process FSM event
'media: low priority from standby'.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] no FSM transition

ZBFW2#
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Active,
addr=10.60.1.1, present=exist, reload=0, intf=Et0/2, priority=200.
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot]
set peer_status 0.
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot] priority_event
'media: high priority from active', role_event 'no event'.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] select
fsm event, priority_event=media: high priority from active, role_event=no event.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] process
FSM event 'media: high priority from active'.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] no FSM
transition
```

일반적인 문제

이 섹션에서는 몇 가지 일반적인 문제를 자세히 설명합니다.

제어 및 데이터 인터페이스 선택

다음은 제어 및 데이터 VLAN에 대한 몇 가지 팁입니다.

- ZBFW 컨피그레이션에 컨트롤 및 데이터 인터페이스를 포함하지 마십시오. 서로 통신하기 위해서만 사용됩니다. 따라서 이러한 인터페이스를 보호할 필요가 없습니다.
- 제어 및 데이터 인터페이스는 동일한 인터페이스 또는 VLAN에 있을 수 있습니다. 이렇게 하면 라우터의 포트가 보존됩니다.

RII 그룹 없음

RII 그룹은 LAN 및 WAN 인터페이스 모두에 적용해야 합니다. LAN 인터페이스는 동일한 서브넷에 있어야 하지만 WAN 인터페이스는 별도의 서브넷에 있을 수 있습니다. 인터페이스에 RII 그룹이 없는 경우 이 syslog는 **debug 이중화 애플리케이션 그룹 라이브 이벤트 출력과 디버그 이중화 애플리케이션 그룹 오류**에서 발생합니다.

```
000515: Dec 20 14:35:07.753 EST: FIREWALL*: RG not found for ID 0
```

자동 장애 조치

자동 장애 조치를 구성하려면 SLA(Service Level Agreement) 객체를 추적하고 이 SLA 이벤트에 따라 우선순위를 동적으로 줄이기 위해 ZBFW HA를 구성해야 합니다. 예 10에서 ZBFW HA는 GigabitEthernet0 인터페이스의 링크 상태를 추적합니다. 이 인터페이스가 다운되면 피어 디바이스가 더 선호되도록 우선 순위가 낮아집니다.

예 10: ZBFW HA 자동 장애 조치 컨피그레이션

```
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 230
control Vlan801 protocol 1
data Vlan801
track 1 decrement 200
!
track 1 interface GigabitEthernet0 line-protocol
```

```
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 180
control Vlan801 protocol 1
data Vlan801
```

우선 순위 이벤트가 감소하더라도 ZBFW HA는 자동으로 장애 조치를 수행하지 않는 경우가 있습니다. 이는 preempt 키워드가 두 디바이스 모두에서 구성되지 않았기 때문입니다. preempt 키워드는 HSRP(Hot Standby Router Protocol) 또는 ASA(Adaptive Security Appliance) 장애 조치 기능과 다릅니다. ZBFW HA에서 preempt 키워드는 디바이스의 우선순위가 변경되면 장애 조치 이벤트가 발생할 수 있도록 합니다. 이 내용은 [보안 컨피그레이션 가이드](#)에 설명되어 있습니다. [Zone-Based Policy Firewall, Cisco IOS Release 15.2M&T](#). 다음은 Zone-Based Policy Firewall High Availability 장에서 추출하는 내용입니다.

"다른 상황에서는 스탠바이 디바이스로의 전환이 발생할 수 있습니다. 전환을 일으킬 수 있는 또 다른 요인은 각 디바이스에서 구성할 수 있는 우선순위 설정입니다. 우선 순위가 가장 높은 디바이스

가 활성 디바이스입니다. 액티브 또는 스탠바이 디바이스에서 결함이 발생할 경우 디바이스의 우선 순위는 구성 가능한 양(가중치)으로 감소합니다. 활성 디바이스의 우선 순위가 대기 디바이스의 우선 순위보다 낮으면 전환이 발생하고 대기 디바이스가 활성 디바이스가 됩니다. 이 기본 동작은 이중화 그룹에 대한 선점 특성을 비활성화하여 재정의할 수 있습니다. 인터페이스의 Layer 1 상태가 다운될 때 우선순위를 낮추도록 각 인터페이스를 구성할 수도 있습니다. 구성된 우선순위는 이중화 그룹의 기본 우선순위를 재정의합니다."

이러한 출력은 적절한 상태를 나타냅니다.

```
ZBFW01#show redundancy application group 1
```

```
Group ID:1
```

```
Group Name:ZBFW_HA
```

```
Administrative State: No Shutdown
```

```
Aggregate operational state : Up
```

```
My Role: ACTIVE
```

```
Peer Role: STANDBY
```

```
Peer Presence: Yes
```

```
Peer Comm: Yes
```

```
Peer Progression Started: Yes
```

```
RF Domain: btob-one
```

```
RF state: ACTIVE
```

```
Peer RF state: STANDBY HOT
```

```
ZBFW01#show redundancy application faults group 1
```

```
Faults states Group 1 info:
```

```
Runtime priority: [230]
```

```
RG Faults RG State: Up.
```

```
Total # of switchovers due to faults: 0
```

```
Total # of down/up state changes due to faults: 0
```

이러한 로그는 활성화된 디버그 없이 ZBFW에서 생성됩니다. 이 로그는 디바이스가 활성화되는 시기를 보여줍니다.

```
*Feb 1 21:47:00.579: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
```

```
Init to Standby
```

```
*Feb 1 21:47:09.309: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Standby
```

```
to Active
```

```
*Feb 1 21:47:19.451: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
```

```
complete.
```

```
*Feb 1 21:47:19.456: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in
```

```
SSO state
```

이 로그에는 디바이스가 대기 모드로 전환되는 시간이 표시됩니다.

```
*Feb 1 21:47:07.696: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
```

```
complete.
```

```
*Feb 1 21:47:07.701: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in
```

```
SSO state
```

```
*Feb 1 21:47:09.310: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Active
```

```
to Init
```

```
*Feb 1 21:47:19.313: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
```

```
Init to Standby
```

비대칭 라우팅

비대칭 라우팅 지원은 Asymmetric [Routing Support](#) 가이드에서 제공됩니다.

비대칭 라우팅을 구성하려면 이중화 애플리케이션 그룹 전역 컨피그레이션과 인터페이스 하위 컨피그레이션 모두에 기능을 추가합니다. 비대칭 라우팅 및 RG는 지원되지 않으므로 동일한 인터페이스에서 활성화할 수 없습니다. 이는 비대칭 라우팅의 작동 방식 때문입니다. 비대칭 라우팅을 위해 인터페이스가 지정된 경우 라우팅이 일관되지 않으므로 해당 시점에서는 HA 연결 복제의 일부가 될 수 없습니다. RG는 인터페이스가 HA 연결 복제의 일부임을 지정하므로 RG를 구성하면 라우터가 구성됩니다.

예 11: 비대칭 라우팅 컨피그레이션

```
redundancy
application redundancy
group 1
asymmetric-routing interface Ethernet0/3

interface Ethernet0/1
redundancy asymmetric-routing enable
```

이 컨피그레이션은 HA 쌍의 두 라우터에 모두 적용해야 합니다.

이전에 나열된 **Ethernet0/3** 인터페이스는 두 라우터 간의 새로운 전용 링크입니다. 이 링크는 두 라우터 간에 비대칭적으로 라우팅된 트래픽을 전달하는 데 배타적으로 사용됩니다. 따라서 외부 연결 인터페이스에 해당하는 전용 링크여야 합니다.

관련 정보

- [보안 구성 가이드: Zone-Based Policy Firewall, Cisco IOS Release 15.2M&T](#)
- [Zone-Based Policy Firewall 고가용성 보안 컨피그레이션 가이드](#)
- [Cisco IOS 15.2M&T](#)
- [Cisco IOS Firewall](#)
- [보안 제품 필드 알림](#)
- [기술 지원 및 문서 - Cisco Systems](#)