



트래픽 흐름, 검사 및 디바이스 동작

업그레이드 중 트래픽 흐름 및 검사에서 잠재적인 중단을 식별해야 합니다. 다음과 같은 경우 발생할 수 있습니다.

- 디바이스를 재부팅할 때.
- 디바이스에서 운영 체제 또는 가상 호스팅 환경을 업그레이드할 때
- 디바이스에서 Firepower 소프트웨어를 업그레이드하거나 패치를 제거할 때
- 업그레이드 또는 삭제 프로세스의 일부로 구성 변경 사항을 배포할 때(Snort 프로세스가 다시 시작).

디바이스 유형, 구축 유형(독립형, 고가용성, 클러스터) 및 인터페이스 구성(패시브, IPS, 방화벽 등)은 중단의 특성을 결정합니다. Cisco는 유지 보수 기간 또는 중단으로 구축에 가장 적은 영향이 발생할 때 업그레이드 또는 삭제를 수행할 것을 강력하게 권장합니다.

- [FTD 업그레이드 동작: Firepower 4100/9300 새시, 1 페이지](#)
- [FTD 업그레이드 동작: 기타 장치, 5 페이지](#)
- [Firepower 7000/8000 Series 업그레이드 동작, 7 페이지](#)
- [ASA FirePOWER 업그레이드 동작, 9 페이지](#)
- [NGIPSv 업그레이드 동작, 10 페이지](#)

FTD 업그레이드 동작: Firepower 4100/9300 새시

이 섹션은 FTD를 사용하는 Firepower 4100/9300 새시를 업그레이드할 때 디바이스 및 트래픽 동작을 설명합니다.

Firepower 4100/9300 새시: FXOS 업그레이드

새시 간 클러스터링 또는 고가용성 쌍이 구성되어 있더라도 각 새시에서 FXOS를 독립적으로 업그레이드합니다. 업그레이드를 수행하는 방법에 따라 FXOS 업그레이드 중에 디바이스가 트래픽을 처리하는 방법이 결정됩니다.

표 1: FXOS 업그레이드 중 트래픽 동작

구축	메서드	트래픽 동작
독립형	—	삭제됨
고가용성	모범 사례: 스탠바이 새시에서 FXOS를 업데이트하고 액티브 피어를 전환한 다음 새 스탠바이 새시를 업그레이드합니다.	영향 없음
	스탠바이 새시 업그레이드가 완료되기 전에 액티브 피어에서 FXOS를 업그레이드합니다.	하나의 피어가 온라인 상태가 될 때까지 삭제됨
새시 간 클러스터 (6.2 이상)	모범 사례: 하나 이상의 모듈이 항상 온라인 상태가 되도록 새시를 한 번에 하나씩 업그레이드합니다.	영향 없음
	특정 시점에 모든 새시가 가동 중지되도록 새시를 동시에 업그레이드합니다.	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨
새시 내 클러스터 (Firepower 9300에만 해당)	하드웨어 우회 활성화됨: 우회: 스탠바이 또는 우회-강제 (6.1 이상)	검사 없이 통과됨
	하드웨어 우회 비활성화됨: 우회: 비활성화됨 (6.1 이상)	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨
	하드웨어 우회 모듈이 없습니다.	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨

독립형 FTD 디바이스: Firepower 소프트웨어 업그레이드

Firepower 디바이스/보안 모듈은 업그레이드 중에 유지 보수 모드로 작동합니다. 업그레이드를 시작할 때 유지 보수 모드에 진입하면 트래픽 검사가 2~3초 중단됩니다. 인터페이스 컨피그레이션에 따라 독립형 디바이스가 업그레이드 도중에 트래픽을 처리하는 방법이 결정됩니다.

표 2: Firepower 소프트웨어 업그레이드 중 트래픽 동작: 독립형 FTD 디바이스

인터페이스 컨피그레이션	트래픽 동작
방화벽 인터페이스 라우팅 또는 스위칭 (EtherChannel, 이중화, 하위 인터페이스 포함) 스위칭 인터페이스는 브리지 그룹 또는 투명 모드 인터페이스라고도 합니다.	삭제됨

인터페이스 컨피그레이션		트래픽 동작
IPS 전용 인터페이스	인라인 집합, 하드웨어 우회 강제 활성화 됨: 우회: 강제(6.1 이상)	하드웨어 우회를 비활성화하거나 다시 스탠바이 모드로 설정할 때까지 검사 없이 통과됨
	인라인 집합, 하드웨어 우회 스탠바이 모드: 우회: 스탠바이(6.1 이상)	디바이스가 유지 보수 모드에 있는 동안 업그레이드 중 삭제된 다음 디바이스 업그레이드 후 재부팅을 완료하는 동안 검사 없이 통과됨
	인라인 집합, 하드웨어 우회 비활성화됨: 우회: 비활성화됨(6.1 이상)	삭제됨
	인라인 집합, 하드웨어 우회 모듈 없음	삭제됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단됨, 검사되지 않음

고가용성 쌍: Firepower 소프트웨어 업그레이드

고가용성 쌍의 디바이스에서 Firepower 소프트웨어를 업그레이드하는 동안 트래픽 흐름 또는 검사가 중단되어서는 안 됩니다. 운영의 연속성을 보장하기 위해 이러한 디바이스는 한 번에 하나씩 업그레이드됩니다. 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다.

스탠바이 디바이스가 먼저 업그레이드됩니다. 디바이스에서 역할을 전환한 후 새 스탠바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스탠바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.

클러스터: Firepower 소프트웨어 업그레이드

Firepower Threat Defense 클러스터의 디바이스에서 Firepower 소프트웨어를 업그레이드하는 동안 트래픽 흐름 또는 검사가 중단되어서는 안 됩니다. 운영의 연속성을 보장하기 위해 이러한 디바이스는 한 번에 하나씩 업그레이드됩니다. 하나 이상의 데이터 보안 모듈이 먼저 업그레이드된 후에 제어 모듈이 업그레이드됩니다. 보안 모듈은 업그레이드 중에 유지 보수 모드로 작동합니다.

제어 보안 모듈이 업그레이드되는 동안에는 트래픽 검사 및 처리가 정상적으로 계속되지만, 시스템에서는 이벤트 로깅이 중지됩니다. 로깅 다운타임 중에 처리되는 트래픽에 대한 이벤트는 업그레이드가 완료된 후 동기화되지 않은 타임스탬프와 함께 표시됩니다. 그러나 로깅 다운타임이 길면 시스템은 가장 오래된 이벤트를 로깅하기 전에 정리할 수 있습니다.



참고

버전 6.2.0, 6.2.0.1 또는 6.2.0.2에서 새시 간 클러스터를 업그레이드하면 트래픽 검사 시 각 모듈이 클러스터에서 제거될 때 약 2~3초의 트래픽 중단이 발생합니다.

고가용성 및 클러스터링 무중단 업그레이드 요구 사항

무중단 업그레이드를 수행하려면 다음 추가 요구 사항이 필요합니다.

플로우 오프로드: 플로우 오프로드 기능의 버그 수정으로 일부 FXOS 및 FTD 조합은 플로우 오프로드를 지원하지 않습니다. [Cisco FirePOWER 호환성 가이드](#)를 참조하십시오.고가용성 또는 클러스터링 구축의 무중단 업그레이드를 수행하려면 항상 호환되는 조합이 실행 중인지 확인해야 합니다.

업그레이드 경로에 FXOS를 2.2.2.91, 2.3.1.130 또는 그 이후 버전(FXOS 2.4.1.x, 2.6.1.x 등 포함)으로 업그레이드하는 내용이 포함된 경우 다음 경로를 사용합니다.

1. FTD를 6.2.2.2 이상으로 업그레이드합니다.
2. FXOS를 2.2.2.91, 2.3.1.130 또는 그 이후 버전으로 업그레이드합니다.
3. FTD를 최종 버전으로 업그레이드합니다.

예를 들어 FXOS 2.2.2.17/FTD 6.2.2.0를 사용 중일 때 FXOS 2.6.1/FTD 6.4.0으로 업그레이드하려는 경우 다음을 수행할 수 있습니다.

1. FTD를 6.2.2.5로 업그레이드합니다.
2. FXOS를 2.6.1로 업그레이드합니다.
3. FTD를 6.4.0으로 업그레이드합니다.

버전 6.1.0 업그레이드: FTD고가용성 쌍을 버전 6.1.0으로 무중단 업그레이드하려면 사전 설치 패키지가 필요합니다. 자세한 내용은 [Firepower System 릴리스 노트 버전 6.1.0 사전 설치 패키지](#)를 참조하십시오.

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)의 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 Snort 프로세스를 재시작하면 HA/확장성 구성을 비롯해 모든 Firepower 디바이스에서 트래픽 검사가 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

표 3: FTD 구축 중 트래픽 동작

인터페이스 컨피그레이션		트래픽 동작
방화벽 인터페이스	라우팅 또는 스위칭(EtherChannel, 이중화, 하위 인터페이스 포함) 스위칭 인터페이스는 브리지 그룹 또는 투명 모드 인터페이스라고도 합니다.	삭제됨

인터페이스 컨피그레이션		트래픽 동작
IPS 전용 인터페이스	인라인 집합, Failsafe 활성화 또는 비활성화됨(6.0.1~6.1)	검사 없이 통과됨 Failsafe 가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
	인라인 집합, Snort Fail Open: 중단: 비 활성화됨(6.2 이상)	삭제됨
	인라인 집합, Snort Fail Open: 중단: 활 성화됨(6.2 이상)	검사 없이 통과됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단됨, 검사되지 않음

FTD업그레이드 동작: 기타 장치

이 섹션에서는 Firepower 1000/2100 series, ASA 5500-X series, ISA 3000 및 FTDv의 Firepower Threat Defense를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

독립형 **FTD** 디바이스: **Firepower** 소프트웨어 업그레이드

Firepower 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다. 업그레이드를 시작할 때 유지 보수 모드에 진입하면 트래픽 검사가 2~3초 중단됩니다. 인터페이스 구성에 따라 독립형 디바이스가 업그레이드 도중에 트래픽을 처리하는 방법이 결정됩니다.

표 4: **Firepower** 소프트웨어 업그레이드 중 트래픽 동작: 독립형 **FTD** 디바이스

인터페이스 컨피그레이션		트래픽 동작
방화벽 인터페이스	라우팅 또는 스위칭(EtherChannel, 이중화, 하위 인터페이스 포함) 스위칭 인터페이스는 브리지 그룹 또는 투명 모드 인터페이스라고도 합니다.	삭제됨

인터페이스 컨피그레이션		트래픽 동작
IPS 전용 인터페이스	인라인 집합, 하드웨어 우회 강제 활성화됨: 우회: 강제(Firepower 2100 Series, 6.3 이상)	하드웨어 우회를 비활성화하거나 다시 스탠바이 모드로 설정할 때까지 검사 없이 통과됨
	인라인 집합, 하드웨어 우회 스탠바이 모드: 우회: 스탠바이(Firepower 2100 Series, 6.3 이상)	디바이스가 유지 보수 모드에 있는 동안 업그레이드 중에 삭제된 디바이스 업그레이드 후 재부팅을 완료하는 동안 검사 없이 통과됨
	인라인 집합, 하드웨어 우회 비활성화됨: 우회: 비활성화됨(Firepower 2100 Series, 6.3 이상)	삭제됨
	인라인 집합, 하드웨어 우회 모듈 없음	삭제됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSpan 패시브	중단됨, 검사되지 않음

고가용성 쌍: Firepower 소프트웨어 업그레이드

고가용성 쌍의 디바이스에서 Firepower 소프트웨어를 업그레이드하는 동안 트래픽 흐름 또는 검사가 중단되어서는 안 됩니다. 운영의 연속성을 보장하기 위해 이러한 디바이스는 한 번에 하나씩 업그레이드됩니다. 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다.

스탠바이 디바이스가 먼저 업그레이드됩니다. 디바이스에서 역할을 전환한 후 새 스탠바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스탠바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)의 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 Snort 프로세스를 재시작하면 HA/확작성 구성을 비롯해 모든 Firepower 디바이스에서 트래픽 검사가 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

표 5: FTD 구축 중 트래픽 동작

인터페이스 컨피그레이션	트래픽 동작	
방화벽 인터페이스 라우팅 또는 스위칭(EtherChannel, 이중화, 하위 인터페이스 포함) 스위칭 인터페이스는 브리지 그룹 또는 투명 모드 인터페이스라고도 합니다.	삭제됨	
IPS 전용 인터페이스	인라인 집합, Failsafe 활성화 또는 비활성화됨(6.0.1~6.1)	검사 없이 통과됨 Failsafe 가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
	인라인 집합, Snort Fail Open: 중단: 비 활성화됨(6.2 이상)	삭제됨
	인라인 집합, Snort Fail Open: 중단: 활 성화됨(6.2 이상)	검사 없이 통과됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단됨, 검사되지 않음

Firepower 7000/8000 Series 업그레이드 동작

다음 섹션에서는 Firepower 7000 및 8000 Series 디바이스를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

독립형 **7000/8000 Series: Firepower** 소프트웨어 업그레이드

인터페이스 컨피그레이션에 따라 독립형 디바이스가 업그레이드 중에 트래픽을 처리하는 방법이 결정됩니다.

표 6: 업그레이드 중 트래픽 동작: 독립형 7000/8000 Series

인터페이스 컨피그레이션	트래픽 동작
인라인, 하드웨어 바이패스 활성화됨(바이패스 모드: 바이패스)	검사 없이 통과됨. 단, 다음의 두 시점에서 트래픽이 잠시 중단됨. <ul style="list-style-type: none"> 업그레이드 프로세스 시작 시 링크가 끊겼다 연결되었다 하고 네트워크 카드가 하드웨어 바이패스로 전환될 때. 업그레이드 완료 후 링크가 끊겼다 연결되었다 하고 네트워크 카드가 바이패스에서 전환될 때. 엔드포인트가 다시 연결되고 디바이스 인터페이스와의 링크가 다시 설정되면 검사가 다시 시작됨.
인라인, 하드웨어 바이패스 모듈 없음 또는 하드웨어 바이패스 비활성화됨(바이패스 모드: 바이패스 없음)	삭제됨
인라인, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
수동	중단되지 않음, 검사되지 않음
라우팅, 스위칭	삭제됨

7000/8000 Series 고가용성 쌍: Firepower 소프트웨어 업그레이드

고가용성 쌍의 디바이스 또는 디바이스 스택을 업그레이드하는 동안 트래픽 흐름 또는 검사가 중단되어서는 안 됩니다. 운영의 연속성을 보장하기 위해 이러한 디바이스는 한 번에 하나씩 업그레이드됩니다. 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다.

먼저 업그레이드되는 피어는 구축에 따라 달라집니다.

- 라우팅 또는 전환: 대기 업그레이드가 먼저 진행됩니다. 디바이스에서 역할을 전환한 후 새 스텐바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스텐바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.
- 액세스 제어만: 액티브 업그레이드가 먼저 진행됩니다. 업그레이드가 완료되면 액티브 및 스텐바이 피어의 이전 역할이 유지됩니다.

8000 Series 스택: Firepower 소프트웨어 업그레이드

8000 Series 스택에서는 디바이스가 동시에 업그레이드됩니다. 기본 디바이스에서 업그레이드를 완료하고 스택의 작동이 다시 시작될 때까지는 스택이 독립형 디바이스인 것처럼 트래픽이 동작합니다. 모든 디바이스가 업그레이드를 완료할 때까지 스택은 제한된 혼합 버전 상태로 작동합니다.

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)의 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 Snort 프로세스를 재시작하면 HA/확작성 구성을 비롯해 모든 Firepower 디바이스에서 트래픽 검사가 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

표 7: 구축 중 트래픽 동작: 7000/8000 Series

인터페이스 컨피그레이션	트래픽 동작
인라인, Failsafe 활성화 또는 비활성화	검사 없이 통과됨 Failsafe 가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인, 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
수동	중단되지 않음, 검사되지 않음
라우팅, 스위칭	삭제됨

ASA FirePOWER 업그레이드 동작

ASA FirePOWER 모듈로 트래픽을 리디렉션하는 것에 대한 ASA 서비스 정책에 따라 Snort 프로세스를 재시작하는 특정 컨피그레이션을 구축할 때를 포함하여 Firepower 소프트웨어 업그레이드 중에 모듈이 트래픽을 처리하는 방법이 결정됩니다.

표 8: ASA FirePOWER 업그레이드 중 트래픽 동작

트래픽 리디렉션 정책	트래픽 동작
Fail open (sfr fail-open)	검사 없이 통과됨
Fail closed (sfr fail-close)	삭제됨
모니터링 전용(sfr {fail-close} {fail-open} monitor-only)	즉시 패킷 이그레스, 복사 검사되지 않음

ASA FirePOWER 구축 중 트래픽 동작

Snort 프로세스가 재시작되는 동안의 트래픽 동작은 ASA FirePOWER 모듈을 업그레이드할 때와 동일합니다.

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. **Snort**는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)의 구축 또는 활성화 시 **Snort** 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 **Snort** 프로세스를 재시작하면 트래픽 검사가 중단됩니다. 서비스 정책에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

NGIPSv 업그레이드 동작

이 섹션에서는 NGIPSv를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

Firepower 소프트웨어 업그레이드

인터페이스 구성은 업그레이드 중 NGIPSv이 트래픽을 처리하는 방법을 결정합니다.

표 9: NGIPSv 업그레이드 중 트래픽 동작

인터페이스 컨피그레이션	트래픽 동작
인라인	삭제됨
인라인, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
수동	중단되지 않음, 검사되지 않음

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. **Snort**는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)의 구축 또는 활성화 시 **Snort** 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 **Snort** 프로세스를 재시작하면 트래픽 검사가 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

표 10: NGIPSv 구축 중 트래픽 동작

인터페이스 컨피그레이션	트래픽 동작
인라인, Failsafe 활성화 또는 비활성화	검사 없이 통과됨 Failsafe 가 비활성화되어 있고 Snort 가 중단되지 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음

인터페이스 컨피그레이션	트래픽 동작
인라인, 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
수동	중단되지 않음, 검사되지 않음

