인라인 표준화 프리프로세서를 활성화하고 Pre-ACK 및 Post-ACK 검사 이해

목차

소개

이 문서에서는 인라인 표준화 프리프로세서를 활성화하는 방법을 설명하고, 인라인 표준화의 두 고급 옵션의 차이점과 영향을 이해하는 데 도움이 됩니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco Firepower 시스템 및 Snort에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco FireSIGHT Management Center 및 Firepower 어플라이언스를 기반으로 합니다.

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.

배경 정보

인라인 표준화 프리프로세서는 공격자가 인라인 구축을 사용하여 탐지를 회피할 수 있는 가능성을 최소화하기 위해 트래픽을 표준화합니다. 표준화는 패킷 디코딩 직후 및 다른 프리프로세서 이전에 발생하며, 패킷의 내부 레이어에서 바깥쪽으로 진행됩니다. 인라인 표준화는 이벤트를 생성하지 않지만 다른 프리프로세서에서 사용할 패킷을 준비합니다.

인라인 표준화 프리프로세서가 활성화된 상태에서 침입 정책을 적용할 경우, Firepower 디바이스는 인라인 구축을 사용하도록 하기 위해 다음 두 가지 조건을 테스트합니다.

- 버전 5.4 이상에서는 NAP(Network Analysis Policy)에서 *인라인 모드*가 활성화되며, 침입 정책이 트래픽을 삭제하도록 설정된 경우 침입 정책에서도 Drop when Inline이 구성됩니다. 버전 5.3 이하의 경우 침입 *정책*에서 Drop when Inline 옵션이 활성화됩니다.

- 정책은 인라인(또는 failopen을 사용하는 인라인) 인터페이스 집합에 적용됩니다.

따라서 인라인 표준화 프리프로세서의 활성화 및 컨피그레이션 외에도 이러한 요구 사항이 충족되는지 확인해야 합니다. 그렇지 않으면 프리프로세서가 트래픽을 표준화하지 않습니다.

- 인라인 구축에서 트래픽을 삭제하도록 정책을 설정해야 합니다.

- 인라인 집합에 정책을 적용해야 합니다.

인라인 표준화 사용

이 섹션에서는 버전 5.4 이상 및 버전 5.3 이하에서 인라인 표준화를 활성화하는 방법에 대해 설명합니다.

버전 5.4 이상에서 인라인 표준화 사용

대부분의 프리프로세서 설정은 버전 5.4 이상에 대한 NAP에서 구성됩니다. NAP에서 인라인 표준화를 활성화하려면 다음 단계를 완료하십시오.

1. FireSIGHT Management Center의 웹 UI에 로그인합니다.

2. **Policies > Access Control**로 **이동합니다**.

3. 페이지의 오른쪽 상단 영역 근처에서 **Network Analysis** Policy를 클릭합니다.

4. 관리되는 *디바이스에* 적용할 네트워크 분석 정책을 선택합니다.

5. 수정을 시작하려면 *연필* 아이콘을 클릭하고 *Edit Policy* 페이지가 나타납니다.

6. 화면의 **왼쪽**에서 Settings(설정)를 클릭하면 Settings(설정) *페이지*가 나타납니다.

7. Transport/*Network Layer* **Preprocessor** 영역에서 *Inline Normalization 옵션을* 찾습니다.

8. 이 기능을 **활성화하려면** Enabled 라디오 버튼을 선택합니다.

인라인 표준화가 수행되려면 액세스 제어 정책에 인라인 표준화가 포함된 NAP를 추가해야 합니다. NAP는 액세스 제어 정책 *고급* 탭을 통해 추가할 수 있습니다.

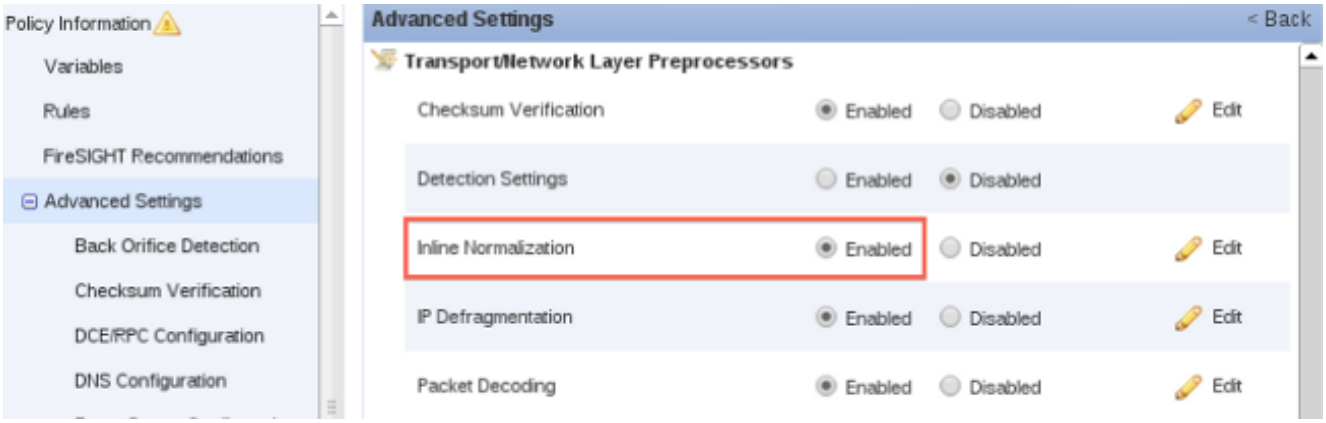
그런 다음 액세스 제어 정책을 검사 장치에 적용해야 합니다.

> **참고:** 버전 5.4 이상에서는 특정 트래픽에 대해 인라인 표준화를 활성화하고 다른 트래픽에 대해서는 비활성화할 수 있습니다. 특정 트래픽에 대해 활성화하려면 *네트워크 분석 규칙*을 추가하고 인라인 표준화가 활성화된 트래픽 기준 및 정책을 설정합니다. 전역적으로 활성화하려면 인라인 표준화가 활성화된 *기본 네트워크 분석* 정책을 설정합니다.

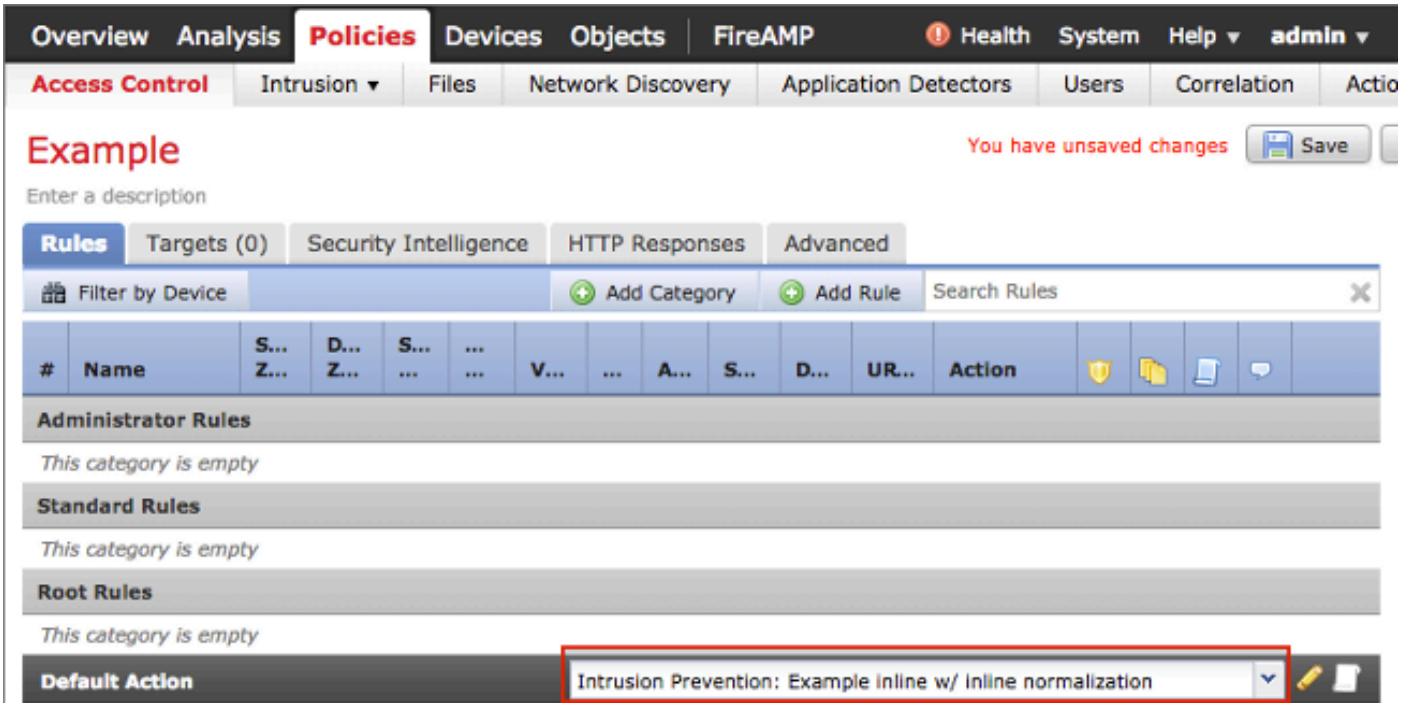
버전 5.3 이하에서 인라인 표준화 사용

침입 정책에서 인라인 표준화를 활성화하려면 다음 단계를 완료하십시오.

1. FireSIGHT Management Center의 웹 UI에 로그인합니다.
2. **Policies > Intrusion > Intrusion Policies로** 이동합니다.
3. 관리되는 *디바이스*에 적용할 침입 정책을 선택합니다.
4. 수정을 시작하려면 *연필* 아이콘을 클릭하고 *Edit Policy* 페이지가 나타납니다.
5. Advanced **Settings**를 클릭하면 ***Advanced Settings 페이지***가 나타납니다.
6. Transport/*Network Layer* **Preprocessor** 영역에서 *Inline Normalization 옵션을* 찾습니다.
7. 이 기능을 **활성화하려면** Enabled 라디오 버튼을 선택합니다.



인라인 표준화를 위해 침입 정책이 구성되면 액세스 제어 정책에서 기본 작업으로 추가해야 합니다 .



그런 다음 액세스 제어 정책을 검사 장치에 적용해야 합니다.

임의의 조합으로 IPv4, IPv6, ICMPv4(Internet Control Message Protocol Version 4), ICMPv6 및 TCP 트래픽을 표준화하도록 인라인 표준화 프리프로세서를 구성할 수 있습니다. 각 프로토콜의 표준화는 해당 프로토콜 표준화가 활성화된 경우 자동으로 발생합니다.

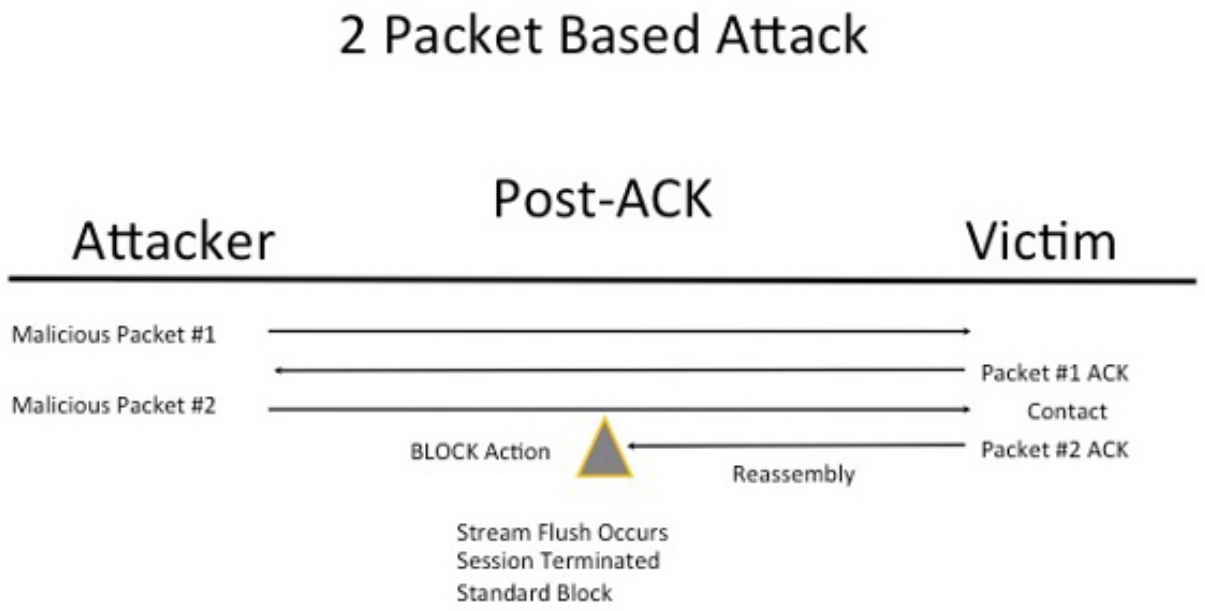
Post-ACK 검사 및 Pre-ACK 검사 활성화

인라인 표준화 프리프로세서를 활성화한 후 Normalize *TCP* Payload(*TCP* 페이로드 표준화) 옵션을 활성화하기 위해 설정을 수정할 수 있습니다. 인라인 표준화 프리프로세서의 이 옵션은 두 가지 서로 다른 검사 모드 간에 전환됩니다.

- 사후 승인(Post-ACK)
- 사전 승인(Pre-ACK)

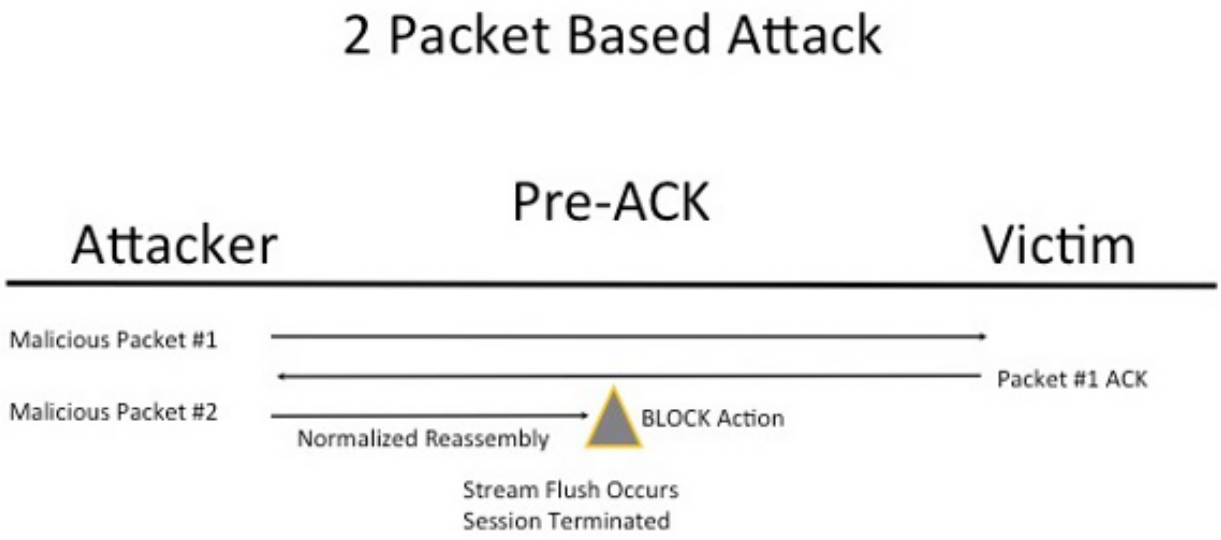
사후 ACK 검사 이해(Normalize TCP/Normalize TCP Payload Disabled)

Post-ACK 검사에서 패킷 스트림 리어셈블리, 플러시(검사 프로세스의 나머지 부분으로 전달), Snort에서의 탐지는 공격을 완료한 패킷에 대한 피해자의 승인(ACK)이 IPS(Intrusion Prevention System)에 수신된 후에 발생합니다. 스트림 플러시가 발생하기 전에 문제의 패킷이 이미 피해자에게 도달했습니다. 따라서 위반 패킷이 피해자에게 도달한 후 알림/드롭이 발생합니다. 이 작업은 문제의 패킷에 대한 피해자의 ACK가 IPS에 도달할 때 발생합니다.



Pre-ACK 검사 이해(Normalize TCP/Normalize TCP Payload Enabled)

이 기능은 TCP 회피 노력을 최소화하기 위해 패킷 디코딩 직후 및 기타 Snort 기능이 처리되기 전에 트래픽을 표준화합니다. 이렇게 하면 IPS에 도달하는 패킷이 피해자에게 전달되는 패킷과 동일합니다. Snort는 공격이 피해자에게 도달하기 전에 공격을 완료한 패킷의 트래픽을 삭제합니다.



Normalize *TCP를 활성화하면* 다음 조건과 일치하는 트래픽도 삭제됩니다.

- 이전에 삭제된 패킷의 복사본을 재전송했습니다.
- 이전에 삭제된 세션을 계속하려는 트래픽
- 다음 TCP 스트림 프리프로세서 규칙 중 하나와 일치하는 트래픽:

  129:1129:3129:4129:6129:8129:11129:14~129:19

  참고: 표준화 프리프로세서에 의해 삭제된 TCP 스트림 규칙에 대한 알림을 활성화하려면 TCP 스트림 컨피그레이션에서 *Stateful Inspection Anomalies* 기능을 활성화해야 합니다.

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.