FTD의 Snort3에서 맞춤형 로컬 Snort 규칙 구성

목차

소개

이 문서에서는 FTD(Firewall Threat Defense)의 Snort3에서 사용자 지정 로컬 Snort 규칙을 구성하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Firepower 관리 센터)
- 방화벽 위협 방어(FTD)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

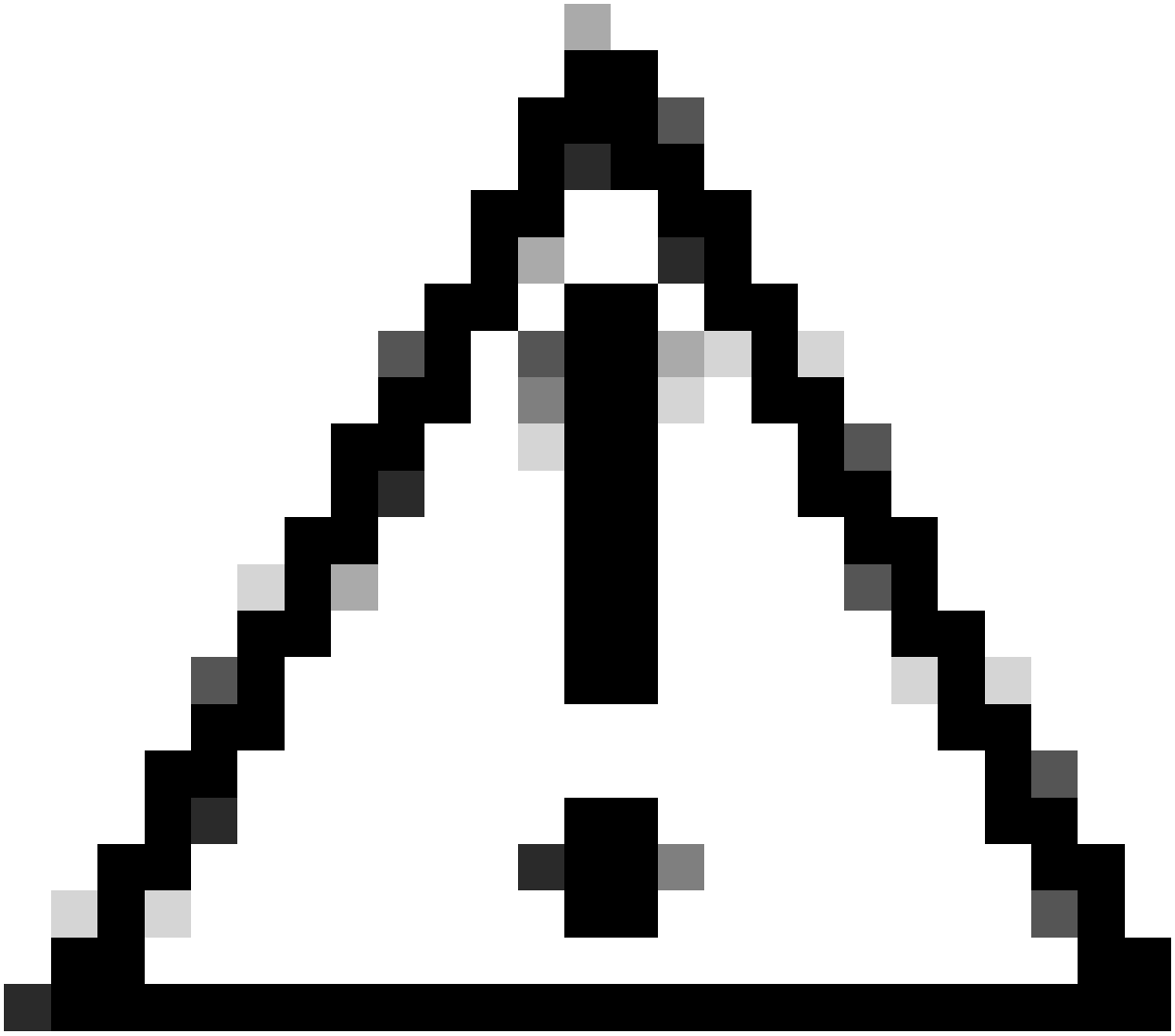
- firepower Cisco Domain Management Center for VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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

Management Center를 통한 위협 방어의 Snort 3 지원은 버전 7.0부터 시작합니다. 버전 7.0 이상의 새로운 및 리이미징된 디바이스의 경우 Snort 3이 기본 검사 엔진입니다.

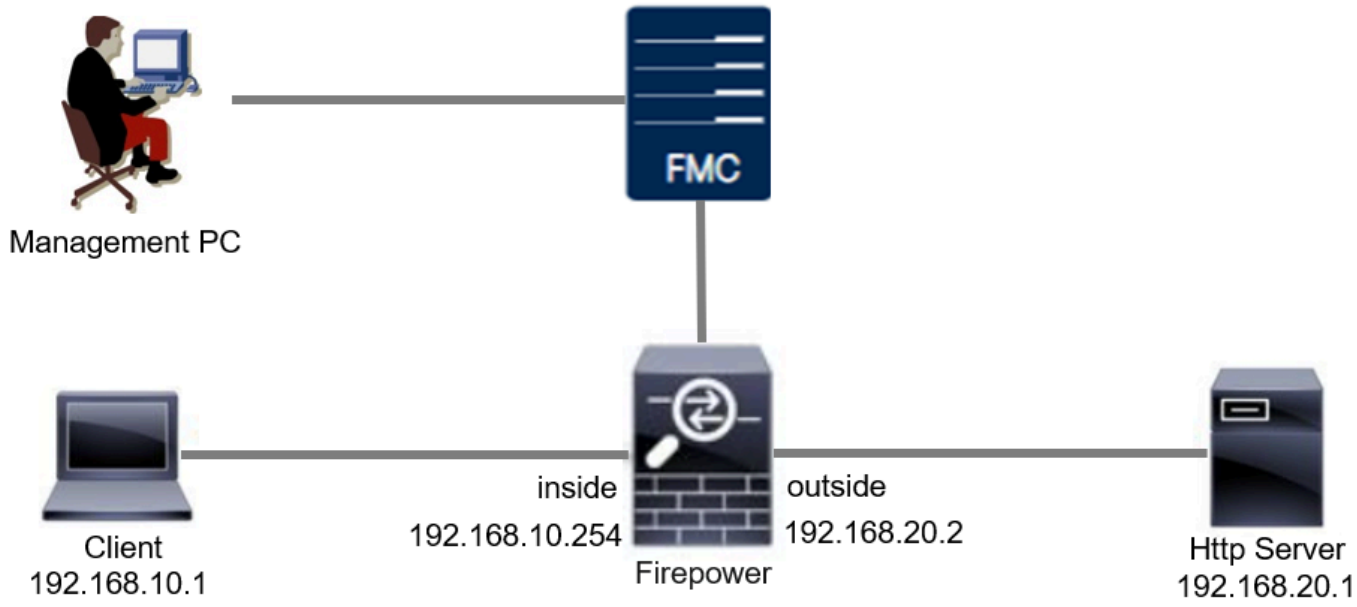
이 문서에서는 Snort 3에 대한 Snort 규칙을 사용자 지정하는 방법의 예와 실제 검증 예를 제공합니다. 특히, 특정 문자열(사용자 이름)을 포함하는 HTTP 패킷을 삭제하기 위해 사용자 지정된 Snort 규칙으로 침입 정책을 구성하고 확인하는 방법을 소개합니다.



주의: 맞춤형 로컬 Snort 규칙을 생성하고 이에 대한 지원을 제공하는 것은 TAC 지원 범위를 벗어납니다. 따라서 이 문서는 참조용으로만 사용할 수 있으며, 이러한 사용자 지정 규칙을 자신의 재량과 책임하에 만들고 관리해 줄 것을 요청합니다.

네트워크 다이어그램

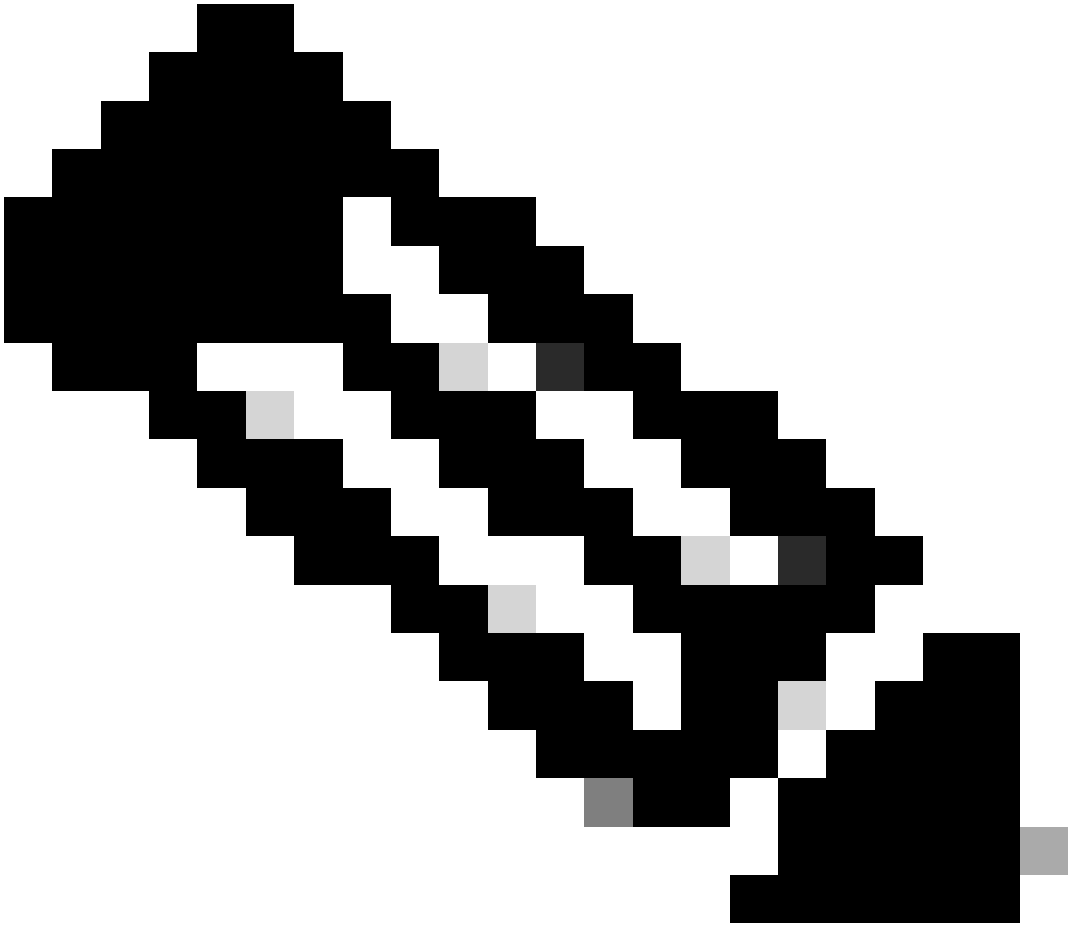
이 문서에서는 이 다이어그램에서 Snort3의 Custom Local Snort Rule에 대한 컨피그레이션 및 확인을 소개합니다.



네트워크 다이어그램

설정

특정 문자열(사용자 이름)을 포함하는 HTTP 응답 패킷을 탐지하고 삭제하기 위한 Custom Local Snort Rule의 컨피그레이션입니다.

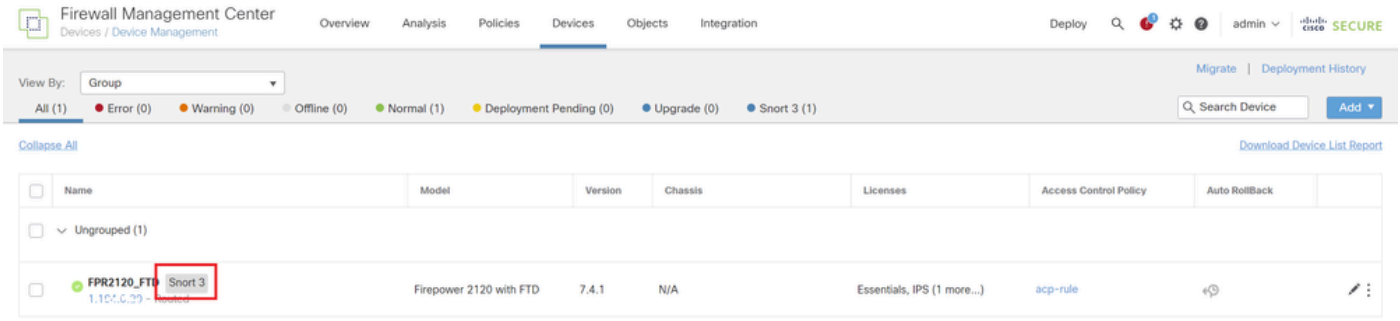


참고: 현재로서는 FMC GUI의 Snort 3 All Rules 페이지에서 Custom Local Snort 규칙을 추가할 수 없습니다. 이 문서에 소개된 방법을 사용해야 합니다.

방법 1. Snort 2에서 Snort 3으로 가져오기

1단계. Snort 버전 확인

FMC에서 Devices>Device Management로 이동하고 Device 탭을 클릭합니다. snort 버전이 Snort3인지 확인합니다.



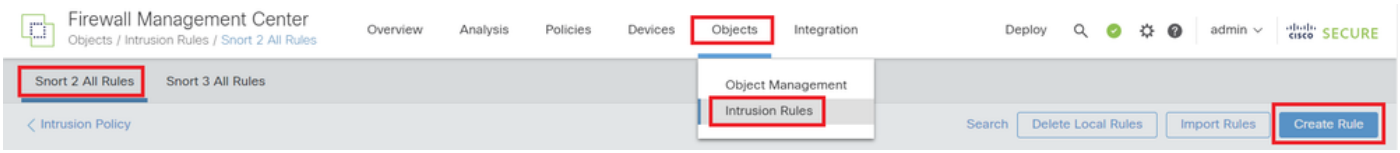
Snort 버전

2단계. Snort 2에서 사용자 지정 로컬 Snort 규칙 생성 또는 편집

Objects(개체) > Intrusion Rules(침입 규칙) > Snort 2 All Rules on FMC(FMC에서 Snort 2 모든 규칙)로 이동합니다. Create Rules(규칙 생성) 버튼을 클릭하여 사용자 지정 로컬 Snort 규칙을 추가하거나 Objects(개체) > Intrusion Rules(침입 규칙) > Snort 2 All Rules(Snort 2 모든 규칙) > Local Rules on FMC(FMC의 로컬 규칙)로 이동하고 Edit(편집) 버튼을 클릭하여 기존 사용자 지정 로컬 Snort 규칙을 편집합니다.

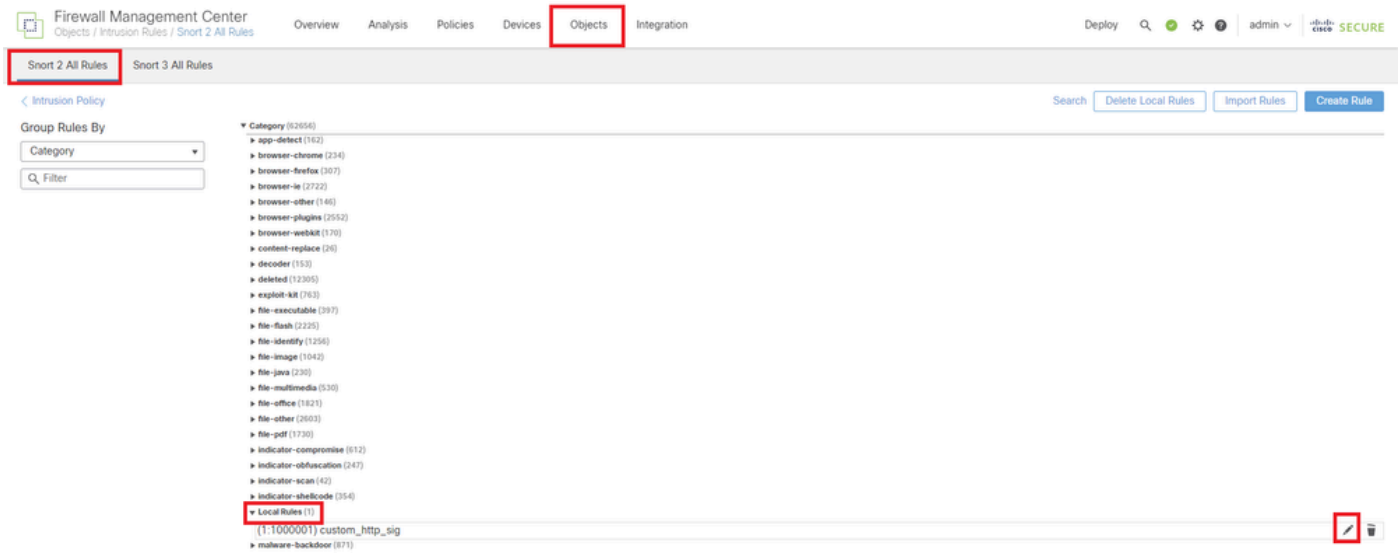
Snort 2에서 사용자 지정 로컬 Snort 규칙을 생성하는 방법에 대한 지침은 FTD의 Snort2에서 사용자 지정 로컬 Snort 규칙 구성을 참조하십시오.

이미지에 표시된 대로 새 사용자 지정 로컬 Snort 규칙을 추가합니다.



새 사용자 지정 규칙 추가

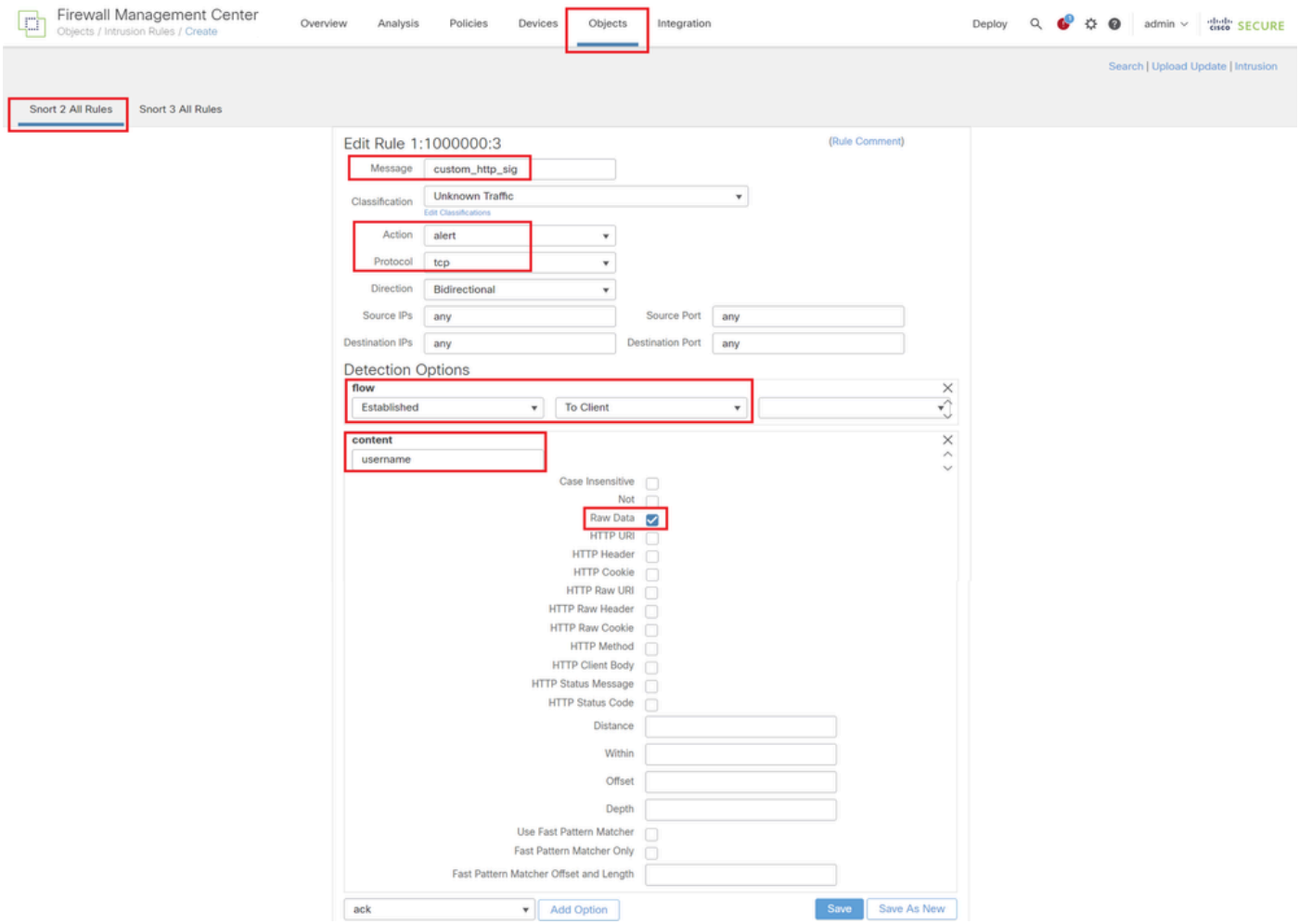
이미지에 표시된 대로 기존 사용자 지정 로컬 Snort 규칙을 수정합니다. 이 예에서는 기존 사용자 지정 규칙을 수정합니다.



기존 사용자 지정 규칙 편집

특정 문자열(사용자 이름)을 포함하는 HTTP 패킷을 탐지하려면 서명 정보를 입력합니다.

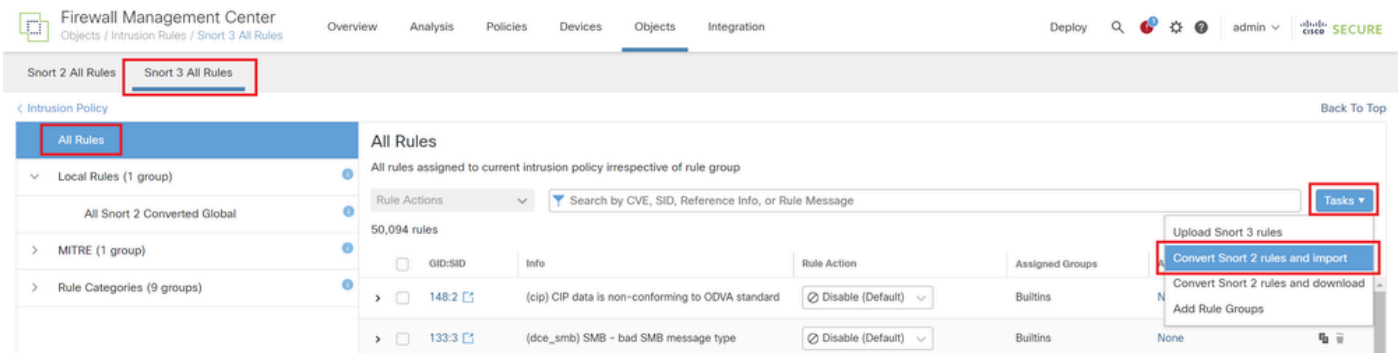
- 메시지: custom_http_sig
- 작업: 경고
- 프로토콜: tcp
- flow: Established, To 클라이언트
- content : 사용자 이름(원시 데이터)



규칙에 필요한 정보 입력

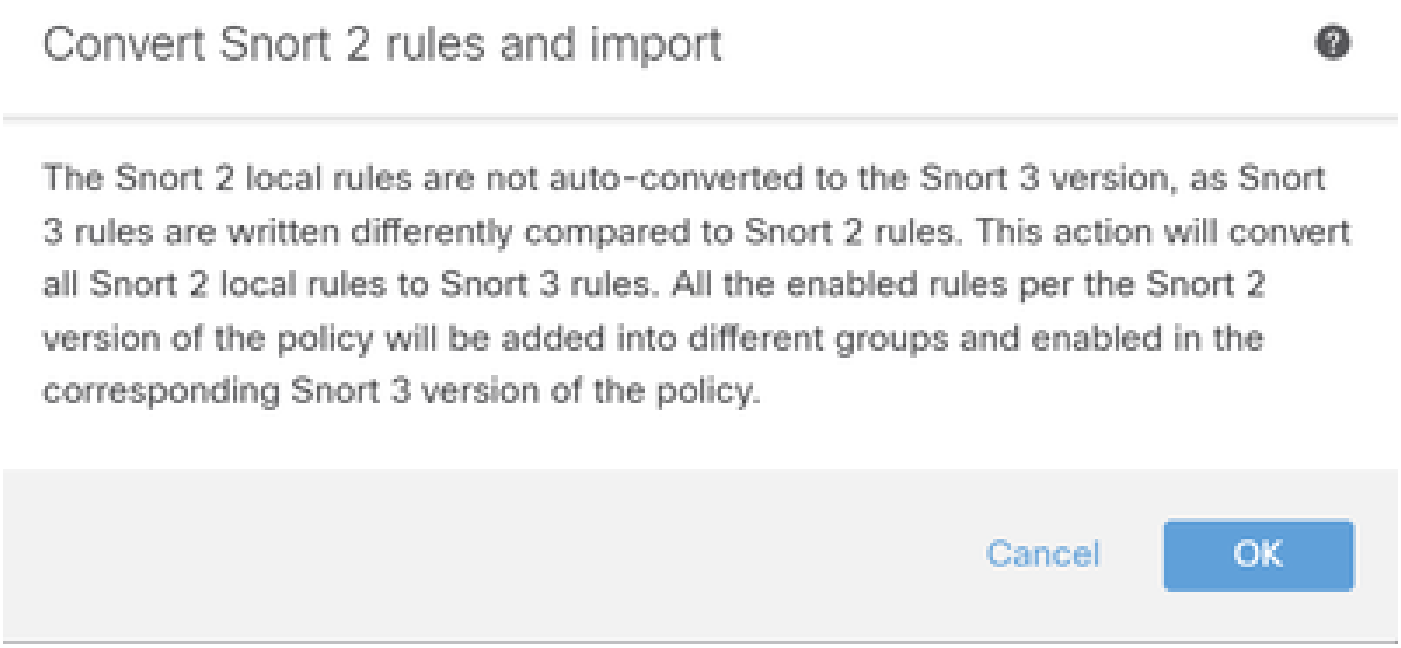
3단계. Snort 2에서 Snort 3으로 맞춤형 로컬 Snort 규칙 가져오기

Objects(개체) > Intrusion Rules(침입 규칙) > Snort 3 All Rules(Snort 3 모든 규칙) > All Rules on FMC(FMC의 모든 규칙)로 이동하고 Convert 2 rules(Snort 2 규칙 변환) 및 Import from Tasks(작업에서 가져오기) 풀다운 목록으로 이동합니다.



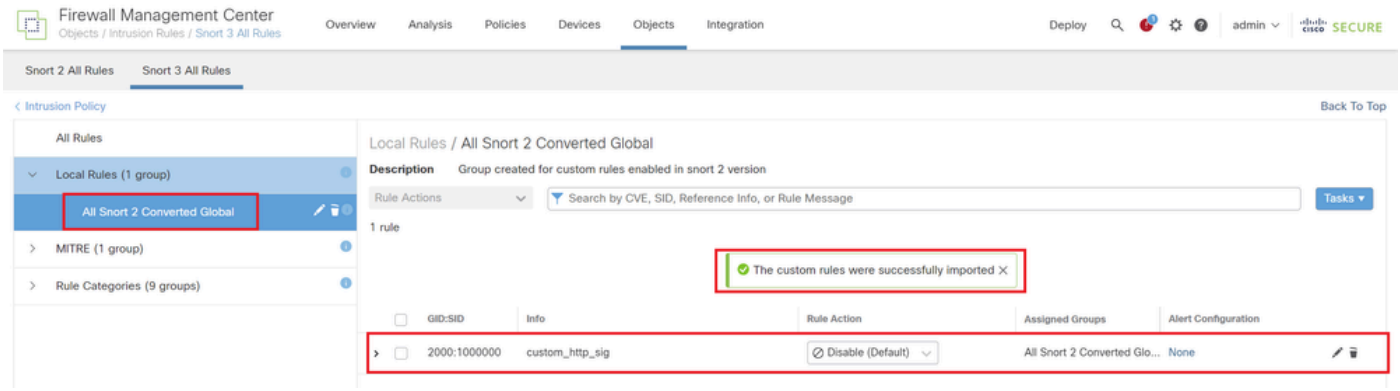
Snort 3에 사용자 지정 규칙 가져오기

경고 메시지를 확인하고 확인을 클릭합니다.



경고 메시지

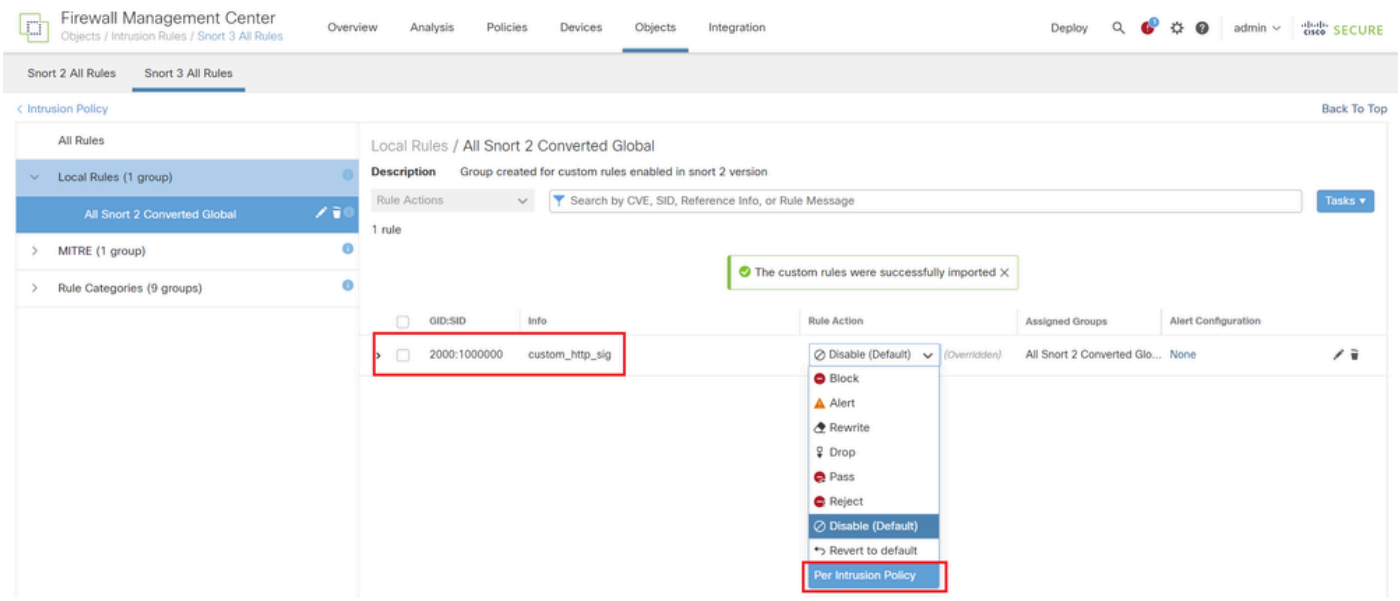
Objects(개체) > Intrusion Rules(침입 규칙) > Snort 3 All Rules on FMC(FMC의 모든 규칙)로 이동하고 All Snort 2 Converted Global(모든 Snort 2 변환된 전역)을 클릭하여 가져온 Custom Local Snort 규칙을 확인합니다.



가져온 사용자 지정 규칙 확인

4단계. 규칙 작업 변경

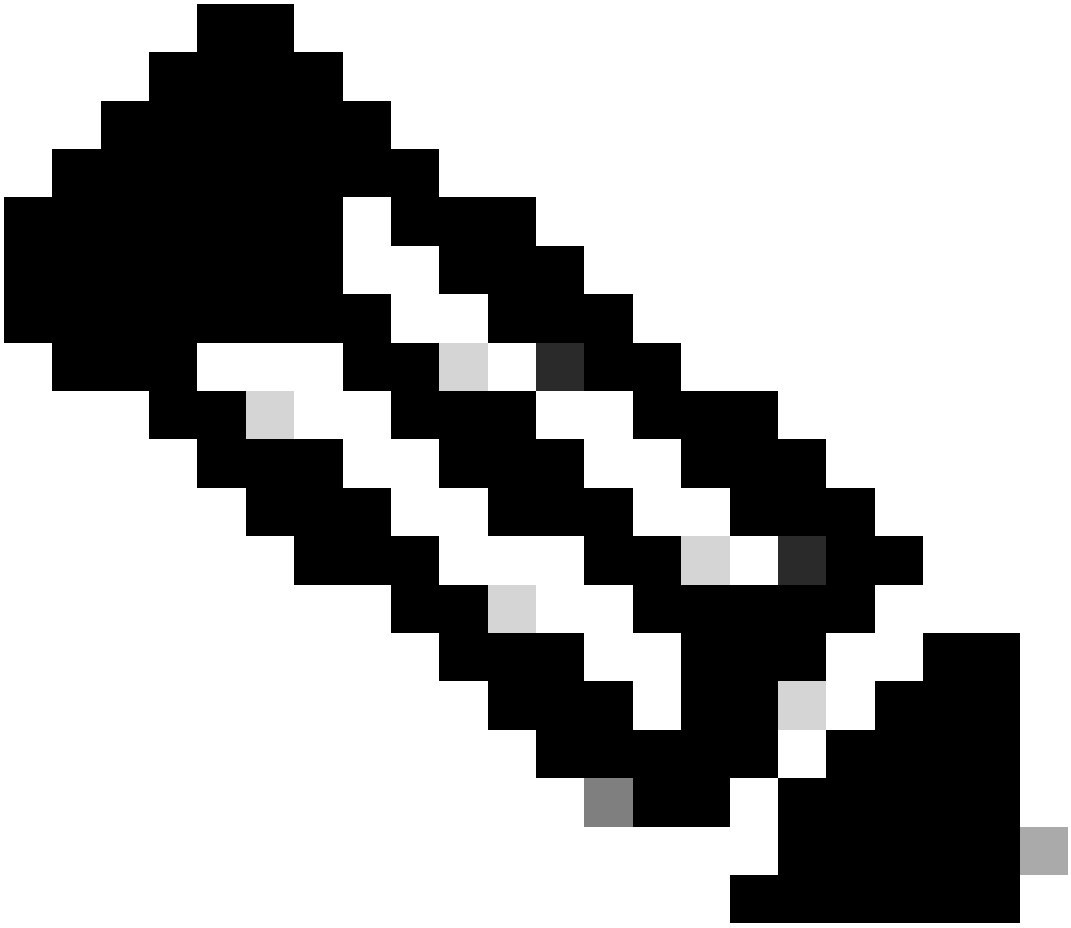
대상 사용자 지정 규칙의 Rule Action에 따라 Per Intrusion Policy를 클릭합니다.



규칙 작업 변경

Edit Rule Action(규칙 작업 수정) 화면에서 Policy and Rule Action(정책 및 규칙 작업)에 대한 정보를 입력합니다.

- 정책: snort_test
- 규칙 작업: 차단



참고: 규칙 작업은 다음과 같습니다.

Block(차단) - 이벤트를 생성하고, 현재 일치하는 패킷 및 이 연결의 모든 후속 패킷을 차단합니다.

Alert(경고) - 일치하는 패킷에 대한 이벤트만 생성하고 패킷 또는 연결은 삭제하지 않습니다.

Rewrite(재작성) - 규칙의 replace(교체) 옵션을 기반으로 이벤트를 생성하고 패킷 내용을 덮어씁니다.

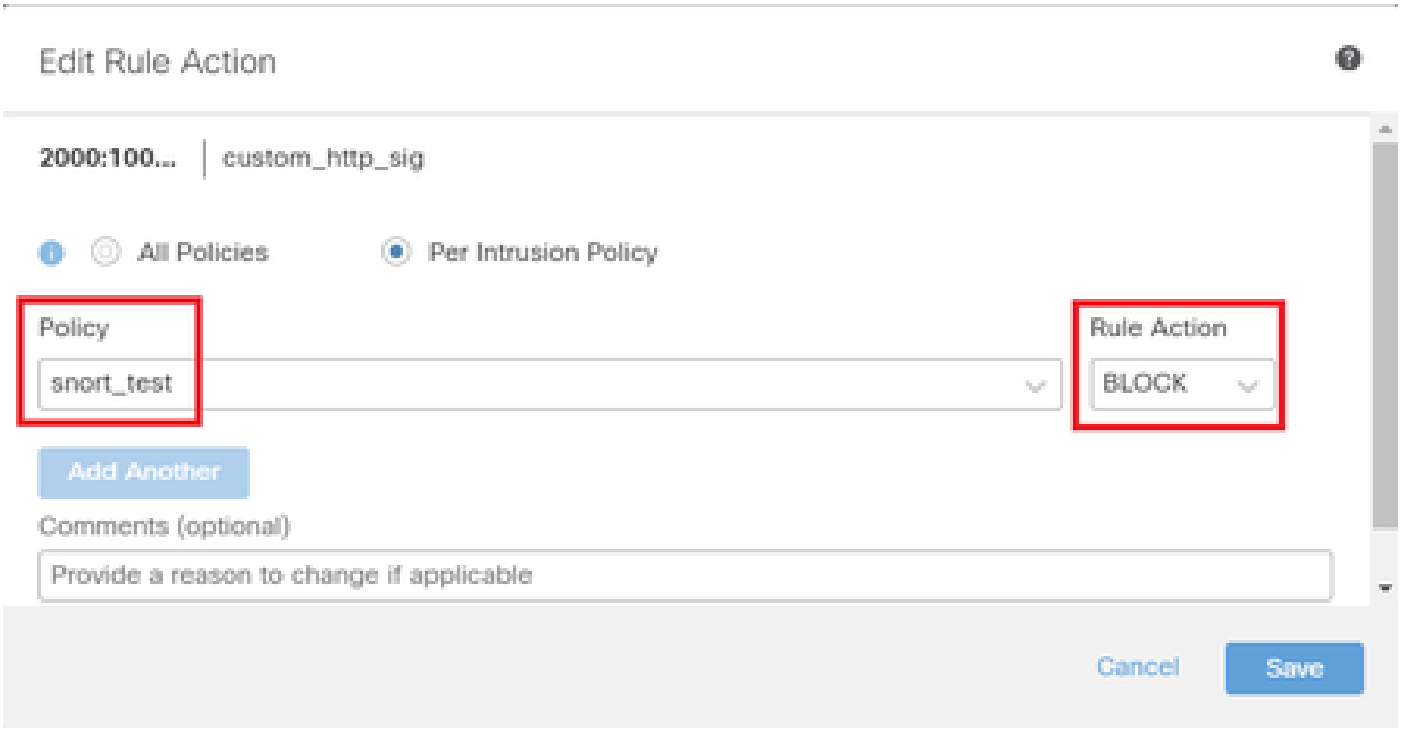
Pass(통과) - 이벤트가 생성되지 않으므로 후속 Snort 규칙에 의한 추가 평가 없이 패킷이 통과할 수 있습니다.

Drop(삭제) - 이벤트를 생성하고, 일치하는 패킷을 삭제하며, 이 연결에서 추가 트래픽을 차단하지 않습니다.

Reject(거부) - 이벤트를 생성하고, 일치하는 패킷을 삭제하고, 이 연결의 추가 트래픽을 차단하고, 소스 및 대상 호스트에 대한 TCP 프로토콜인 경우 TCP 재설정을 전송합니다.

Disable(비활성화) - 이 규칙에 대해 트래픽을 매칭하지 않습니다. 이벤트가 생성되지 않습니다.

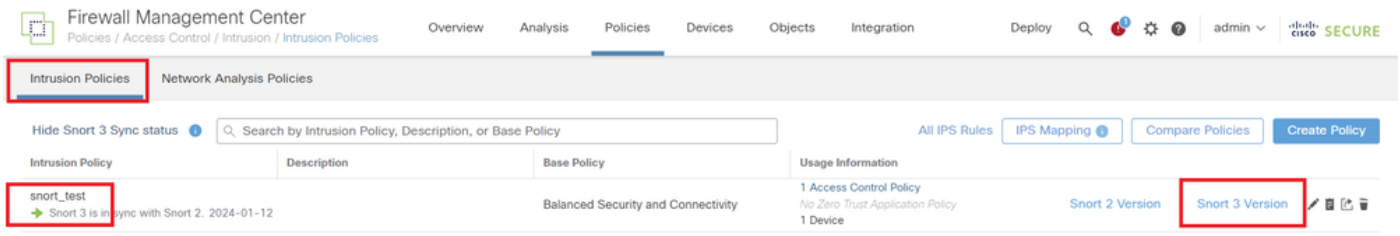
Default(기본값) - 시스템 기본 작업으로 돌아갑니다.



규칙 작업 편집

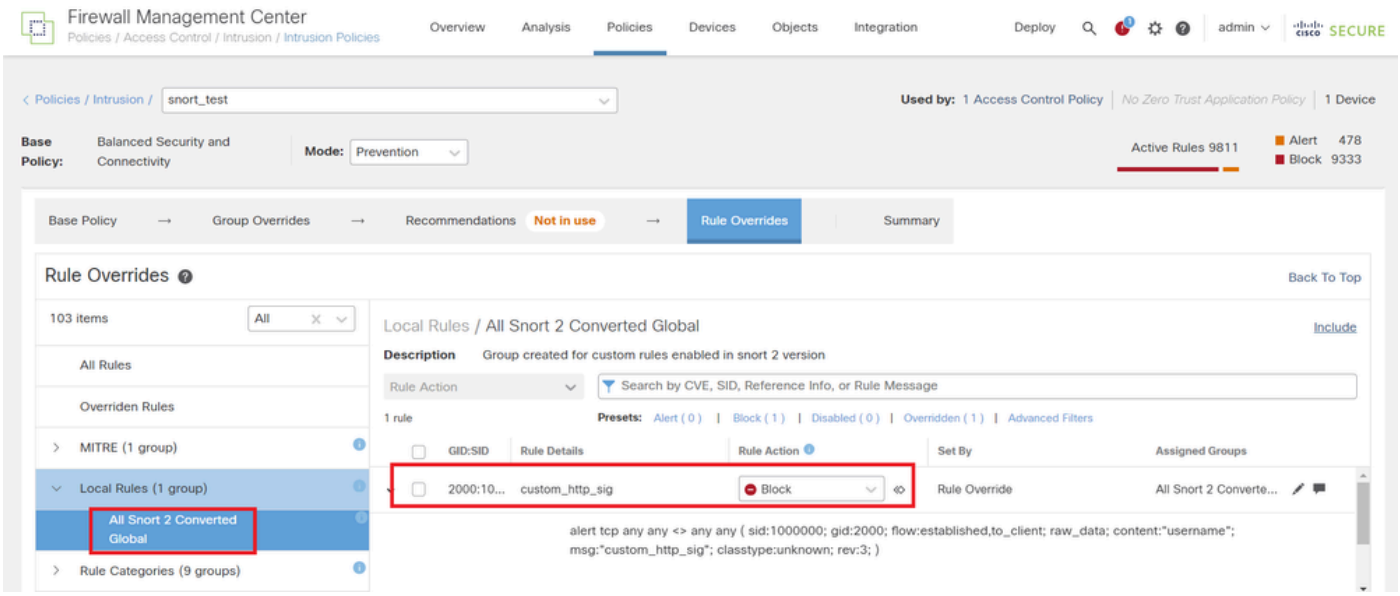
5단계. 가져온 사용자 지정 로컬 Snort 규칙 확인

Policies(정책) > Intrusion Policies on FMC(FMC의 침입 정책)로 이동하고 행에서 대상 침입 정책에 해당하는 Snort 3 Version(Snort 3 버전)을 클릭합니다.



가져온 사용자 지정 규칙 확인

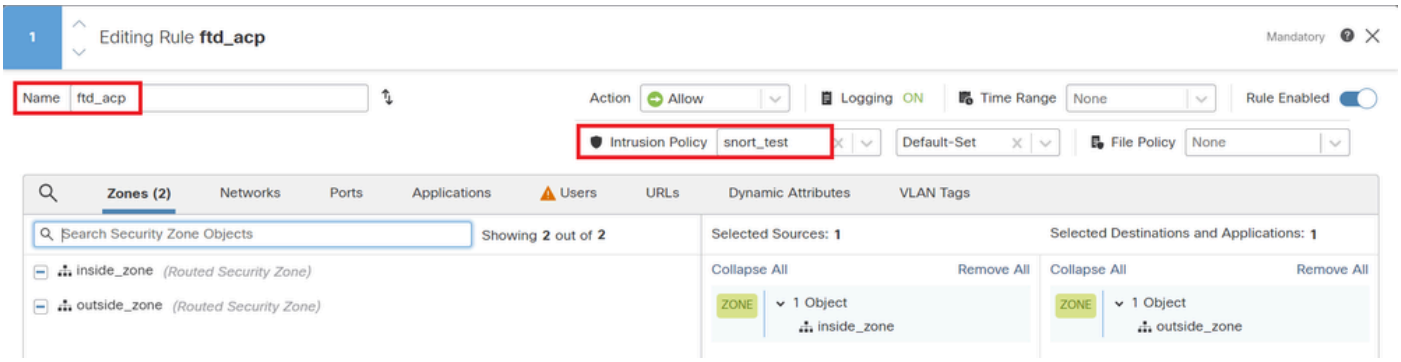
Local Rules(로컬 규칙) > All Snort 2 Converted Global(All Snort 2 변환된 전역)을 클릭하여 맞춤형 로컬 Snort 규칙의 세부사항을 확인합니다.



가져온 사용자 지정 규칙 확인

6단계. 침입 정책을 ACP(액세스 제어 정책) 규칙과 연결

Policies>Access Controlon FMC로 이동하여 침입 정책을 ACP와 연결합니다.



ACP 규칙과 연결

7단계. 변경 사항 배포

FTD에 변경 사항을 구축합니다.

변경 사항 배포

방법 2. 로컬 파일 업로드

1단계. Snort 버전 확인

방법 1의 단계 1과 같습니다.

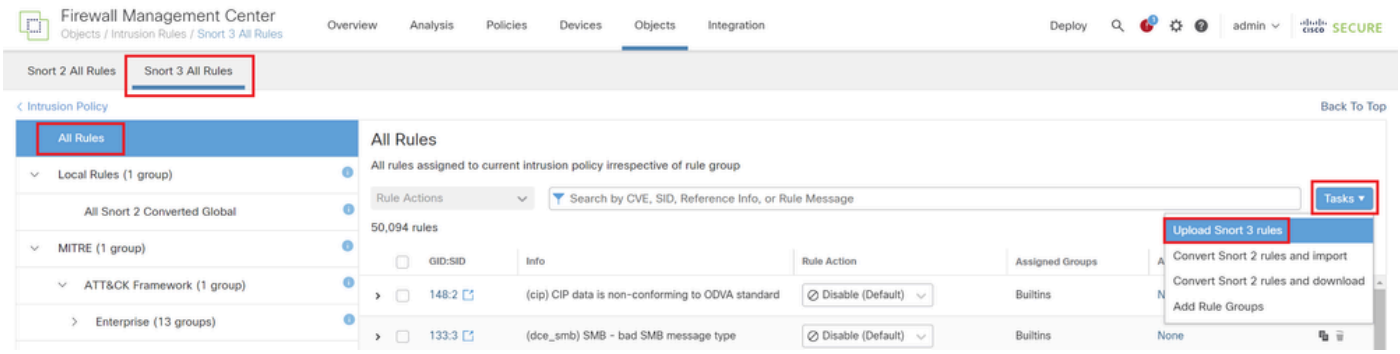
2단계. 사용자 지정 로컬 Snort 규칙 생성

수동으로 사용자 지정 로컬 Snort 규칙을 생성하고 custom-rules.txt라는 로컬 파일에 저장합니다.

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

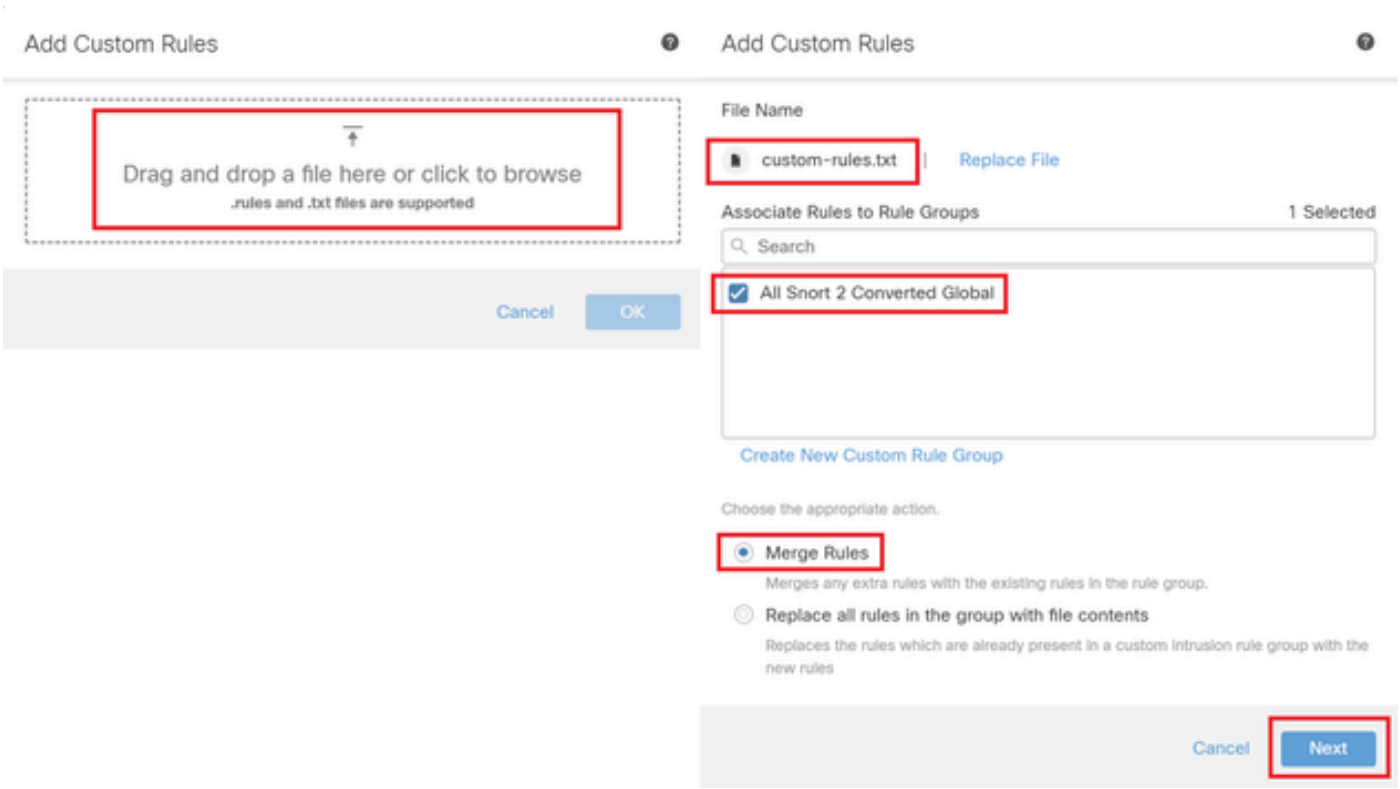
3단계. 사용자 지정 로컬 Snort 규칙 업로드

Objects(개체) > Intrusion Rules(침입 규칙) > Snort 3 All Rules(Snort 3 모든 규칙) > All Rules on FMC(FMC의 모든 규칙)로 이동하여 Upload Snort 3 rules from Tasks(작업) 풀다운 목록에서 Upload Snort 3 rules(Snort 3 규칙 업로드)를 클릭합니다.



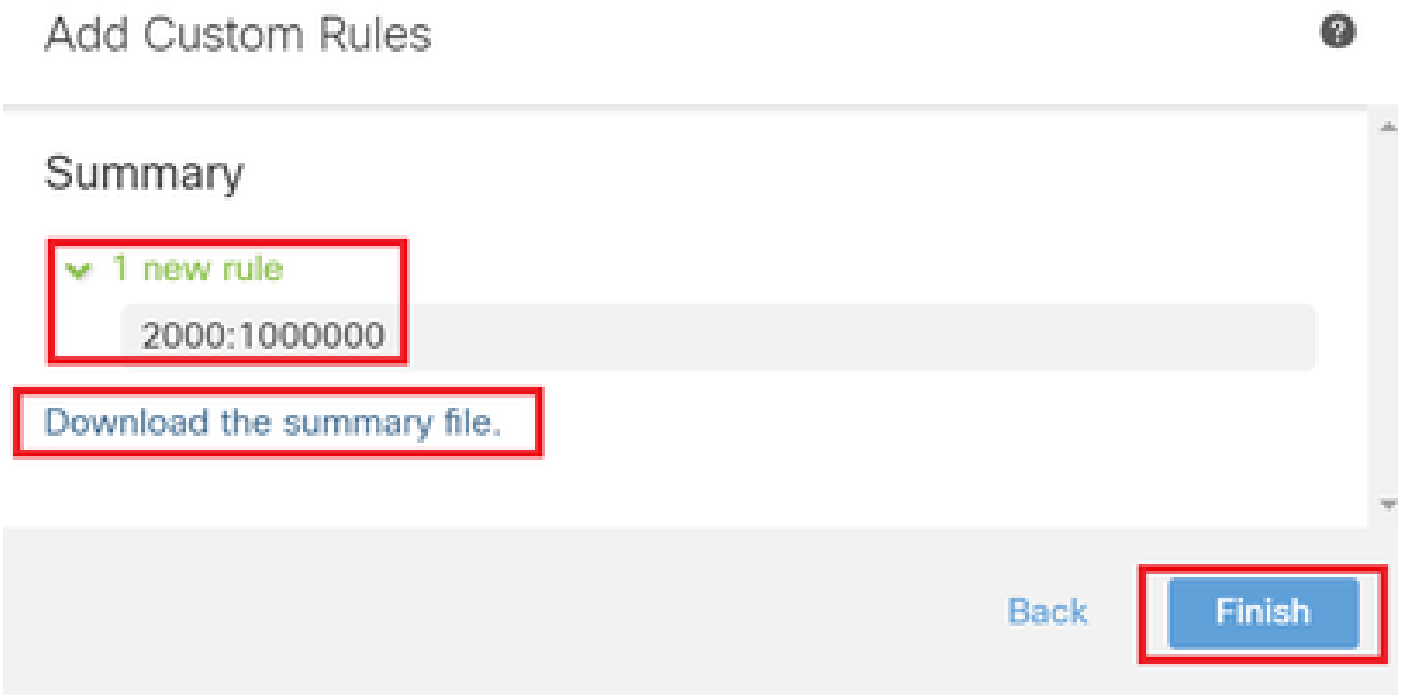
사용자 지정 규칙 업로드

Add Custom Rules(사용자 지정 규칙 추가) 화면에서 로컬 custom-rules.txt 파일을 끌어서 놓고 규칙 그룹과 적절한 작업(이 예에서는 규칙 병합)을 선택한 다음 Next(다음) 버튼을 클릭합니다.



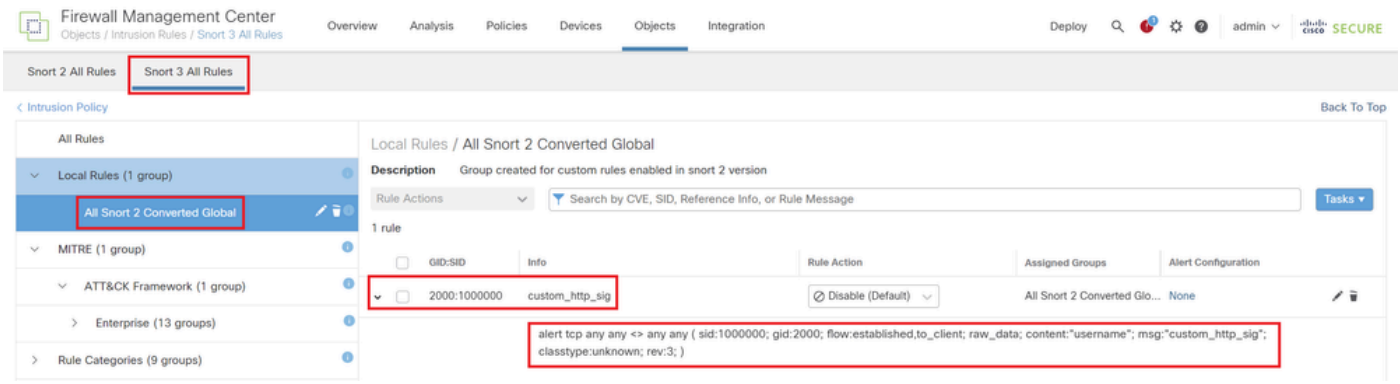
사용자 지정 규칙 추가

로컬 규칙 파일이 성공적으로 업로드되었는지 확인합니다.



업로드 결과 확인

Objects(개체) > Intrusion Rules(침입 규칙) > Snort 3 All Rules on FMC(FMC의 모든 규칙)로 이동하고 All Snort 2 Converted Global(모든 Snort 2 변환된 전역)을 클릭하여 업로드된 Custom Local Snort 규칙을 확인합니다.



사용자 지정 규칙의 세부 정보

4단계. 규칙 작업 변경

방법 1의 단계 4와 같습니다.

5단계. 업로드된 사용자 지정 로컬 Snort 규칙 확인

방법 1의 단계 5와 같습니다.

6단계. 침입 정책을 ACP(액세스 제어 정책) 규칙과 연결

방법 1의 단계 6과 같습니다.

7단계. 변경 사항 배포

방법 1의 단계 7과 같습니다.

다음을 확인합니다.

1단계. HTTP 서버에서 파일 내용 설정

HTTP 서버 측의 test.txt 파일 내용을 username으로 설정합니다.

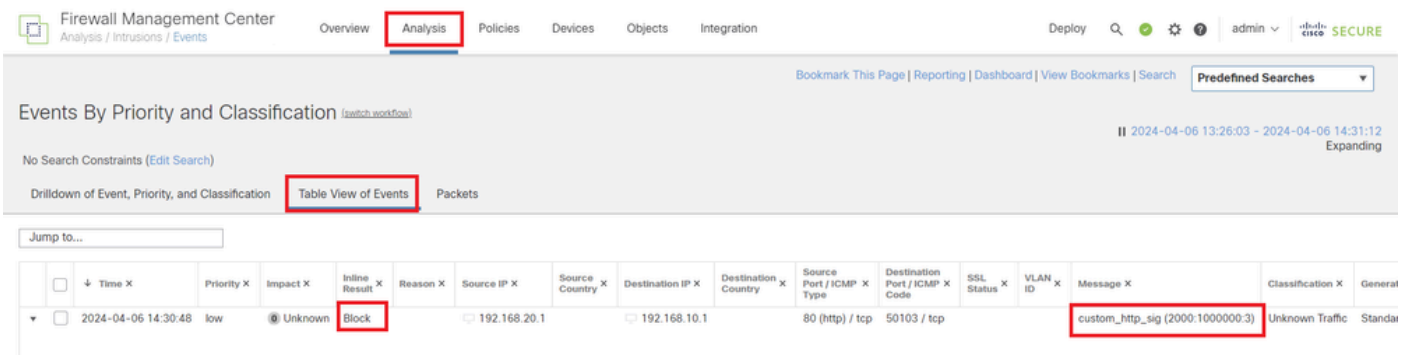
2단계. 초기 HTTP 요청

클라이언트(192.168.10.1)의 브라우저에서 HTTP 서버(192.168.20.1/test.txt)에 액세스하고 HTTP 통신이 차단되었는지 확인합니다.

초기 HTTP 요청

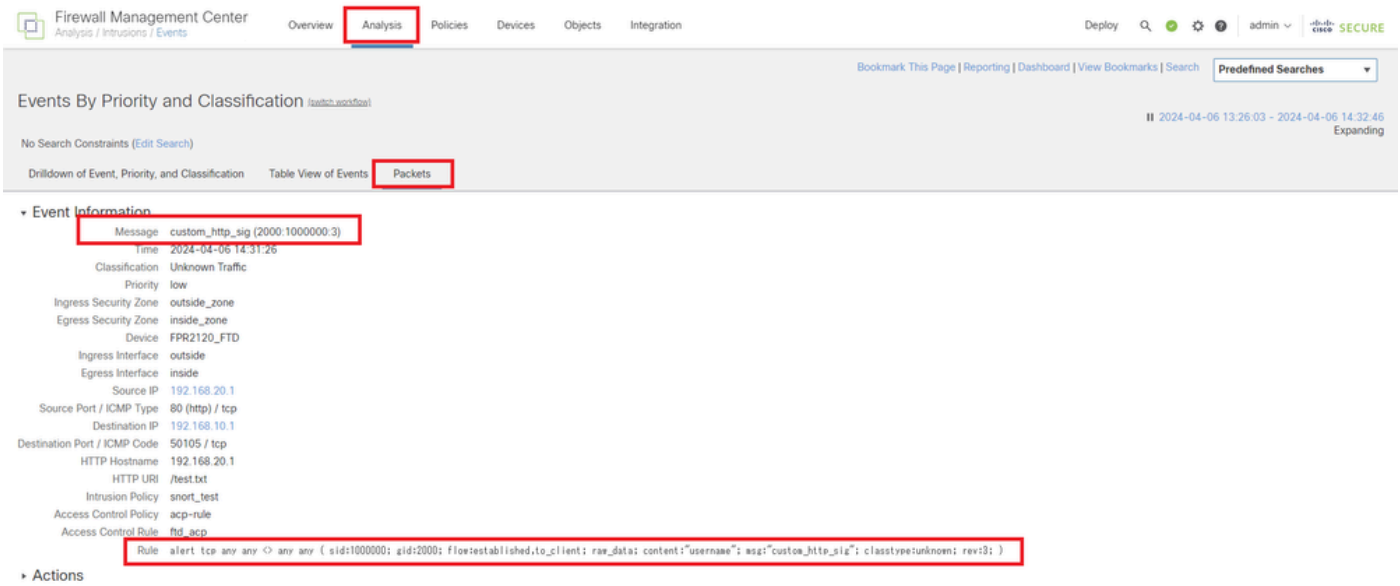
3단계. 침입 이벤트 확인

Analysis>Intrusions>Eventson>FMC로 이동하여 Intrusion Event가 Custom Local Snort 규칙에 의해 생성되었는지 확인합니다.



침입 이벤트

패킷 탭을 클릭하고 침입 이벤트의 세부사항을 확인합니다.



침입 이벤트의 세부사항

FAQ(자주 묻는 질문)

Q: Snort 2 또는 Snort 3 중 어떤 것을 권장합니다.
A: Snort 2에 비해 Snort 3은 처리 속도가 향상되고 새로운 기능이 추가되어 더욱 권장되는 옵션입니다.

Q: FTD 7.0 이전 버전에서 7.0 이상 버전으로 업그레이드하면 Snort 버전이 Snort 3으로 자동 업데이트됩니까?
A: 아닙니다. 검사 엔진은 Snort 2에 그대로 있습니다. 업그레이드 후 Snort 3을 사용하려면 명시적으로 활성화해야 합니다. Snort 2는 향후 릴리스에서 더 이상 사용되지 않을 예정이며, 지금 사용을 중지하는 것이 좋습니다.

Q: Snort 3에서 기존 사용자 지정 규칙을 수정할 수 있습니까?
A: 아니요. 편집할 수 없습니다. 특정 사용자 지정 규칙을 수정하려면 관련 규칙을 삭제하고 다시 생성해야 합니다.

문제 해결

FTD의 동작을 확인하려면 명령을 실행합니다system support trace. 이 예에서는 HTTP 트래픽이 IPS 규칙 (2000:1000000:3)에 의해 차단됩니다.

<#root>

>

system support trace

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
```

```
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '
```

ftd_acp

```
', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1
```

Event

```
:
```

2000:1000000:3

```
, Action
```

block

```
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:
```

ips, block

참조

Cisco Secure Firewall Management Center Snort 3 컨피그레이션 가이드

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.