FTD의 Snort2에서 맞춤형 로컬 Snort 규칙 구성

목차

소개

이 문서에서는 FTD(Firewall Threat Defense)의 Snort2에서 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.

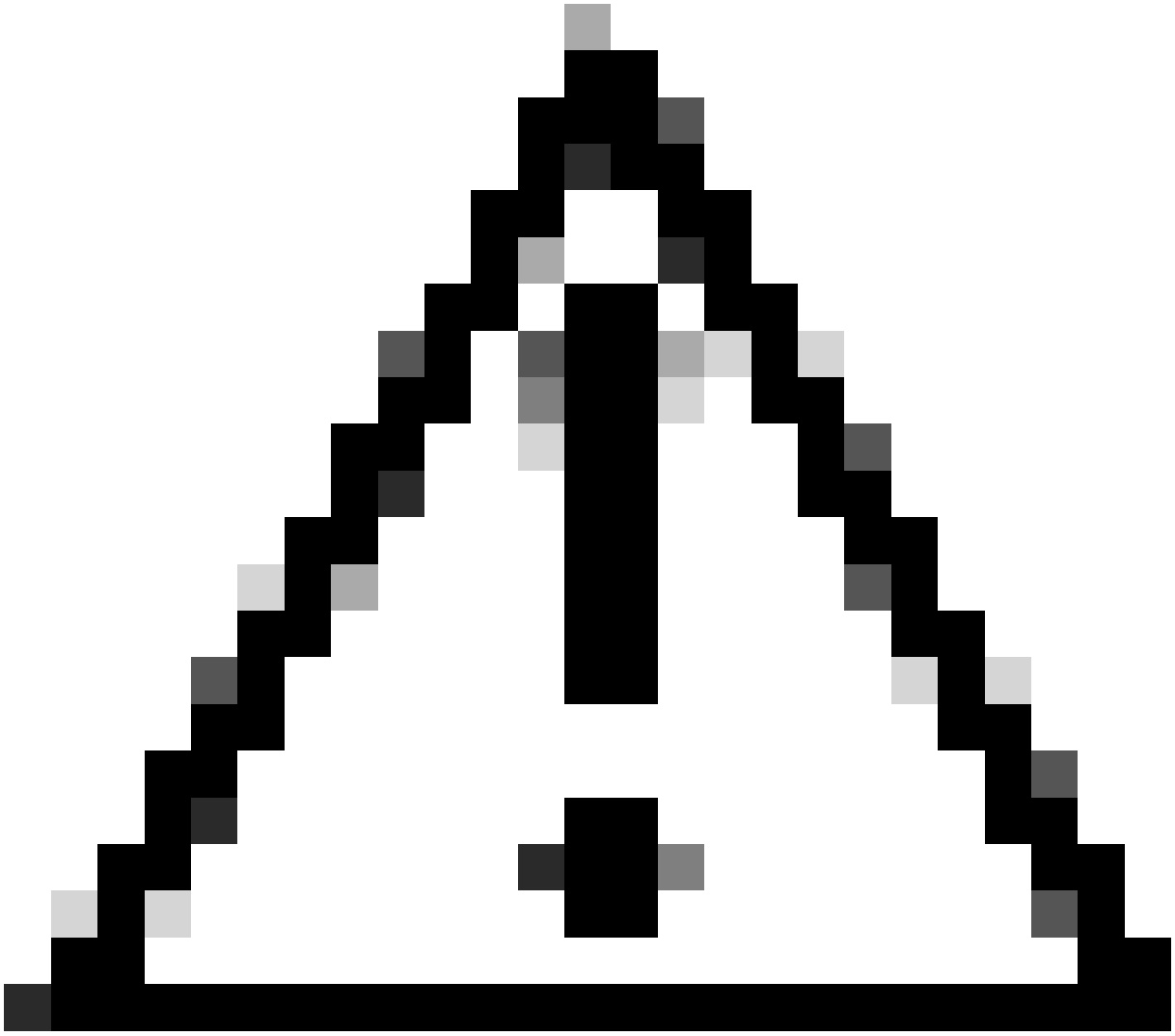
- firepower Cisco Domain Management Center for VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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

Custom Local Snort Rule(맞춤형 로컬 Snort 규칙)은 FTD에 통합된 Snort 침입 탐지 및 방지 시스템 내에서 생성하고 구현할 수 있는 사용자 정의 규칙을 의미합니다. Cisco FTD에서 사용자 지정 로컬 Snort 규칙을 생성할 때 기본적으로 Snort 엔진이 감시할 수 있는 새로운 패턴 또는 조건 집합을 정의합니다. 네트워크 트래픽이 사용자 지정 규칙에 지정된 조건과 일치하면 Snort는 경고 생성 또는 패킷 삭제와 같이 규칙에 정의된 작업을 수행할 수 있습니다. 관리자는 사용자 지정 로컬 Snort 규칙을 사용하여 일반 규칙 집합에서 다루지 않는 특정 위협을 처리합니다.

이 문서에서는 특정 문자열(사용자 이름)을 포함하는 HTTP 응답 패킷을 탐지하고 삭제하도록 설계된 사용자 지정 로컬 Snort 규칙을 구성하고 확인하는 방법을 소개합니다.

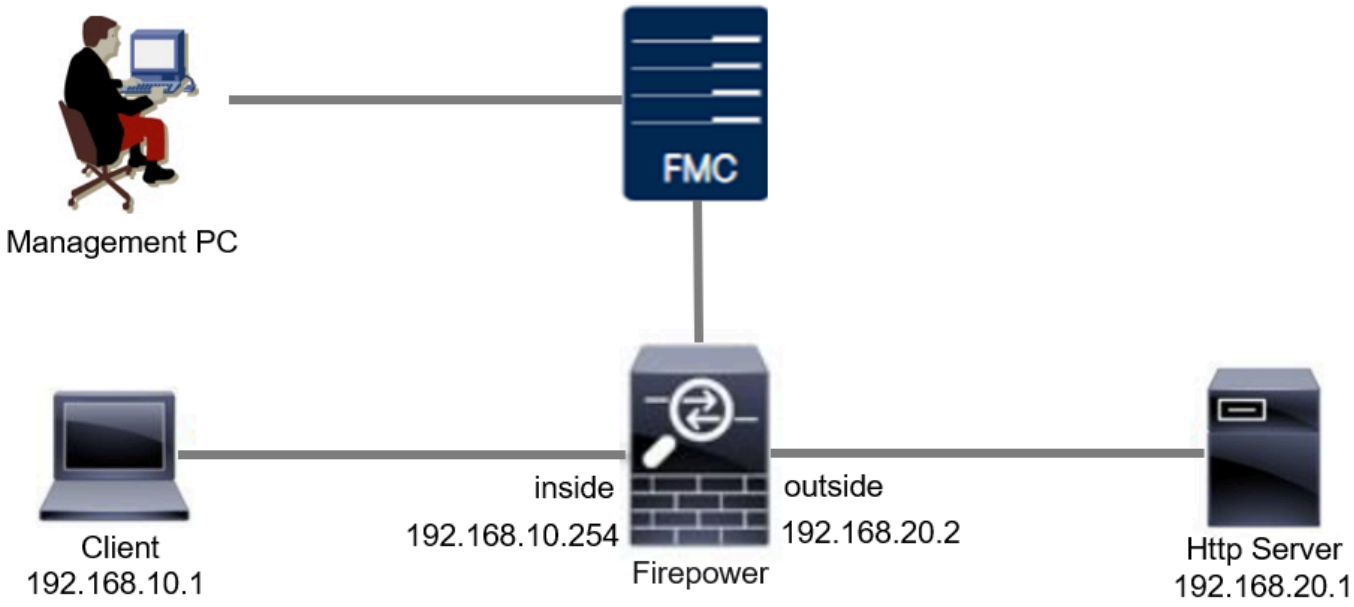


주의: 맞춤형 로컬 Snort 규칙을 생성하고 그에 대한 지원을 제공하는 것은 TAC 지원 범위를 벗어납니다. 따라서 이 문서는 참조용으로만 사용할 수 있으며, 이러한 사용자 지정 규칙을 자신의 재량과 책임하에 만들고 관리해 줄 것을 요청합니다.

구성

네트워크 다이어그램

이 문서에서는 이 다이어그램에서 Snort2의 Custom Local Snort Rule에 대한 컨피그레이션 및 확인을 소개합니다.

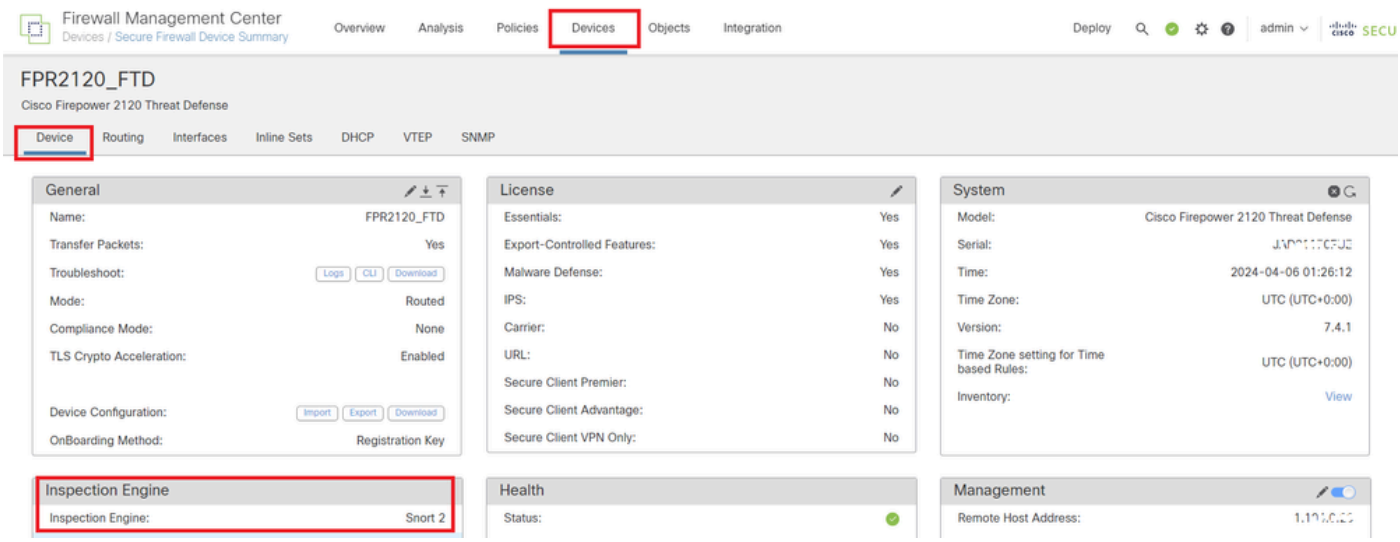


설정

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

1단계. Snort 버전 확인

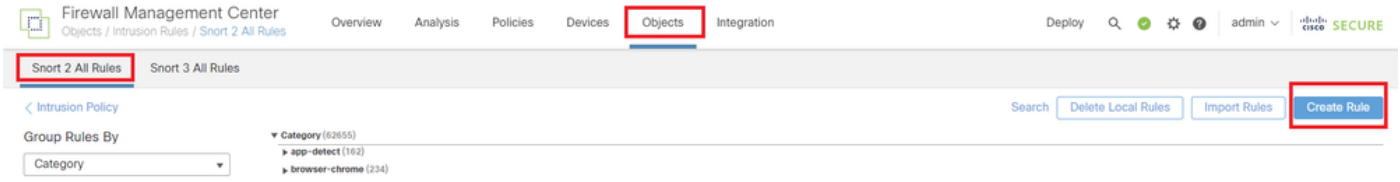
FMC에서 Devices > Device Management로 이동하고 Device 탭을 클릭합니다. snort 버전을 확인하는 것은 Snort2입니다.



Snort 버전

2단계. Snort 2에서 사용자 지정 로컬 Snort 규칙 생성

Objects(개체) > Intrusion Rules(침입 규칙) > Snort 2 All Rules on FMC(FMC에서 모든 규칙 Snort 2로 이동하여 Create Rule(규칙 생성) 버튼을 클릭합니다.

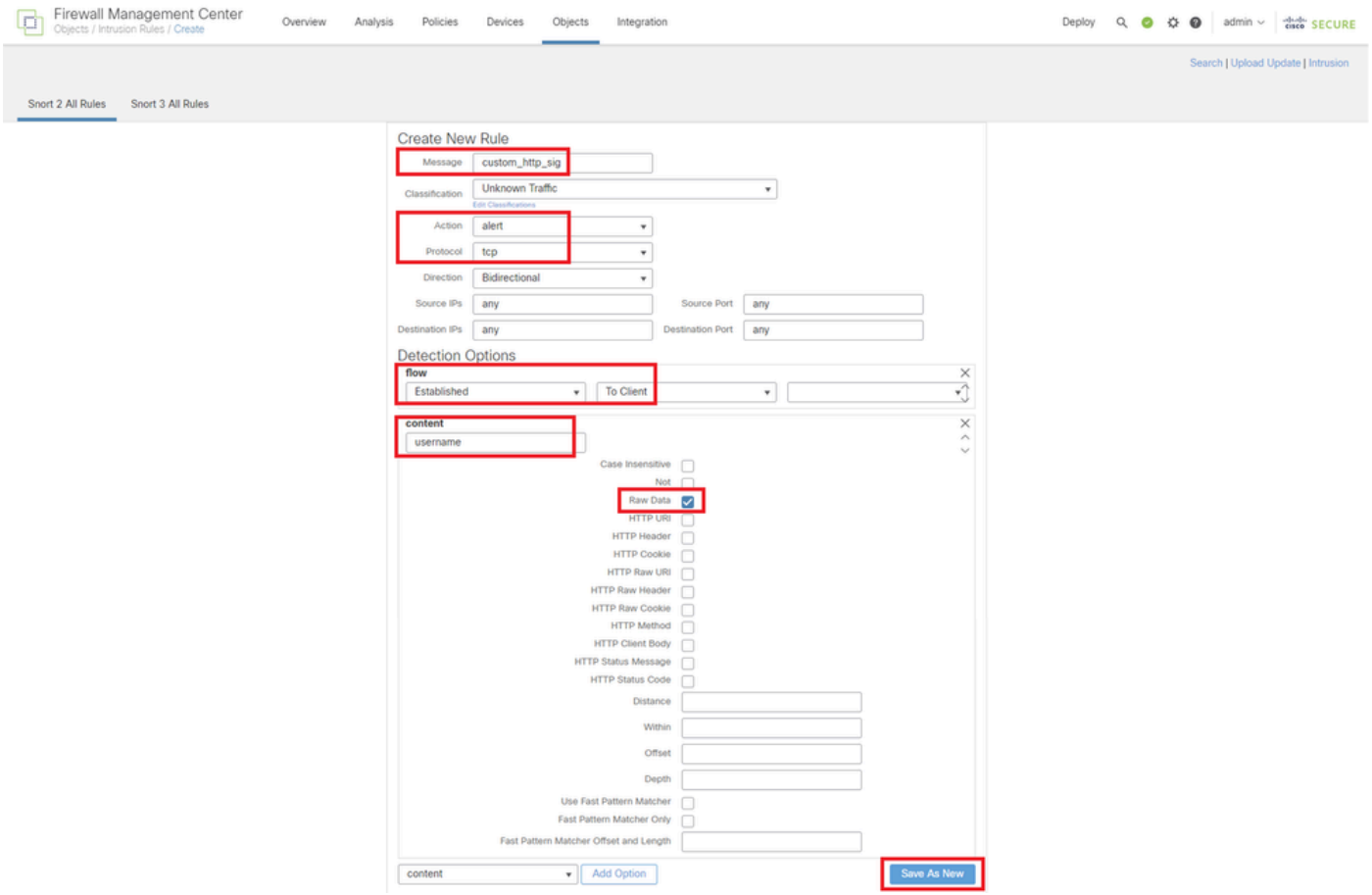


사용자 지정 규칙 만들기

사용자 지정 로컬 Snort 규칙에 필요한 정보를 입력합니다.

- 침입 : custom_http_sig
- 작업: 경고
- 프로토콜: tcp
- flow: Established, To 클라이언트

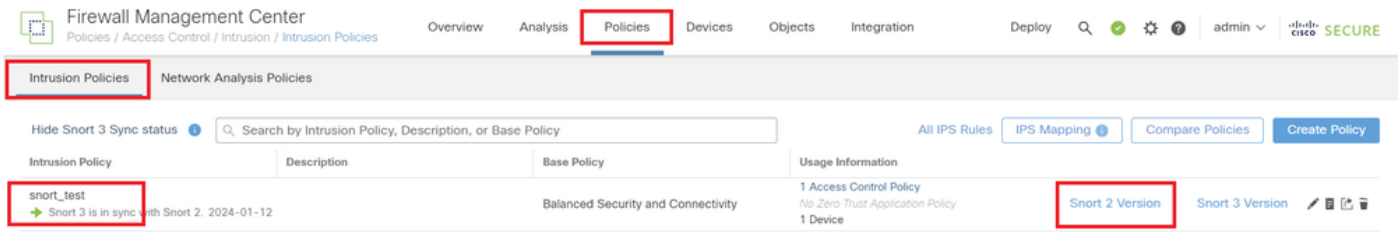
- content : 사용자 이름(원시 데이터)



규칙에 필요한 정보 입력

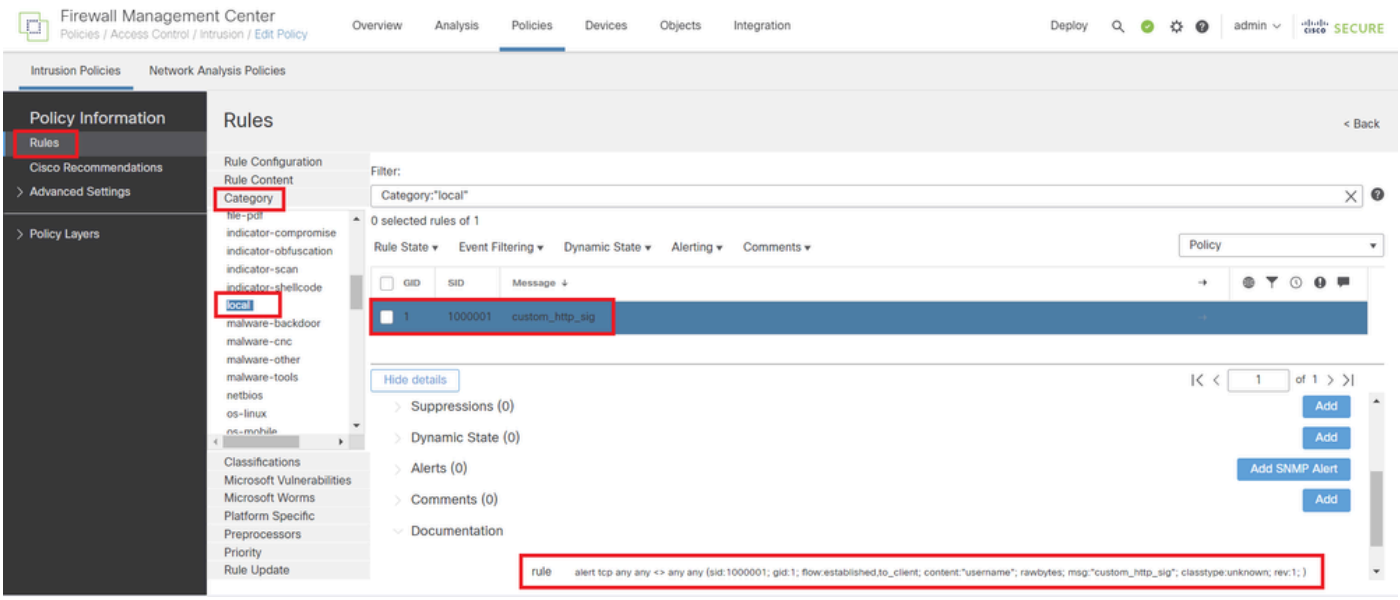
3단계. 사용자 지정 로컬 Snort 규칙 확인

Policies(정책) > Intrusion Policies on FMC(FMC의 침입 정책)로 이동하고 Snort 2 Version(Snort 2 버전) 버튼을 클릭합니다.



사용자 지정 규칙 확인

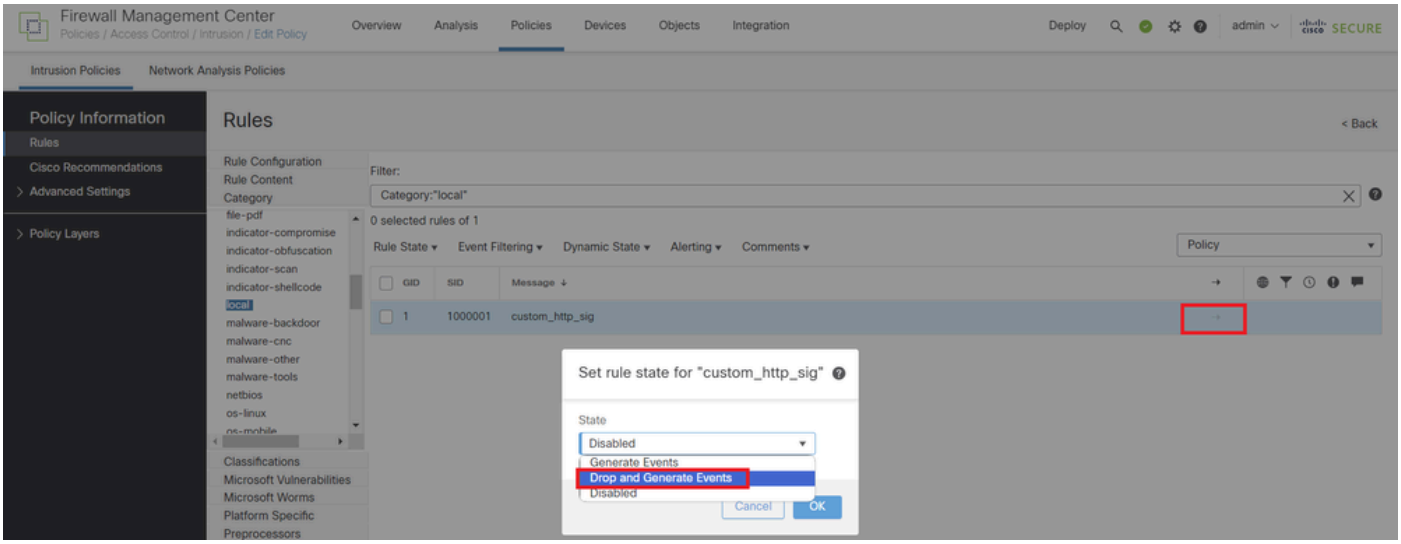
FMC에서 Rules > Category > local로 이동하여 Custom Local Snort Rule의 세부사항을 확인합니다.



사용자 지정 규칙의 세부 정보

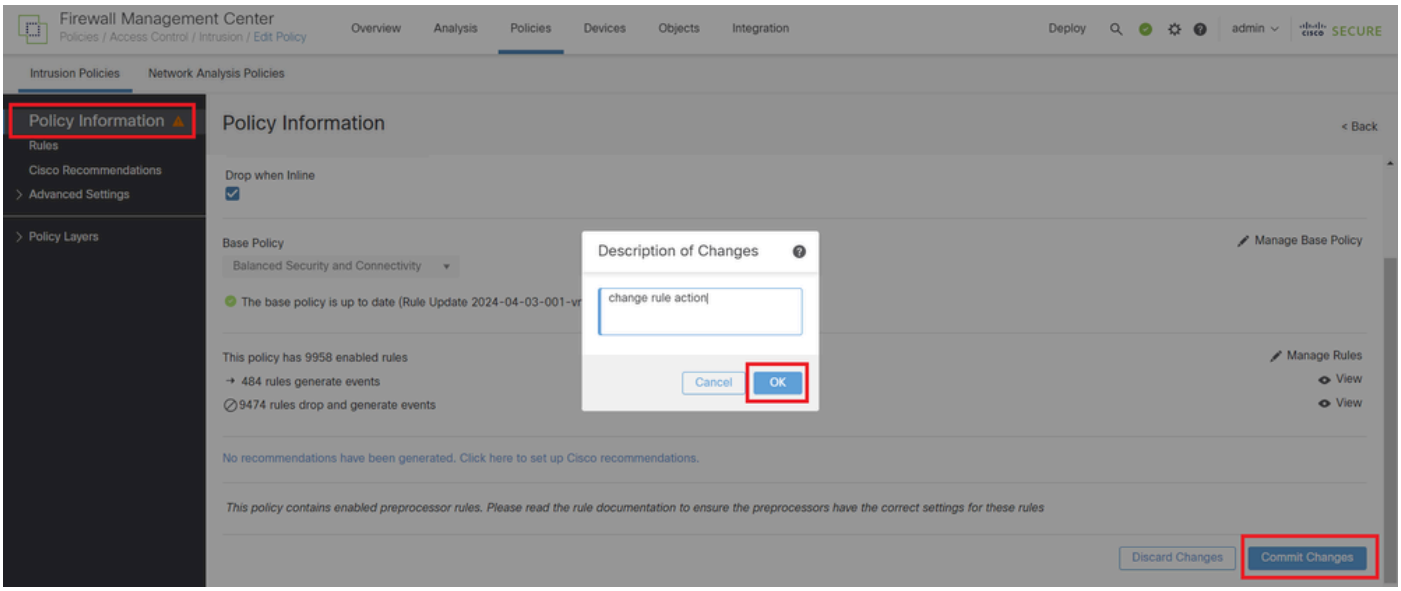
4단계. 규칙 작업 변경

State(상태) 버튼을 클릭하고 State(상태)를 Drop and Generate Events(이벤트 삭제 및 생성)로 설정한 다음 OK(확인) 버튼을 클릭합니다.



규칙 작업 변경

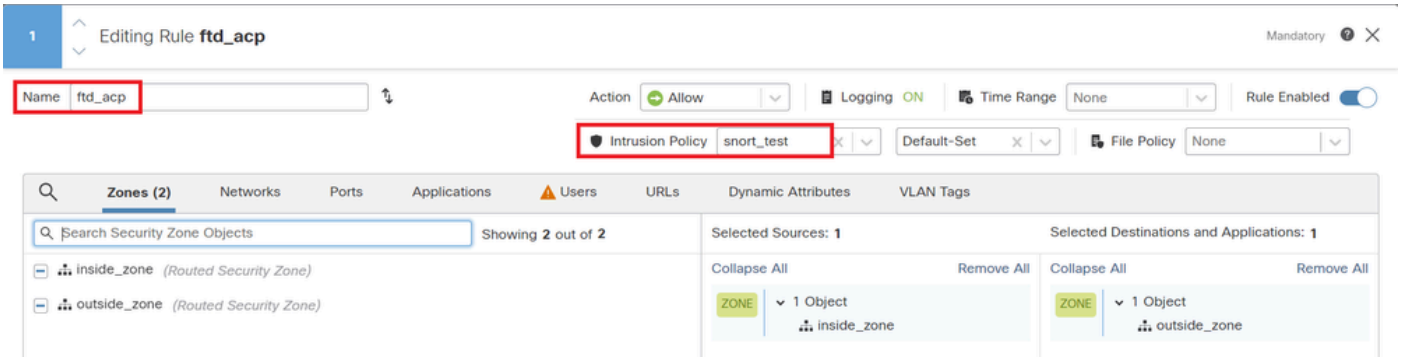
Policy Information(정책 정보) 버튼을 클릭하고 Commit Changes(변경 사항 커밋) 버튼을 클릭하여 변경 사항을 저장합니다.



변경 사항 커밋

5단계. 침입 정책을 ACP(액세스 제어 정책) 규칙과 연결

Policies(정책) > Access Control on FMC, associate Intrusion Policy with ACP로 이동합니다.



ACP 규칙과 연결

6단계. 변경 사항 배포

FTD에 변경 사항을 구축합니다.

변경 사항 배포

다음을 확인합니다.

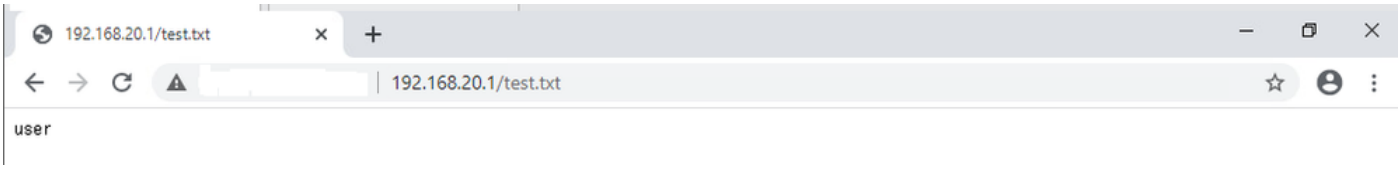
사용자 지정 로컬 Snort 규칙이 트리거되지 않음

1단계. HTTP 서버에서 파일 내용 설정

HTTP 서버 측의 test.txt 파일 내용을 user로 설정합니다.

2단계. 초기 HTTP 요청

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



초기 HTTP 요청

맞춤형 로컬 Snort 규칙이 트리거됨

1단계. HTTP 서버에서 파일 내용 설정

HTTP 서버 측의 test.txt 파일 내용을 username으로 설정합니다.

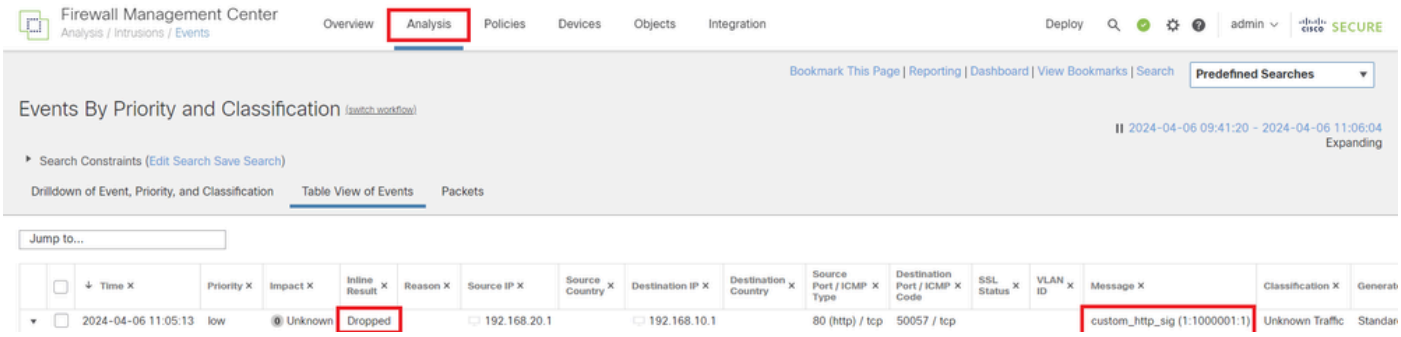
2단계. 초기 HTTP 요청

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

초기 HTTP 요청

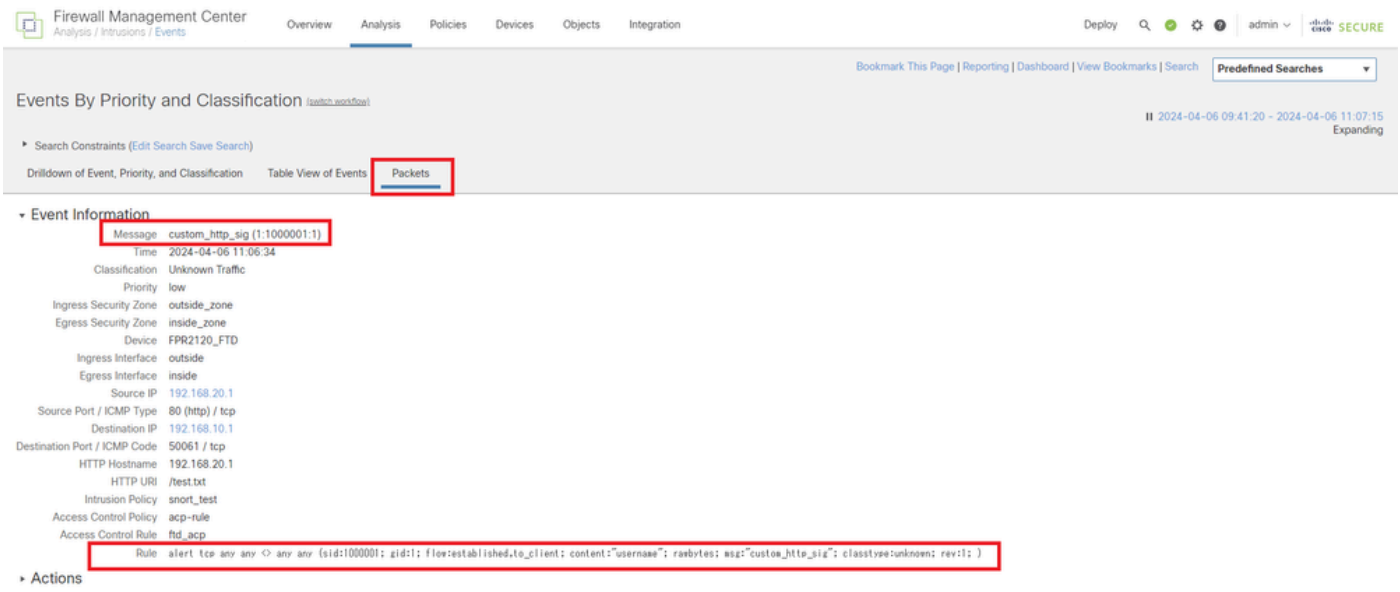
3단계. 침입 이벤트 확인

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



침입 이벤트

Packets 탭을 클릭하고 Intrusion Event의 세부사항을 확인합니다.



침입 이벤트의 세부사항

문제 해결

FTD의 동작을 확인하려면 명령을 실행합니다system support trace. 이 예에서는 HTTP 트래픽이 IPS 규칙(gid 1, sid 1000001)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:

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '
```

ftd_acp

', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

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.