CLI 및 FMC GUI를 사용하여 Firepower 센서에서 맞춤형 SID 목록 확인

소개

이 문서에서는 CLI 및 FMC GUI를 사용하여 Firepower Threat Defense(FTD) 또는 FirePOWER 모듈에서 사용자 지정 SID 목록을 가져오는 방법에 대해 설명합니다.SID 정보는 Objects(개체) > Intrusion Rules(침입 규칙)로 이동하면 FMC GUI에서 찾을 수 ***있습니다***.경우에 따라 CLI에서 사용 가능한 SID 목록을 가져오는 것이 필요합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제를 알고 있는 것이 좋습니다.

- Cisco FTD(Firepower Threat Defense)
- Cisco ASA with FirePOWER Services
- Cisco FMC(Firepower Management Center)
- Linux 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Firepower Management Center 6.6.0
- Firepower Threat Defense 6.4.0.9
- FirePOWER 모듈 6.2.3.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

침입 규칙은 시스템이 네트워크의 취약성을 악용하려는 시도를 탐지하기 위해 사용하는 키워드와 인수의 집합입니다.시스템은 네트워크 트래픽을 분석할 때 패킷을 각 규칙에 지정된 조건과 비교합니다.패킷 데이터가 규칙에 지정된 모든 조건과 일치하면 규칙이 트리거됩니다.규칙이 경고 규칙이면 침입 이벤트가 생성됩니다.통과 규칙이면 트래픽을 무시합니다.인라인 구축에서 삭제 규칙의 경우 시스템은 패킷을 삭제하고 이벤트를 생성합니다.Firepower Management Center 웹 콘솔에서 침입 이벤트를 보고 평가할 수 있습니다.

Firepower System은 두 가지 침입 규칙 유형을 제공합니다.***공유 객체 규칙*** 및 ***표준 텍스트 규칙***.Talos(Cisco Talos Security Intelligence and Research Group)는 공유 객체 규칙을 사용하여 기존 표준 텍스트 규칙이 할 수 없는 방식으로 취약점에 대한 공격을 탐지할 수 있습니다.공유 객체 규칙을 만들 수 없습니다.침입 규칙이 자체적으로 작성될 경우 표준 텍스트 규칙을 생성해야 합니다.보려는 이벤트 유형을 조정하기 위한 사용자 지정 표준 텍스트 규칙입니다.규칙을 작성하고 규칙의

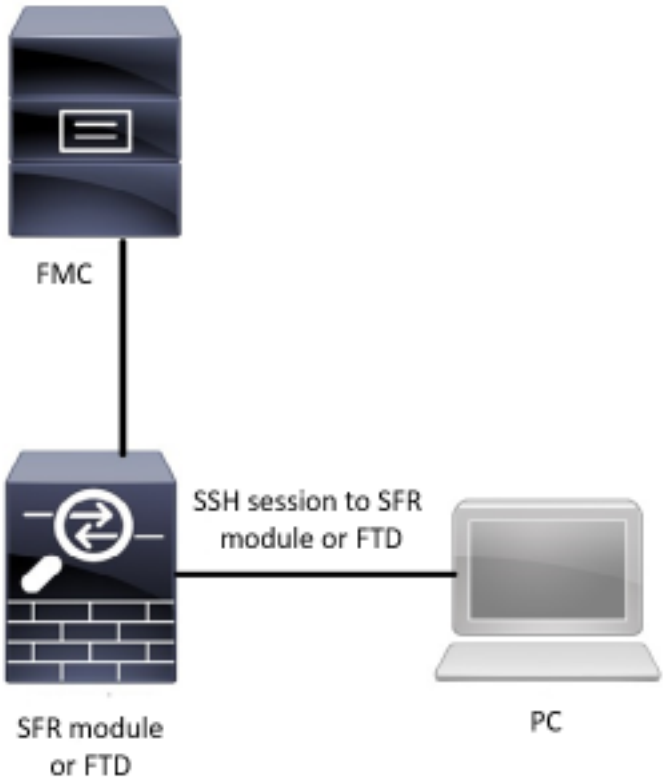
이벤트 메시지를 지정하면 공격 및 정책 회피를 나타내는 트래픽을 더 쉽게 식별할 수 있습니다.

사용자 지정 침입 정책에서 사용자 지정 표준 텍스트 규칙을 활성화할 경우, 일부 규칙 키워드와 인수는 트래픽을 특정 방식으로 먼저 디코딩하거나 전처리해야 한다는 점에 유의하십시오.

Firepower System의 사용자 지정 로컬 규칙은 로컬 시스템에서 ASCII 텍스트 파일 형식으로 가져오는 사용자 지정 표준 Snort 규칙입니다.Firepower System에서는 웹 인터페이스를 사용하여 로컬 규칙을 가져올 수 있습니다.로컬 규칙을 가져오는 단계는 매우 간단합니다.그러나 최적의 로컬 규칙을 작성하려면 Snort 및 네트워킹 프로토콜에 대한 심층적인 지식이 필요합니다.

> **경고:**프로덕션 환경에서 규칙을 사용하기 전에 작성한 침입 규칙을 테스트하려면 제어된 네트워크 환경을 사용해야 합니다.잘못 작성된 침입 규칙은 시스템 성능에 심각한 영향을 미칠 수 있습니다.

네트워크 다이어그램

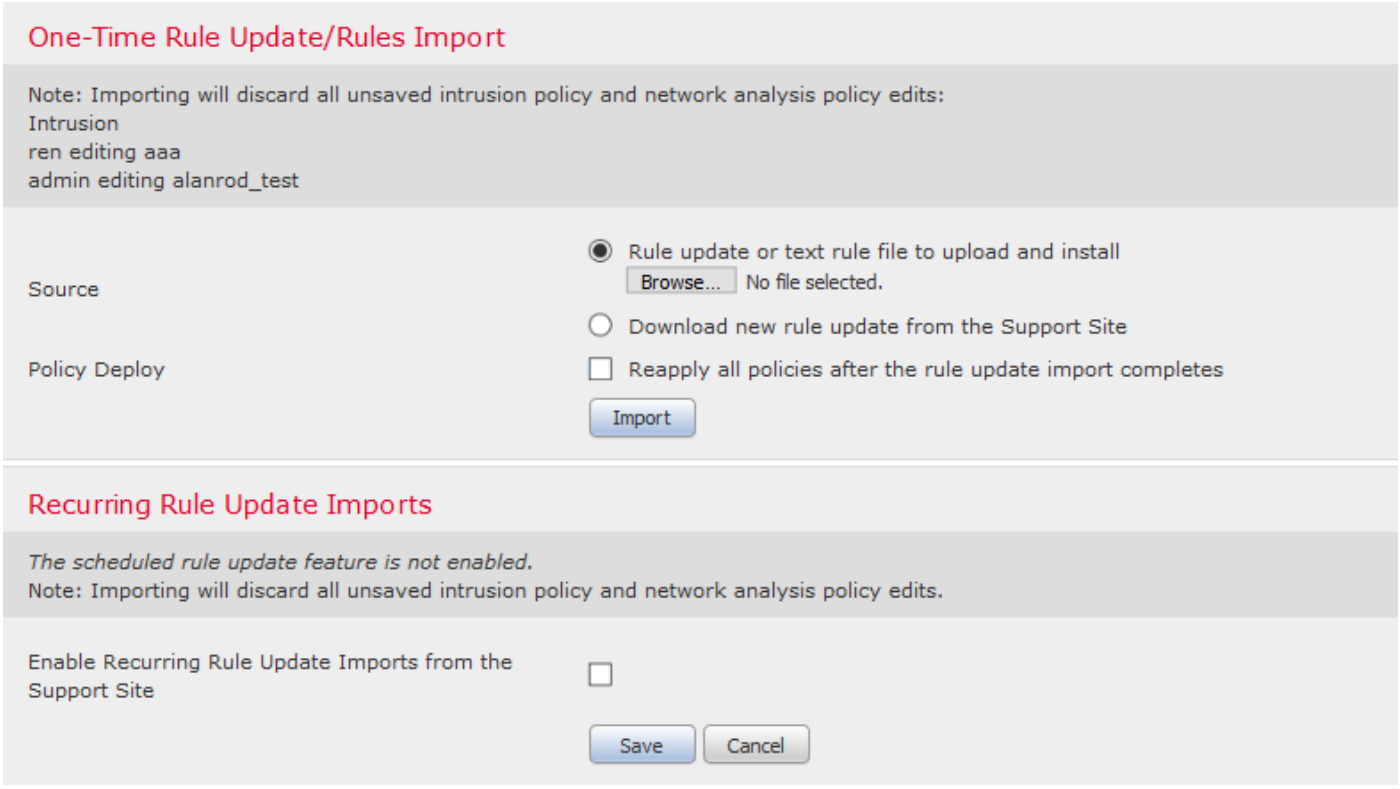


구성

로컬 규칙 가져오기

시작하기 전에 사용자 지정 파일에 나열된 규칙에 특수 문자가 포함되지 않았는지 확인해야 합니다.규칙 가져오기 도구를 사용하려면 ASCII 또는 UTF-8 인코딩을 사용하여 모든 사용자 지정 규칙을 가져와야 합니다.아래 절차에서는 로컬 컴퓨터에서 로컬 표준 텍스트 규칙을 가져오는 방법에 대해 설명합니다.

1단계. Objects(개체) > **Intrusion Rules(침입 규칙) > Import Rules(가져오기 규칙)로 이동하여 Import Rules(규칙 가져오기) 탭에 액세스합니다.**Rule **Updates** 페이지가 아래 이미지와 같이 나타납니다.



2단계. Rule update or text rule file to upload and install(업로드 및 설치할 규칙 업데이트 또는 텍스트 규칙 파일을 선택하고 **Browse**(찾아보기)를 클릭하여 사용자 지정 규칙 파일을 선택합니다.

> **참고:**업로드된 모든 규칙은 **로컬 규칙** 카테고리에 저장됩니다.

3단계. 가져오기를 **클릭합니다**.규칙 파일을 가져옵니다.

> **참고**: Firepower Systems는 검사에 새 규칙 집합을 사용하지 않습니다.로컬 규칙을 활성화하려면 Intrusion Policy에서 활성화한 다음 정책을 적용해야 합니다.

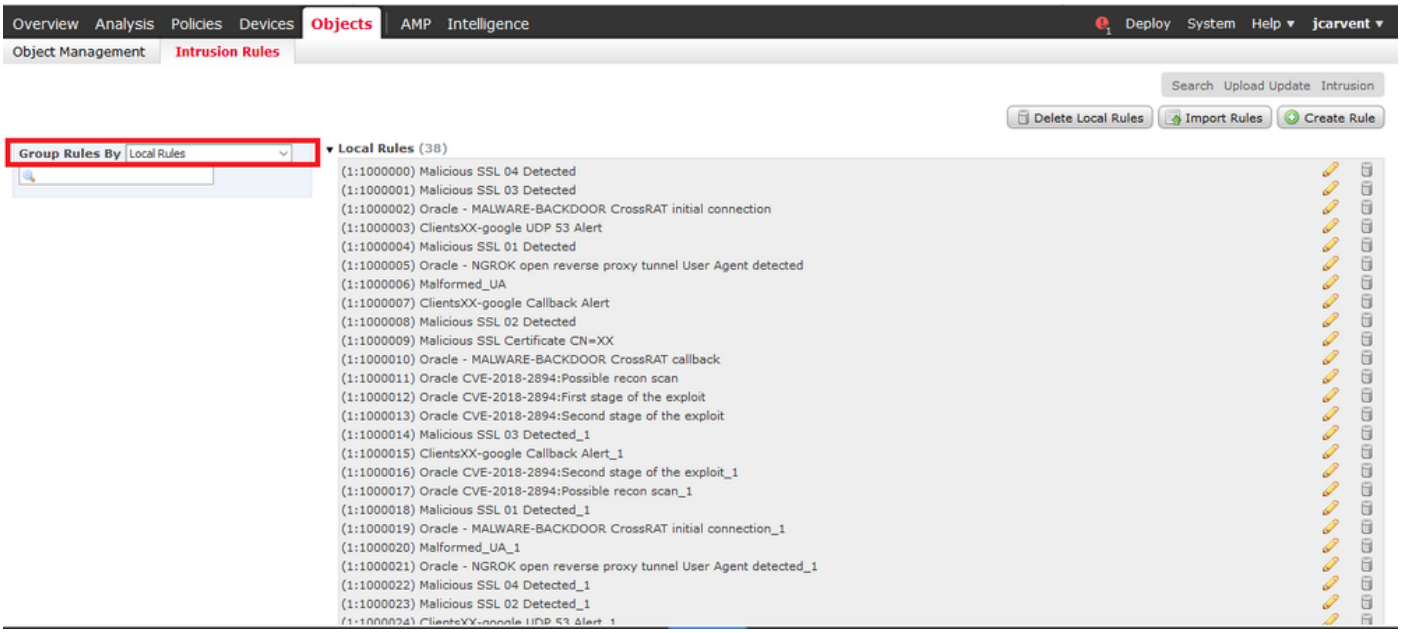
다음을 확인합니다.

FMC GUI에서

1. FMC GUI에서 가져온 로컬 규칙 보기

1단계. Objects **> Intrusion Rules로 이동합니다.**

2단계. 그룹 규칙에서 **로컬 규칙 선택**



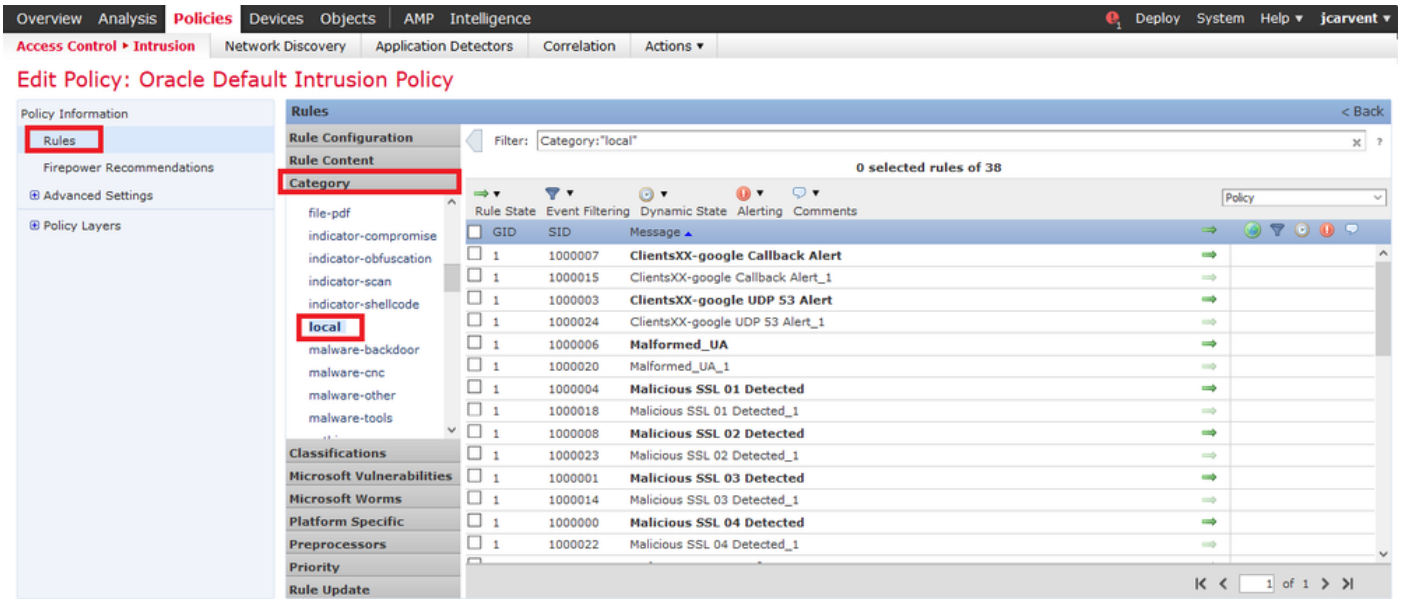
기본적으로 Firepower System은 로컬 규칙을 비활성화된 상태로 설정합니다.이러한 로컬 규칙은 침입 정책에서 사용할 수 있으려면 먼저 로컬 규칙의 상태를 수동으로 설정해야 합니다.

2. 침입 정책에서 로컬 규칙을 활성화합니다.

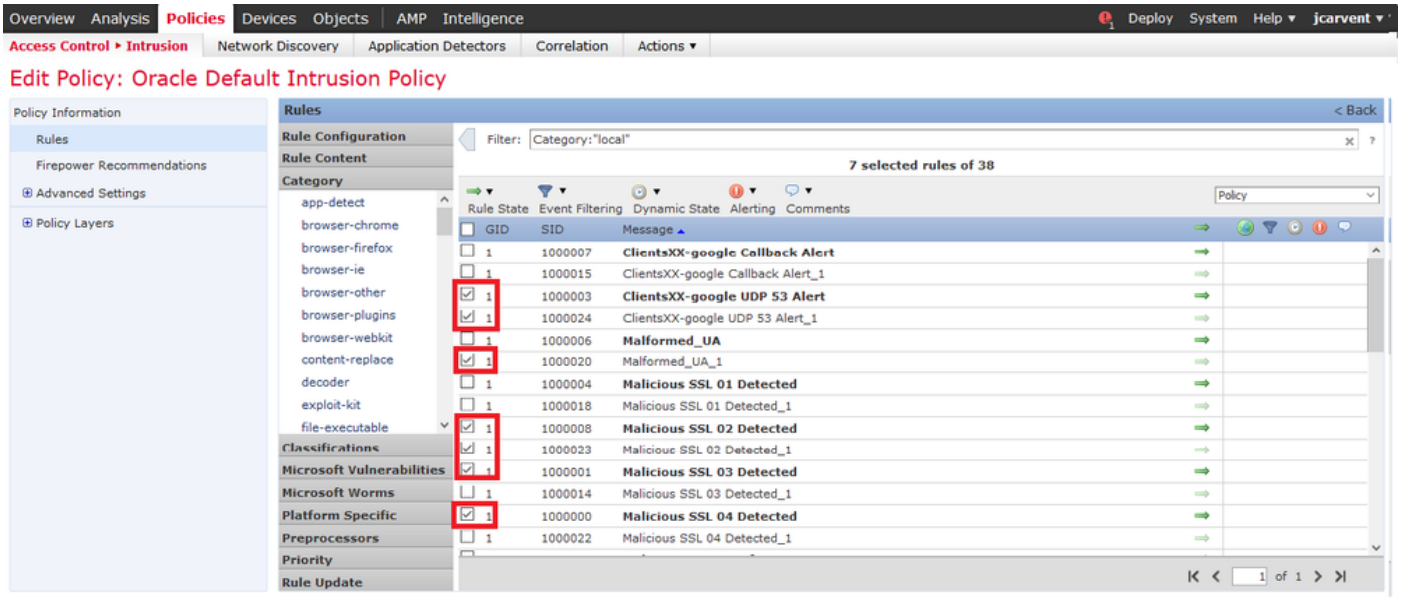
1단계. Policies(정책) > Intrusion(침입) > **Intrusion(침입 정책)** 아래의 Policy Editor(정책 편집기) 페이지로 이동합니다.

2단계. 왼쪽 패널에서 Rules를 선택합니다.

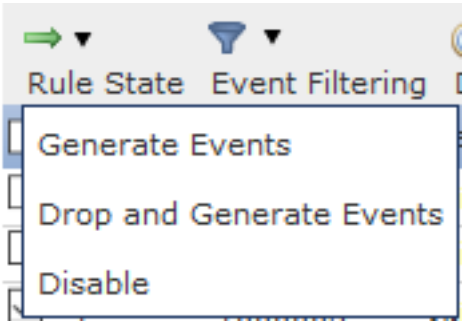
3단계. [범주]에서 **로컬**를 선택합니다. 사용 가능한 경우 모든 로컬 규칙이 나타납니다.



4단계. 원하는 로컬 규칙을 선택합니다.



5단계.원하는 로컬 규칙을 선택한 후 **Rule State**(규칙 상태)에서 상태를 선택합니다.



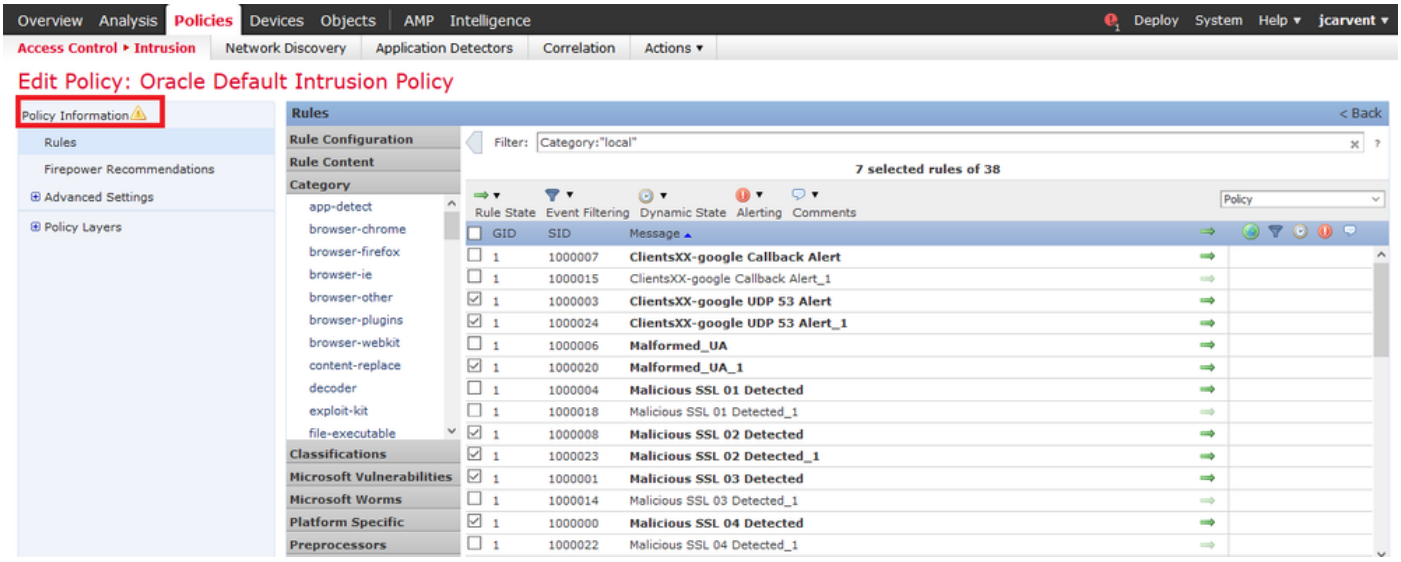
다음 옵션을 사용할 수 있습니다.

- 이벤트 생성:규칙을 활성화하고 이벤트를 생성합니다.

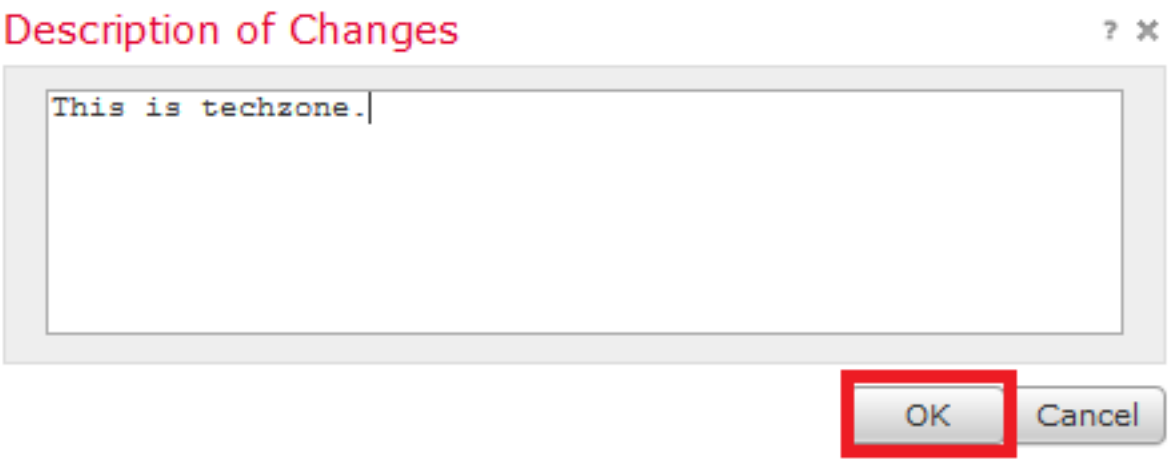
- 이벤트 삭제 및 생성:규칙을 활성화하고, 트래픽을 삭제하고, 이벤트를 생성합니다.

- 사용 안 함:규칙 사용 안 함, 이벤트 없음

6단계. 규칙 상태가 선택되면 왼쪽 패널의 **정책 정보** 옵션



7단계. 변경 사항 **커밋** 버튼을 선택하고 변경 사항에 대한 간단한 설명을 제공합니다.나중에 **OK**(확인)를 클릭합니다.침입 정책이 검증됩니다.



참고: 사용되지 않는 threshold 키워드를 침입 정책의 침입 이벤트 임계값 기능과 함께 사용하는 가져온 로컬 규칙을 활성화하면 정책 검증이 실패합니다.

8단계. 변경 사항 구축

FTD 또는 SFR 모듈 CLI에서

1. FTD 또는 SFR 모듈 CLI에서 가져온 로컬 규칙을 봅니다.

1단계. SFR 모듈 또는 FTD에서 SSH 또는 CLI 세션을 설정합니다.

2단계. 전문가 모드로 이동합니다.

```
> expert
admin@firepower:~$
```

3단계. 관리자 권한 가져오기

```
admin@firepower:~$ sudo su -
```

4단계. 비밀번호를 입력합니다.

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

5단계. /ngfw/var/sf/detection_engines/UUID/intrusion/로 이동합니다.

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

참고:SFR 모듈을 사용하는 경우 /ngfw/var/sf/detection_engines/*/intrusion path를 사용하지 마십시오.설치 **/var/sf/detection_engines/*/intrusion**

6단계. 다음 명령을 소개합니다.

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```

아래 이미지를 작업 예로 참조하십시오.

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```

FTD 또는 SFR 모듈에서 활성화된 고객 SID 목록이 나열됩니다.

문제 해결

1단계. FMC detection_engines에서 SSH 세션이 SFR 모듈 또는 FTD에 설정되어 있는지 확인합니다.

2단계. 명령 grep -Eo "sid:*([0-9]{1,8})" */*local.rules는 침입 디렉토리에서만 작동하며 다른 디렉토리에서 명령을 사용할 수 없습니다.

3단계. 모든 범주에서 전체 SID 목록을 가져오려면 grep -Eo "sid:*([0-9]{1,8})" */*.rules 명령을 사용합니다.

로컬 침입 규칙 가져오기 모범 사례

로컬 규칙 파일을 가져올 때 지침을 준수합니다.

- 규칙 가져오기 도구를 사용하려면 모든 사용자 지정 규칙을 ASCII 또는 UTF-8로 인코딩된 일반 텍스트 파일로 가져와야 합니다
- 텍스트 파일 이름에는 영숫자 문자, 공백 및 밑줄(_), 마침표(.) 및 대시(-) 이외의 특수 문자를 포함할 수 없습니다.
- 시스템은 단일 파운드 문자(#)로 시작하는 로컬 규칙을 가져오지만 삭제된 것으로 플래그가 지정됩니다
- 시스템은 단일 파운드 문자(#)로 시작하는 로컬 규칙을 가져오고 2파운드 문자(##)로 시작하는 로컬 규칙은 가져오지 않습니다
- 규칙은 이스케이프 문자를 포함할 수 없습니다.
- 로컬 규칙을 가져올 때 GID(Generator ID)를 지정할 필요가 없습니다.이 경우 표준 텍스트 규칙에 대해 GID 1만 지정합니다.
- 규칙을 처음 가져올 때 다음을 수행합니다. *아님* 지정 Snort ID (SID) 또는 수정 번호입니다.이렇게 하면 삭제된 규칙을 비롯한 다른 규칙의 SID와의 충돌이 방지됩니다.시스템은 사용 가능한 다음 사용자 지정 규칙 SID 100000 이상과 수정 번호 1을 자동으로 할당합니다
- SID로 규칙을 가져와야 하는 경우 SID는 1,000,000에서 9,999,999 사이의 고유한 숫자여야 합니다.
- 다중 도메인 구축에서 시스템은 의 모든 도메인에서 사용하는 공유 풀에서 가져온 규칙에

SID를 할당합니다 Firepower Management Center.여러 관리자가 동시에 로컬 규칙을 가져오는 경우, 시스템이 시퀀스의 중간 번호를 다른 도메인에 할당했기 때문에 개별 도메인 내의 SID가 비순차적 것으로 보일 수 있습니다

- 이전에 가져온 로컬 규칙의 업데이트된 버전을 가져오거나 삭제한 로컬 규칙을 복원할 때 시스템에서 할당한 SID와 현재 수정 번호보다 큰 수정 번호를 포함해야 ***합니다***.규칙을 편집하여 현재 또는 삭제된 규칙의 개정 번호를 결정할 수 있습니다

  참고: 로컬 규칙을 삭제하면 시스템에서 자동으로 개정 번호를 증가시킵니다.로컬 규칙을 복원할 수 있는 디바이스입니다.삭제된 모든 로컬 규칙은 로컬 규칙 카테고리에서 삭제된 규칙 카테고리로 이동합니다.

- SID 번호 지정 문제를 방지하려면 고가용성 쌍의 기본 Firepower Management Center에서 로컬 규칙을 가져옵니다.
- 규칙에 다음 중 하나가 포함된 경우 가져오기가 실패합니다.SID가 2147483647보다 큽니다 .64자를 초과하는 소스 또는 대상 포트 목록
- 사용되지 않는 ***threshold 키워드***를 침입 정책의 침입 이벤트 임계값 기능과 함께 사용하는 가져온 로컬 규칙을 활성화하면 정책 검증이 실패합니다.
- 가져온 모든 로컬 규칙은 로컬 규칙 카테고리에 자동으로 저장됩니다.
- 시스템은 사용자가 비활성화된 규칙 상태로 가져오는 로컬 규칙을 항상 설정합니다.침입 정책에서 사용하려면 먼저 로컬 규칙의 상태를 수동으로 설정해야 합니다

관련 정보

다음은 Snort SID와 관련된 참조 문서입니다.

침입 규칙 업데이트

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

침입 규칙 편집기

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html