Secure Firewall Management Center에서 Snort 2를 Snort 3로 마이그레이션

Snort 2에서 Snort 3로 마이그레이션

Snort는 버전 2에서 버전 3으로 업그레이드되며 상당한 변경 사항이 적용된 침입 탐지 및 방지 시스템입니다. Snort 3의 향상된 기능을 활용하려면 Snort 2에서 기존 규칙 집합을 마이그레이션하는 것이 중요합니다. 이 마이그레이션 프로세스에는 Snort 2 규칙을 Snort 3 규칙 구문으로 변환 및 조정하며 향상된 탐지 및 성능을 위해 최적화하는 작업이 포함됩니다.

경우에 따라 조직은 Secure Firewall Management Center에서 관리하는 Threat Defense 디바이스를 사용할 수 있습니다. 조직은 Snort 2에서 Snort 3로 마이그레이션하는 동안 하이브리드 구축 접근 방식을 선택할 수 있습니다. 이 접근 방식을 사용하면 점진적 전환이 가능하며 잠재적인 중단(있는 경우)을 최소화할 수 있습니다.

Snort 3로의 마이그레이션 이점

- 향상된 프로토콜 지원 - Snort 3는 향상된 프로토콜 지원을 제공하므로, 암호화된 트래픽을 포함하여 광범위한 최신 프로토콜에 걸쳐 위협을 모니터링하고 탐지할 수 있습니다.
- 간소화된 규칙 관리 - Snort 3는 사용자 친화적 규칙 언어 및 규칙 관리 시스템을 제공하므로, 규칙을 보다 쉽게 생성, 수정 및 관리할 수 있습니다.

- 향상된 성능 - Snort 3는 더 많은 트래픽을 더욱 효율적으로 처리하도록 최적화되어 성능 병목 현상의 위험을 줄이고 적시에 위협 탐지를 보장합니다.

샘플 비즈니스 시나리오

Alice는 네트워크 인프라를 모니터링하고 보호하기 위해 Snort 검사 엔진에 크게 의존하는 대규모 조직에서 보안 분석가로 일하고 있습니다. 이 조직에서는 수년 동안 Snort 버전 2를 사용해 왔지만, 몇 가지 제한 사항과 문제가 발생했습니다.

네트워크 관리자인 Bon은 이러한 문제를 해결하고 조직의 네트워크 보안 기능을 강화하기 위해 Snort 2에서 Snort 3로 마이그레이션하려고 합니다.

또한 이러한 마이그레이션을 수행하면 네트워크 보안 모니터링이 개선되고, 성능이 향상되며, 규칙 관리가 간소화됩니다.

Snort 2에서 Snort 3로 마이그레이션하기 위한 모범 사례

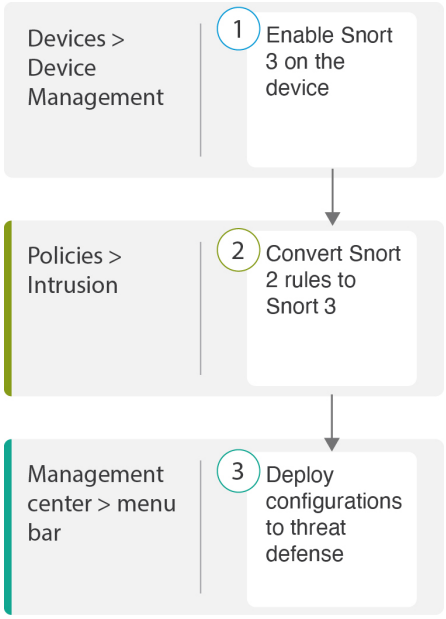
- 마이그레이션을 수행하기 전에 침입 정책을 백업합니다. *Cisco Secure Firewall Management Center* 관리 가이드의 구성 내보내기 작업을 참조하십시오.
- 디바이스를 Snort 3로 업그레이드하기 전에 Snort 2에서 변경한 경우 Snort 2에서 Snort 3로 최신 동기화를 포함하도록 동기화 유틸리티를 사용하여 유사한 커버리지로 시작할 수 있습니다. Snort 2 규칙과 Snort 3 동기화의 내용을 참조하십시오.
- Snort 2 맞춤형 규칙은 Snort 3로 자동 변환되지 않으므로 수동으로 마이그레이션해야 합니다. Snort 2 사용자 지정 IPS 규칙을 Snort 3로 변환의 내용을 참조하십시오.
- 동기화는 임계값 또는 억제가 포함된 Snort 2 규칙을 마이그레이션하지 않습니다. 이러한 규칙은 Snort 3에서 다시 생성해야 합니다.

사전 요구 사항

- Snort에 대한 실제 지식이 있어야 합니다. Snort 3 아키텍처에 대한 자세한 내용은 Snort 3 도입을 참조하십시오.
- Management Center를 백업합니다. Management Center 백업을 참조하십시오.
- 침입 정책을 백업합니다. 구성 내보내기를 참조하십시오.

엔드 투 엔드 마이그레이션 워크플로우

다음 순서도에는 Secure Firewall Management Center에서 Snort 2를 Snort 3로 마이그레이션하기 위한 워크플로우가 나와 있습니다.

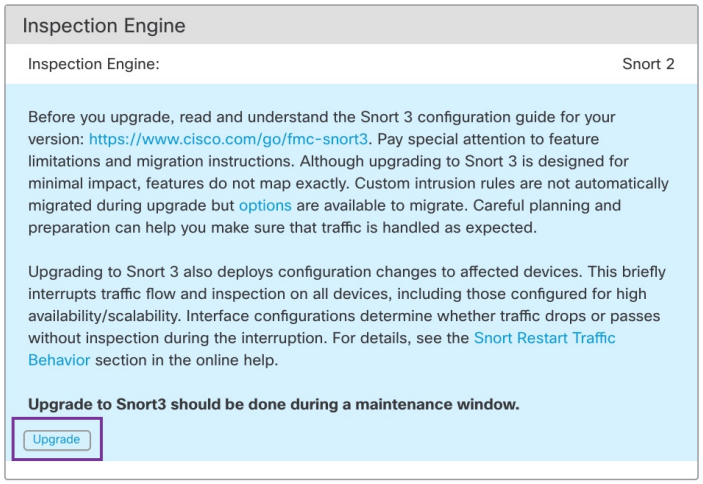


단계	설명
1	디바이스에서 Snort 3를 활성화합니다. Threat Defense에서 Snort 3 활성화, 3 페이지의 내용을 참조하십시오.
2	Snort 2 규칙을 Snort 3로 변환합니다. 단일 침입 정책의 Snort 2 규칙을 Snort 3로 변환, 4 페이지의 내용을 참조하십시오.
3	구성을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

Threat Defense에서 Snort 3 활성화

주의 구축 프로세스 중에는 현재 검사 엔진을 종료해야 하므로 일시적인 트래픽 손실이 발생할 수 있습니다.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
단계 **2** 해당 디바이스를 클릭하여 디바이스 홈페이지로 이동합니다.
단계 **3** **Device(**디바이스**)** 탭을 클릭합니다.
단계 **4** **Inspection Engine(**검사 엔진**)** 섹션에서 **Upgrade(**업그레이드**)**를 클릭합니다.



단계 **5** **Yes(**예**)**를 클릭합니다.

다음에 수행할 작업

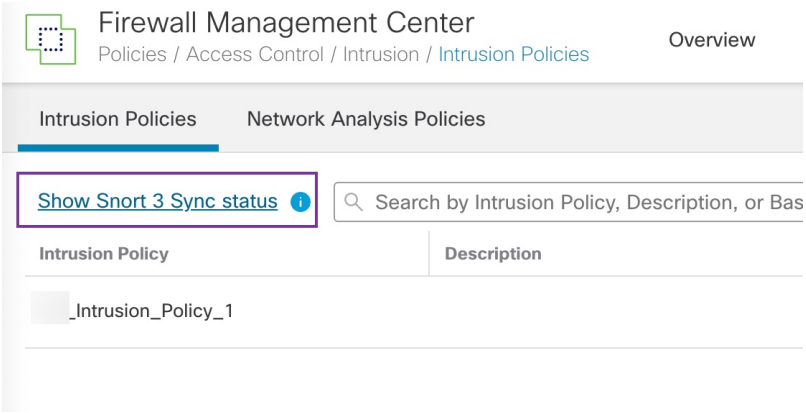
디바이스에서 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

시스템은 구축 프로세스 중에 선택한 Snort 버전과 호환되도록 정책 설정을 변환합니다.

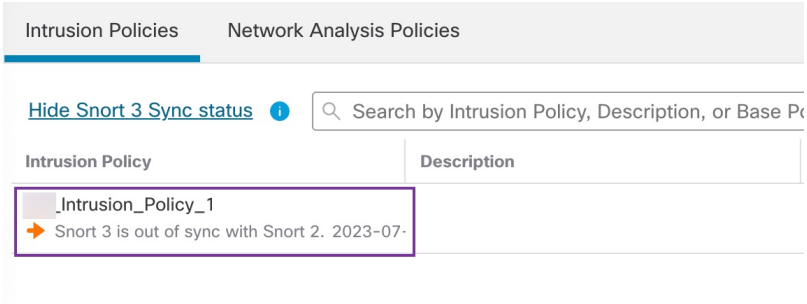
단일 침입 정책의 Snort 2 규칙을 Snort 3로 변환

단계 **1** **Policies(**정책**)** > **Intrusion(**침입**)**을 선택합니다.

단계 **2** **Intrusion Policies(**침입 정책**)** 탭에서 **Show Snort 3 Sync status(Snort 3** 동기화 상태 표시**)**를 클릭합니다.

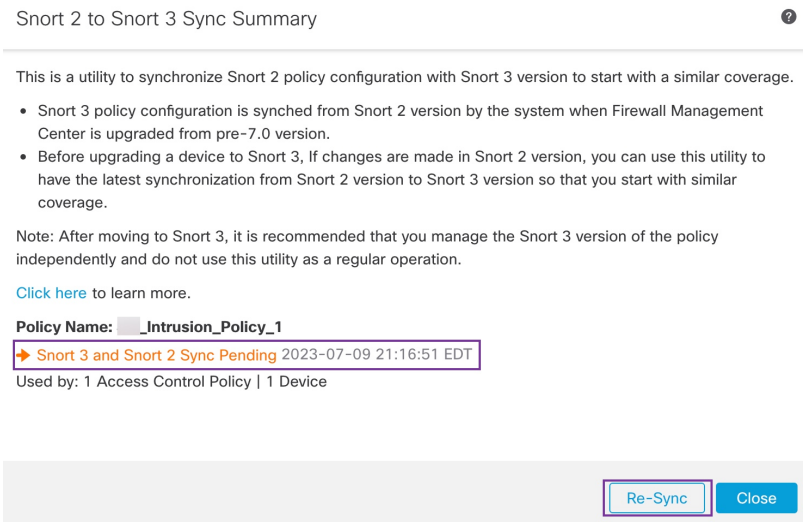


정책에 주황색 화살표가 표시되면 Snort 2 및 Snort 3 버전의 침입 정책이 동기화되지 않았음을 나타냅니다.



단계 **3** 주황색 화살표를 클릭합니다.

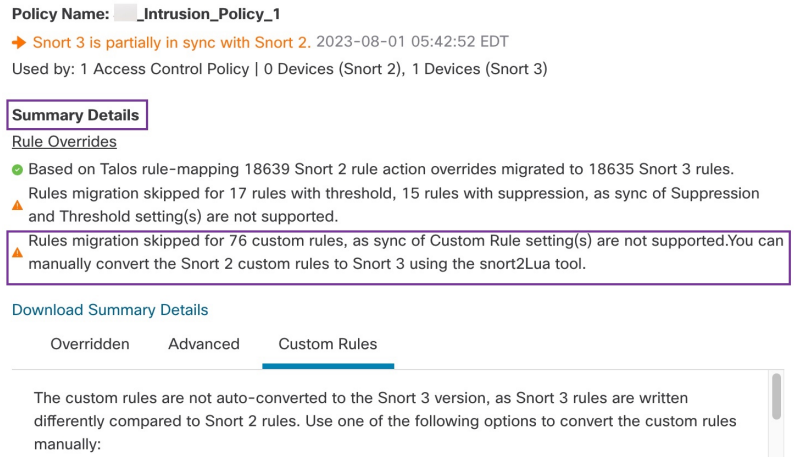
Snort 2 to Snort 3 Sync Summary(Snort 2에서 **Snort 3**로의 동기화 요약**)** 페이지에 Snort 2에서 Snort 3로의 동기화가 보류 중이라는 메시지가 표시됩니다.



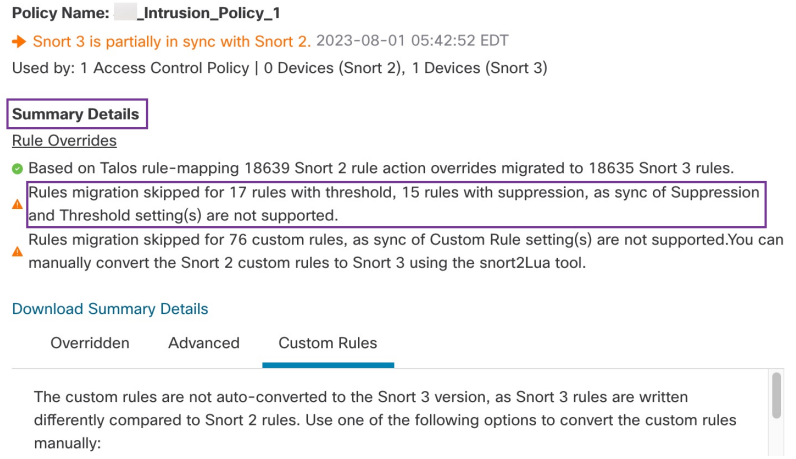
단계 **4** **Re-Sync(**재동기화**)**를 클릭하여 동기화를 시작합니다.

참고 **Re-Sync(**재동기화**)**를 클릭하면 snort2Lua 툴이 규칙을 Snort 2에서 Snort 3로 변환합니다.

Summary Details(요약 세부 정보**)** 섹션에는 마이그레이션되었거나 건너뛴 규칙이 나열됩니다. 이 활용 사례에는 동기화 프로세스 중에 건너뛴 사용자 지정 Snort 2 규칙 76개, 임계값이 있는 규칙 17개, 억제가 포함된 규칙 15개가 있습니다. 사용자 지정 규칙을 마이그레이션하려면 다음 단계로 이동합니다.

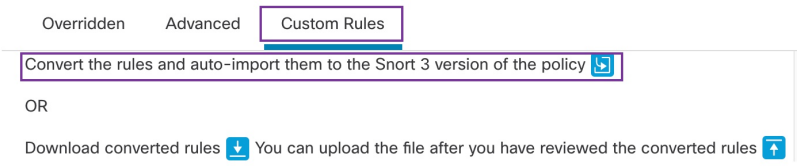


임계값 및 억제가 포함된 규칙을 마이그레이션하려면 단계 6으로 이동합니다.



단계 **5** 76개의 사용자 지정 규칙을 마이그레이션하려면 다음 단계 중 하나를 수행합니다.

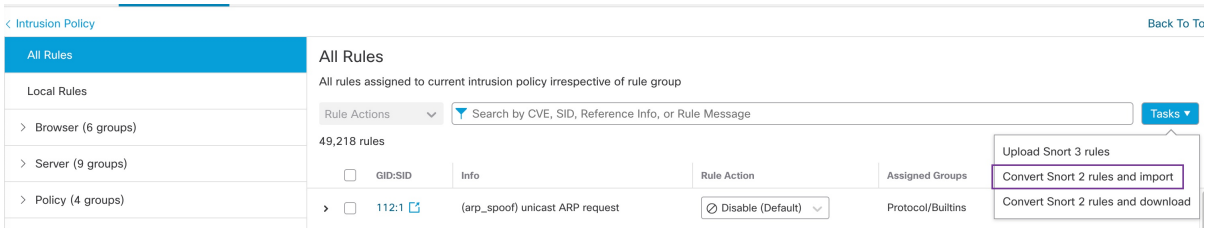
- **Custom Rules(**사용자 지정 규칙**)** 탭에서 **Import(**가져오기**)** 아이콘을 클릭하여 로컬 규칙을 Snort 3 버전 정책으로 변환하고 자동으로 가져옵니다.



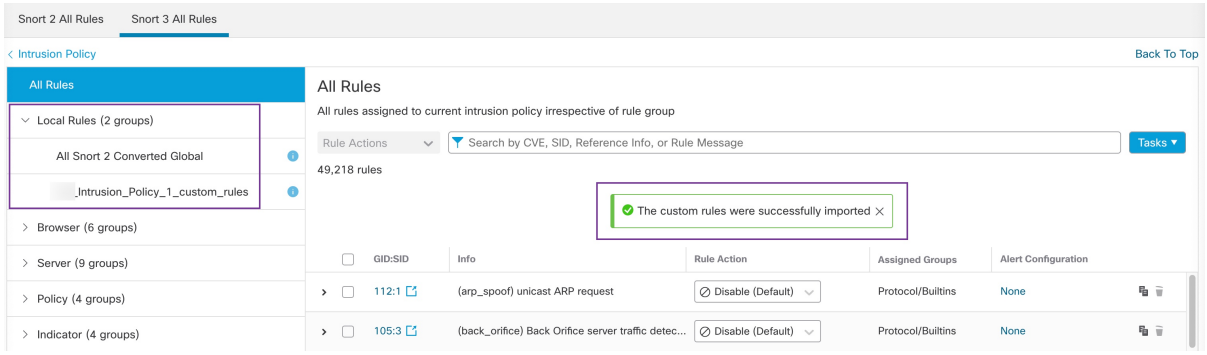
  규칙을 성공적으로 가져오고 나면 확인 메시지가 표시됩니다.

- **Objects(**개체**) > Intrusion Rules(**침입 규칙**)**를 선택하고 **Snort 3 All Rules(**모든 **Snort 3** 규칙**)**를 클릭합니다.

  1. 왼쪽 패널에서 **Local Rules(**로컬 규칙**)**를 클릭하여 규칙이 마이그레이션되었는지 확인합니다. Snort 2의 사용자 지정 규칙은 마이그레이션되지 않았습니다.
  2. **Tasks(**작업**)** 드롭다운 목록에서 **Convert Snort 2 rules and import(Snort 2** 규칙 변환 및 가져오기**)**를 선택합니다.

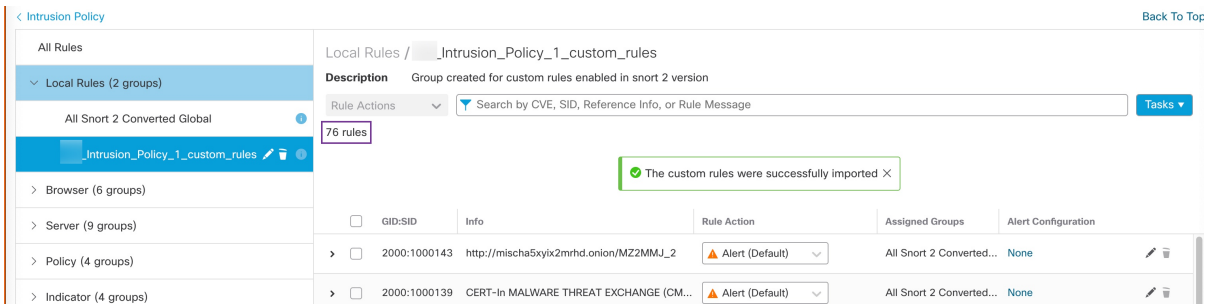


3. **OK(확인)**를 클릭합니다.



새로 생성된 규칙 그룹(**All Snort 2 Converted Global(**모든 **Snort 2** 변환 전역**)**)이 왼쪽 패널의 **Local Rules(**로컬 규칙**)**에 생성됩니다.

다음 그림에 나와 있는 것처럼 76개의 사용자 지정 규칙이 모두 마이그레이션되었습니다.



아니면 이전 단계에서 **Convert Snort 2 rules and download(Snort 2** 규칙 변환 및 다운로드**)**를 선택하여 규칙 파일을 로컬에 저장할 수 있습니다. 다운로드한 파일에서 변환된 규칙을 검토한 후 나중에 **Upload Snort 3 Rules(Snort 3** 규칙 업로드**)** 옵션을 사용하여 업로드할 수 있습니다.

단계 **6** .txt 형식의 규칙을 다운로드하려면 **Download Summary Details(**요약 세부 정보 다운로드**)** 링크를 클릭합니다.

다음은 표시되는 요약의 샘플입니다.

```
"id": "00505691-15DC-0ed3-0000-004294988561",
"name": "_Intrusion_Policy_1",
"type": "IntrusionPolicy",
"syncStatus": {
  "source": {
    "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
    "type": "IntrusionPolicy"
  },
  "status": "WARN",
```

```
    "description": "Migration is partially successful. Some of the rules are not copied to Snort3.",
    "timestamp": 1690883954814,
    "lastUser": {
      "name": "admin"
    },
    "details": [
      {
        "type": "Summary",
        "status": "INFO",
        "description": "Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to
18635 Snort 3 rules."
      },
      {
        "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,

1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,

1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,


1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,


1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,


1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,


1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,


1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,


1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,


1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,

         1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",
        "type": "PolicyInfo",
        "description": "Corresponding Snort 2 policy overridden custom (local) rules."
      },
      {
        "type": "AssignedDevices",
        "status": "INFO",
        "description": "Snort3:0 , Snort2:0"
      },
      {
        "id": "122:6",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
      },
      {
        "id": "122:15",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_IP_PORTSWEEP_FILTERED"
       },
      {
        "id": "122:1",
```

```
    "type": "Threshold",
    "status": "ERROR",
    "description": "PSNG_TCP_PORTSCAN"
  },
```


단계 **7** **Close(**닫기**)**를 클릭하여 **Sync Summary(**동기화 요약**)** 대화 상자를 닫습니다.

단계 **8** : ERROR 상태의 규칙을 확인하려면 **Policies(**정책**) > Intrusion(**침입**)**을 선택하고 **Snort 2** 버전 침입 정책을 클릭합니다.

단계 **9** **Policy Information(**정책 정보**)**에서 **Rules(**규칙**)**를 클릭하고 규칙을 기준으로 필터링합니다. 예를 들어, 규칙을 찾으려면 **Filter(**필터**)** 필드에 **PSNG_TCP_PORTSCAN**을 입력합니다.

단계 **10** **Show Details(**세부 정보 표시**)**를 클릭하여 규칙의 상세 버전을 확인합니다.

단계 **11** Snort 3 규칙 지침을 사용하여 Snort 3에서 다시 규칙을 생성하고 파일을 .txt 또는 .rules 파일로 저장합니다. 자세한 내용은 www.snort3.org를 참조하십시오.

단계 **12** 방금 로컬로 만든 사용자 지정 규칙을 모든 Snort 3 규칙 목록에 업로드합니다. 규칙 그룹에 사용자 지정 규칙 추가를 참조하십시오.

다음에 수행할 작업

구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

구성 변경 사항 구축

구성을 변경한 후 해당하는 디바이스에 구축합니다.

참고 이 주제에서는 구성 변경 사항 구축과 관련된 기본 단계를 다룹니다. 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에서 구성 변경 사항 구축 주제를 참조하여 단계를 진행하기 전에 변경 사항 구축의 사전 요건과 영향을 파악할 것을 강력하게 권장합니다.

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 구성을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다.

단계 **1** Secure Firewall Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭하고 **Deployment(**구축**)**를 선택합니다.

GUI 페이지에는 **Pending(**보류 중**)** 상태인 오래된 구성이 있는 디바이스가 나열됩니다.

- **Modified By(**수정 주체**)** 열에는 정책 또는 개체를 수정한 사용자가 나열됩니다. 디바이스 목록을 확장하여 각 정책 목록에 대한 정책을 수정한 사용자를 볼 수 있습니다.

  참고 삭제된 정책 및 개체에 대해서는 사용자 이름이 제공되지 않습니다.

- **Inspect Interruption(**검사 중단**)** 열은 구축 중에 디바이스에서 트래픽 검사 중단이 발생할 수 있는지 여부를 나타냅니다.

  디바이스에 대한 이 열이 비어 있으면 구축 중에 해당 디바이스에서 트래픽 검사가 중단되지 않음을 나타냅니다.

- **Last Modified Time(**마지막 수정 시간**)** 열은 구성 변경을 마지막으로 수행한 시간을 지정합니다.
- **Preview(**미리보기**)** 열에서는 다음 구축에 대한 변경 사항을 미리 볼 수 있습니다.
- **Status(**상태**)** 열은 각 구축의 상태를 제공합니다.

단계 **2** 구성 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스별 구성 변경 사항을 보려면 확장 화살표( )를 클릭합니다.

  디바이스에 인접한 체크박스를 선택하면 디바이스에 대해 이루어지고 디바이스 아래에 나열된 모든 변경 사항이 구축을 위해 푸시됩니다. 그러나 정책 선택( )을 사용하면 구축하지 않고 나머지 변경 사항을 보류하면서 구축할 개별 정책 또는 특정 구성을 선택할 수 있습니다.

  참고

  - **Inspect Interruption(**검사 중단**)** 열의 상태가 (**Yes(**예**)**)인 경우(구축하면 위협 방어 디바이스에서 검사가 중단되며 트래픽도 중단될 수 있음) 확장된 목록에서 검사 중단( ) 중단을 야기하는 특정 구성을 표시합니다.
  - 인터페이스 그룹, 보안 영역 또는 개체가 변경되면 영향을 받는 디바이스는 management center에서 오래된 것으로 표시됩니다. 이러한 변경 사항을 적용하려면 이러한 인터페이스 그룹, 보안 영역 또는 개체가 포함된 정책도 이러한 변경 사항과 함께 구축해야 합니다. 영향을 받는 정책은 management center의 **Preview(**미리보기**)** 페이지에서 만료된 것으로 표시됩니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 창에 이를 표시합니다. 전체 세부 사항을 보려면 경고 또는 오류 앞에 있는 화살표 아이콘을 클릭합니다.

다음 옵션을 이용할 수 있습니다.

- Deploy(구축) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) - 구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 구성을 재구축합니다.

다음에 수행할 작업

구축 중에 구축 장애가 발생하는 경우 해당 장애가 트래픽에 영향을 미칠 수 있습니다. 그러나 특정 조건에 따라 달라집니다. 구축의 특정 구성이 변경된 경우 구축 장애로 인해 트래픽이 중단될 수 있습니다. 자세한 내용은 최신 버전의 *Cisco Secure Firewall Management Center* 구성 가이드에 있는 구성 변경 사항 구축 주제를 참조하십시오.