Snort 3 침입 정책 시작

다음 항목에서는 Snort 3 침입 정책을 시작하는 방법을 설명합니다.

침입 정책 기본 사항

침입 정책은 트래픽에서 보안 위반을 검사하고 인라인 구축에서 악성 트래픽을 차단 또는 변경할 수 있는 침입 탐지 및 방지 구성의 정의된 집합입니다. 침입 정책은 액세스 제어 정책에 따라 호출되며, 트래픽이 대상에 허가되기 전 시스템의 마지막 방어선입니다.

각 침입 정책의 핵심에는 침입 규칙이 있습니다. 활성화된 규칙은 시스템이 규칙과 일치하는 트래픽의 침입 이벤트를 생성하도록 (하거나 선택적으로 차단하도록) 합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다.

Firepower System은 Cisco Talos(Talos Intelligent Group)의 경험을 활용할 수 있는 여러 기본 침입 정책을 제공합니다. Talos는 이 정책에 대해 침입 및 전처리기 규칙 상태(활성화 또는 비활성화)를 설정할 뿐 아니라 다른 고급 설정의 초기 구성을 제공합니다.

팁 시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다.

사용자 지정 침입 정책을 생성하는 경우, 다음을 수행할 수 있습니다.

- 규칙 활성화/비활성화 및 고유의 규칙 작성과 추가를 통해 탐지 기능을 조정할 수 있습니다.
- Firepower 권장 사항을 사용하여 네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산을 보호하기 위해 특별히 작성한 규칙과 연결합니다.
- 외부 경고, 민감한 데이터 전처리 및 전역 규칙 임계값과 같은 다양한 고급 설정을 구성합니다.
- 효율적으로 여러 침입 정책을 관리하기 위해 레이어를 구성 요소로 사용합니다.

침입 정책은 일치하는 패킷을 삭제하고 침입 이벤트를 생성할 수 있습니다. 침입 또는 전처리기 삭제 규칙을 구성하려면 해당 상태를 Block(차단)으로 설정합니다.

침입 정책을 조정할 경우, 특히 규칙을 활성화하고 추가할 경우, 일부 침입 규칙에서는 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 합니다. 침입 정책이 패킷을 검토하기 전에, 패킷은 네트워크 분석 정책 내 구성에 따라 전처리됩니다. 검사기를 비활성화한 경우, 검사기가 네트워크 분석 정책 웹 사용자 인터페이스에서 비활성화된 상태로 남아 있다고 해도 시스템은 자동으로 검사기를 현재의 설정으로 사용합니다.

주의 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 반드시 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 고급 작업입니다.

사용자 지정 침입 정책을 구성한 후, 하나 이상의 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 침입 정책을 연결함으로써 액세스 제어 구성의 일부로 사용할 수 있습니다. 이는 트래픽이 최종 대상으로 전달되기 전에 허용되는 특정 트래픽을 검토하기 위해 시스템이 침입 정책을 강제로 사용하도록 합니다. 침입 정책과 페어링된 변수 집합을 통해 홈 네트워크 및 외부 네트워크와 사용자 네트워크의 서버를 적절하게 반영할 수 있습니다.

기본적으로 시스템은 암호화된 페이로드의 침입 검사를 비활성화합니다. 이는 암호화 연결이 침입 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

침입 정책을 위한 라이선스 요건

FTD 라이센스

위협

기본 라이선스

보호

침입 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

사용자 지정 **Snort 3** 침입 정책 생성

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

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다.

Intrusion Policies(침입 정책) 탭이 선택되었는지 확인합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력하고, 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **4** **Inspection Mode(**검사 모드**)**를 선택합니다.

선택한 작업에 따라 침입 규칙이 차단 및 알림(예방 모드) 또는 알림만(탐지 모드)인지 여부가 결정됩니다.

참고 예방 모드를 선택하기 전에 차단 규칙이 알림만 표시할 수 있도록 하여 많은 오탐을 유발하는 규칙을 식별할 수 있습니다.

단계 **5** **Base Policy(**기본 정책**)**를 선택합니다.

시스템 제공 정책 또는 다른 맞춤형 정책을 기본 정책으로 사용할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

새로운 정책의 설정은 기본 정책의 설정과 같습니다.

다음에 수행할 작업

정책을 사용자 지정하려면 Snort 3 침입 정책 편집, 4 페이지 항목을 참조하십시오.

Snort 3 침입 정책 편집

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

단계 2 **Intrusion Policies(**침입 정책**)** 탭이 선택되었는지 확인합니다.

단계 3 설정하려는 침입 정책 옆의 **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다.

단계 4 정책 수정:

- 모드 변경 - 검사 모드를 변경하려면 **Mode(**모드**)** 드롭다운을 클릭합니다.
  - **Prevention(**방지**)** - 트리거된 차단 규칙은 이벤트(경고)를 생성하고 연결을 삭제합니다.
  - **Detection(**탐지**)** - 트리거된 차단 규칙 알림입니다.

    탐지를 시작하기 전에 예방을 위해 탐지 모드를 선택할 수 있습니다. 예를 들어, 예방 모드를 선택하기 전에 차단 규칙이 경고만 할 수 있도록 하여 많은 오탐을 유발하는 규칙을 식별할 수 있습니다.

  참고 검사 모드는 정책의 Snort 3 버전에 대해서만 변경됩니다. 기존 검사 모드는 Snort 2 버전에서 그대로 유지됩니다.

- **Rule Action(**규칙 작업**)** 수정 - 규칙 작업을 수정하려면 다음 중 하나를 선택합니다.
  - 대량 수정 - 하나 이상의 규칙을 선택한 다음 **Rule Action(**규칙 작업**)** 드롭다운 목록에서 필요한 작업을 선택하고 **Save(**저장**)**를 클릭합니다.

    참고 대량 규칙 작업 변경은 처음 500개 규칙에 대해서만 지원됩니다.

  - 단일 규칙 수정 - **Rule Action(**규칙 작업**)** 열의 드롭다운 상자에서 규칙에 대한 작업을 선택합니다.

  참고 규칙 작업은 다음과 같습니다.
    - **Block(**차단**)** - 이 규칙이 트래픽과 일치할 경우, 이벤트를 생성하고 연결도 삭제합니다.
    - **Alert(**알림**)** - 이 규칙이 트래픽과 일치할 경우, 이벤트를 생성하지만 연결을 삭제하지는 않습니다.
    - **Disabled(**비활성화됨**)** - 트래픽을 이 규칙과 일치시키지 않습니다. 아무런 이벤트도 생성되지 않습니다.
    - **Revert to default(**기본값으로 되돌리기**)** - 시스템 기본 작업으로 되돌립니다.

- 검색 규칙 - 검색 필드를 사용하여 표시를 필터링합니다. GID, SID 또는 참조 정보를 입력할 수 있습니다. 예를 들어 GID:1; SID:9621은 1:962 규칙만 표시하고, SID:9621,9622,9623은 서로 다른 SID의 여러 규칙을 표시합니다. 또한 다음 옵션 중 하나를 선택할 수 있습니다.

- **Action = Alert** 또는 **Action: Block** 필터 적용
- **Disabled Rules** 필터 적용
- **Custom/User Defined Rules** 표시
- GID, SID 또는 GID:SID로 필터링
- cve로 필터링
- 코멘트로 필터링

- Search Rule Groups(규칙 그룹 검색) - 규칙 그룹을 검색할 키워드를 입력하거나 검색 창 아래에서 다음 사전 설정 필터 옵션을 선택합니다.
  - Excluded(제외됨) - 제외된 규칙 그룹의 경우
  - Included(포함) - 포함된 규칙 그룹의 경우
  - Overriden(재정의됨) - 재정의된 규칙이 있는 규칙 그룹의 경우

- Set the security level for a rule group(규칙 그룹의 보안 레벨 설정) - 왼쪽 창에서 필요한 규칙 그룹으로 이동하여 선택합니다. 규칙 그룹의 **Security Level(**보안 레벨**)** 옆에 있는 **Edit(**수정**)**을 클릭하여 시스템 정의 규칙 설정에 따라 보안 수준을 높이거나 낮춥니다.

  FMC는 설정된 보안 레벨에 대해 규칙 그룹의 규칙에 대한 작업을 자동으로 변경합니다. 보안 레벨을 변경할 때마다 **Preset Filters(**사전 설정 필터**)**에서 Block Rules(차단 규칙) 및 Disabled Rules(비활성화 규칙)의 변경 사항을 확인합니다.

- View filtered rules(필터링된 규칙 보기) - 사전 설정 필터를 선택하여 알림, 차단, 비활성화 또는 재정의로 설정된 규칙을 봅니다.

  재정의된 규칙은 규칙 작업이 기본 작업에서 다른 작업으로 변경된 규칙을 나타냅니다. 변경되면 원래 기본 작업으로 다시 변경하더라도 규칙 작업 상태가 재정의됩니다. 그러나 **Rule Action(**규칙 작업**)** 드롭다운 목록에서 **Revert to default(**기본값으로 되돌리기**)**를 선택하면 재정의됨 상태가 제거됩니다.

  Advanced Filters(고급 필터**)**는 LSP(Lightweight Security Package) 릴리스, 침입 분류 및 Microsoft 취약성을 기반으로 하는 필터 옵션을 제공합니다.

- Include or exclude Rule Groups(규칙 그룹 포함 또는 제외) - 표시되는 규칙 그룹은 시스템에서 제공하는 기본 침입 정책과 연결된 기본 규칙 그룹입니다. 침입 정책에서 규칙 그룹을 포함하거나 제외할 수 있습니다. 제외된 규칙 그룹은 침입 정책에서 제거되며 해당 규칙은 트래픽에 적용되지 않습니다. 정책에서 규칙을 적용하려면 FMC에 업로드된 사용자 지정 규칙을 포함해야 합니다. FMC의 사용자 지정 규칙 업로드에 대한 자세한 내용은 사용자 지정 규칙 업로드 항목을 참조하십시오.

  규칙 그룹을 제외하려면 다음과 같이 합니다.

  1. Rule Groups(규칙 그룹) 창을 탐색하고 규칙 그룹을 선택합니다.
  2. 오른쪽 창에서 **Exclude(**제외**)** 링크를 클릭합니다.
  3. 필요에 따라 규칙 그룹의 규칙 재정의를 기본 설정으로 되돌리려면 **Do you want to remove rule overrides?(**규칙 재정의를 제거하시겠습니까**?)** 체크 박스를 선택합니다.

참고 이 체크 박스는 재정의된 규칙이 있는 경우에만 표시됩니다.

4. **Exclude(**제외**)**를 클릭합니다.

업로드된 사용자 지정 규칙이 있는 새 규칙 그룹 또는 이전에 제외된 규칙 그룹을 포함하려면 다음과 같이 합니다.

1. Rule Groups(규칙 그룹) 검색 창 옆에 있는 **Add(**추가**)**( )를 클릭합니다.
2. 해당 규칙 그룹 옆의 체크 박스를 선택하여 추가할 모든 규칙 그룹을 선택합니다.
3. **Save(**저장**)**를 클릭합니다.

- View rule documentation(규칙 문서 보기) - 규칙 ID 또는 규칙 문서 아이콘을 클릭하여 규칙에 대한 TALOS 문서를 표시합니다.
- View a rule message(규칙 메시지 보기) - 규칙 세부 정보를 보려면 규칙 행의 확장 화살표( ) 아이콘을 클릭합니다.
- Add rule comments(규칙 코멘트 추가) - 규칙에 대한 코멘트를 추가하려면 Comments(코멘트) 열 아래의 **Comment(**코멘트**)**( )를 클릭합니다.

참고
- 기본 정책을 변경하려면 침입 정책의 기본 정책 변경, 6 페이지 항목을 참조하십시오.
- 모든 변경 사항이 즉시 저장됩니다. 변경 사항을 저장하는 데 추가 작업이 필요하지 않습니다.

다음에 수행할 작업

컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 9 페이지를 참고하십시오.

침입 정책의 기본 정책 변경

다른 시스템 제공 정책 또는 맞춤형 정책을 기본 정책으로 선택할 수 있습니다.

최대 다섯 개의 사용자 지정 정책을 묶을 수 있는데, 다섯 중 넷은 이전에 만들어진 다른 넷 중 하나를 기본 정책으로 사용하는 것이며, 다섯 번째는 반드시 시스템이 제공하는 정책을 기본 정책으로 사용해야 합니다.

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

단계 **2** 구성하려는 침입 정책 옆에 있는 **Edit(**수정**)**( )을 클릭합니다.

단계 **3** **Base Policy(**기본 정책**)** 드롭다운 목록에서 정책을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

컨피그레이션 변경사항을 구축합니다. 를 참고하십시오.

Snort 2 버전과 Snort 3 버전 침입 정책의 검사 모드 변경

기존 침입 정책에서 다른 검사 모드를 사용하도록 선택할 수 있습니다. 변경 사항은 성공적인 구축 후 디바이스에 적용됩니다. Snort 2 버전과 Snort 3 버전 침입 정책의 검사 모드를 변경하려면 이 항목에 나온 단계를 수행합니다.

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

단계 **2** 변경하려는 침입 정책 옆에 있는 **Edit(**수정**)**( )을 클릭합니다.

단계 **3** 정책에 적용할 **Inspection Mode(**검사 모드**)**를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 9 페이지를 참고하십시오.

침입 정책 관리

Intrusion Policy(침입 정책) 페이지(**Policies(**정책**)** > **Intrusion(**침입**)**)에서 다음 정보와 함께 현재의 사용자 지정 침입 정책을 볼 수 있습니다.

- 정책이 최종 수정된 시간과 날짜(로컬 시간) 및 정책을 수정한 사용자
- 트래픽을 검사하기 위해 침입 정책을 사용하는 액세스 제어 정책 및 디바이스의 유형
- 정책에 저장되지 않은 변경 사항이 있는지 여부 및 현재 정책을 수정하고 있는 사람에 관한 정보
- 다중 도메인 구축에서 정책이 생성된 도메인

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

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

단계 **2** 침입 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다(최신 버전의 *Firepower Management Center* 구성 가이드에 있는 정책 비교 항목 참조).
- 생성 - **Create Policy(**정책 생성**)**를 클릭합니다(사용자 지정 Snort 3 침입 정책 생성 , 3 페이지 참조).

- 삭제 - 삭제하려는 정책 옆에 있는 삭제( )를 클릭합니다. 다른 사용자가 정책 변경 사항을 저장하지 않은 경우, 시스템은 확인하라는 메시지를 표시하고 사용자에게 알립니다. **OK(**확인**)**를 클릭하여 확인합니다.

  컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

- 침입 정책 세부 정보 수정 - 수정하려는 정책 옆에 있는 수정( )을 클릭합니다. 침입 정책의 **Name(**이름**)**, **Inspection Mode(**검사 모드**)** 및 **Base Policy(**기본 정책**)**를 수정할 수 있습니다.

- 침입 정책 설정 수정 - **Snort 3 Version(Snort 3** 버전**)**을 클릭합니다(Snort 3 침입 정책 편집, 4 페이지 참조).

- 내보내기 - 다른 Firepower Management Center에서 가져오기 위해 침입 정책을 내보내려는 경우 Export(내보내기)를 클릭합니다(최신 버전의 *Firepower Management Center* 구성 가이드에 있는 구성 내보내기 항목 참조).

- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다(컨피그레이션 변경 사항 구축, 9 페이지 참조).

- 보고서 - **Report(**보고서**)**를 클릭합니다(최신 버전의 *Firepower Management Center* 구성 가이드에 있는 현재 정책 보고서 생성 항목 참조).

침입 방지를 수행하는 액세스 제어 규칙 설정

액세스 제어 정책에는 침입 정책과 관련된 여러 액세스 제어 규칙이 포함될 수 있습니다. 모든 Allow or Interactive Block(허용 또는 인터랙티브 차단) 액세스 제어 규칙에 대해 침입 검사를 구성할 수 있습니다. 이를 통해 트래픽이 최종 대상에 도달하기 전에 네트워크 상에 있는 다양한 유형의 트래픽에 대해 다양한 침입 검사 프로파일과 맞춰볼 수 있습니다.

시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 연결된 변수 집합을 사용합니다. 집합의 변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책 내 변수를 사용하여 규칙 삭제 및 동적 규칙 상태의 IP 주소를 나타낼 수 있습니다.

팁 시스템에서 제공한 침입 정책을 사용하더라도 Cisco는 네트워크 환경을 정확하게 반영할 수 있도록 시스템의 침입 변수를 구성할 것을 강력히 권장합니다. 최소한 기본값 집합의 기본 변수라도 수정하시기 바랍니다.

시스템이 제공하는 침입 정책 및 사용자 정의 침입 정책의 이해

Cisco는 Firepower System에서 여러 침입 정책을 제공합니다. 시스템이 제공하는 침입 정책을 사용하여 Cisco Talos(Talos Intelligence Group)의 경험을 활용할 수 있습니다. Talos는 이 정책에 대해 침입 및 전처리 규칙 상태를 설정할 뿐만 아니라 고급 설정의 초기 구성을 제공합니다. 사용자는 시스템이 제공하는 정책을 있는 그대로 사용할 수도 있고, 이를 맞춤형 정책을 위한 기반으로 사용할 수도 있습니다. 맞춤형 정책을 구축하면 사용자 환경에서 시스템의 성능을 개선할 수 있으며, 사용자 네트워크에서 발생하는 악의적인 트래픽 및 정책 위반을 집중적으로 확인할 수 있습니다.

연결 및 침입 이벤트 로깅

액세스 제어 규칙에 의해 호출된 침입 정책이 침입을 탐지하고 침입 이벤트를 생성할 경우, 해당 이벤트는 Firepower Management Center에 저장됩니다. 시스템은 또한 액세스 제어 규칙의 기록 구성에 관계없이 침입이 발생한 연결의 종료를 Firepower Management Center 데이터베이스에 자동으로 기록합니다.

액세스 제어 규칙 설정 및 침입 정책

단일한 액세스 제어 정책에서 사용할 수 있는 고유한 침입 정책의 수는 대상 디바이스의 모델에 따라 다르며, 성능이 뛰어난 디바이스일수록 더 많은 정책을 처리할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 쌍은 하나의 정책으로 계산됩니다. 다양한 침입 정책-변수 집합 쌍을 Allow(허용) 및 Interactive Block(인터랙티브 차단) 규칙(및 기본 작업)에 연결할 수 있지만 대상 디바이스에 구성된 대로 검사를 수행할 수 있는 리소스가 부족한 경우, 액세스 제어 정책을 구축할 수 없습니다.

침입 방지 수행을 위한 액세스 제어 규칙 구성

이 작업을 수행하려면 관리자, 액세스 관리자 또는 네트워크 관리자 여야합니다.

단계 **1** 액세스 제어 정책 편집기에서 새 규칙을 생성하거나 기존 규칙을 수정합니다. 최신 버전의 *Firepower Management Center* 구성 가이드에 있는 액세스 제어 규칙 구성 요소 항목을 참조하십시오.

단계 **2** 규칙 작업이 **Allow(**허용**)**, **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 초기화**)**으로 설정되어 있는지 확인합니다.

단계 **3** **Inspection(**검사**)**을 클릭합니다.

단계 **4** 시스템이 제공하는 정책 또는 사용자 지정 침입 정책을 선택하거나 **None(**없음**)**을 선택하여 액세스 제어 규칙과 일치하는 트래픽에 대한 침입 검사를 비활성화합니다.

단계 **5** 침입 정책에 관련된 변수 집합을 변경하려면 **Variable Set(**변수 집합**)** 드롭다운 목록에서 값을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **7** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

컨피그레이션 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축, 9 페이지를 참고하십시오.

컨피그레이션 변경 사항 구축

컨피그레이션을 변경한 후 해당하는 디바이스에 구축합니다.

참고 이 항목에서는 구성 변경 사항을 구축하는 기본 단계에 대해 설명합니다. 최신 버전의 *Firepower Management Center* 구성 가이드에서 구성 변경 사항 구축 항목을 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 컨피그레이션을 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** Firepower Management Center 메뉴 모음에서 **Deploy(**구축**)**를 클릭한 다음 **Deployment(**구축**)**를 선택합니다.

GUI 페이지에는 만료된 컨피그레이션이 보류중인 디바이스가 나열됩니다.

- **Modified By(**수정 주체**)** 열에는 정책 또는 개체를 수정한 사용자가 나열됩니다. 디바이스 목록을 확장하면 각 정책 목록에 대해 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 열의 항목이 비어 있으면 구축 중에 해당 디바이스에서 트래픽 검사가 중단되지 않음을 나타냅니다.

- 마지막 수정 시간 열은 컨피그레이션을 마지막으로 변경한 시간을 나타냅니다.
- **Preview(**미리보기**)** 열에서는 다음 구축에 대한 변경 사항을 미리 볼 수 있습니다.
- **Status(**상태**)** 열은 각 구축의 상태를 제공합니다.

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

- Search(검색)-검색 상자에서 디바이스 이름, 유형, 도메인, 그룹 또는 상태를 검색합니다.
- Expand(확장)-구축할 디바이스 별 컨피그레이션 변경 사항을 보려면 확장 화살표(›)을 클릭합니다.

디바이스 확인란을 선택하면 디바이스 아래에 나열된 디바이스에 대한 모든 변경 사항이 푸시되어 구축됩니다. 그러나 정책 선택( )를 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(컨피그레이션을 구축하면 Firepower Threat Defense 디바이스에서 검사가 중단되며 트래픽도 중단될 수 있는 경우) 확장된 목록에 중단을 야기하는 특정 컨피그레이션이 검사 중단( )으로 표시됩니다.
- 인터페이스 그룹, 보안 영역 또는 개체가 변경되면 영향을 받는 디바이스는 FMC (Firepower Management Center)에서 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 FMC의 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 컨피그레이션을 재구축합니다.

다음에 수행할 작업

구축 중에 어떤 이유로든 구축 장애가 발생하는 경우 해당 장애가 트래픽에 영향을 미칠 수 있습니다. 그러나 특정 조건에 따라 달라집니다. 구축에 특정 컨피그레이션이 변경된 경우 구축 장애로 인해 트래픽이 중단될 수 있습니다. 자세한 내용은 최신 버전의 *Firepower Management Center* 구성 가이드에 있는 구성 변경 사항 구축 항목을 참조하십시오.