Snort 2에서 Snort 3로 마이그레이션

버전 7.0부터, Snort 3은 Management Center에 새로운 Threat Defense 구축에 대해 기본 검사 엔진입니다. 아직 Snort 2 검사 엔진을 사용 중이라면 지금 바로 Snort 3으로 전환하여 탐지 및 성능을 개선합니다.

Threat Defense을 버전 7.2~7.6으로 업그레이드하면 적격 Snort 2 디바이스도 Snort 3으로 업그레이드됩니다. 맞춤형 침입 또는 네트워크 분석 정책을 사용하기 때문에 부적합한 디바이스의 경우 여기에 설명된 대로 수동으로 Snort 3으로 업그레이드합니다.

개별 디바이스를 다시 예전으로 전환할 수는 있지만, 그렇게 해서는 안 됩니다.Snort 2는 향후 릴리스에서 더 이상 사용되지 않으며 결국 Threat Defense 업그레이드할 수 없게 됩니다.

Snort 3 검사 엔진

Snort 3는 버전 7.0 이상의 새로 등록된 Threat Defense 디바이스에 대한 기본 검사 엔진입니다. 그러나 하위 버전의 Threat Defense 디바이스의 경우 Snort 2가 기본 검사 엔진입니다. 매니지드 Threat Defense 디바이스를 버전 7.0 이상으로 업그레이드할 경우 검사 엔진은 Snort 2에 남아 있습니다. 버전 7.0 이상의 업그레이드된 Threat Defense 에서 Snort 3를 사용하려면 명시적으로 활성화해야 합니다. Snort 3가 디바이스의 검사 엔진으로 활성화되면 액세스 제어 정책을 통해 디바이스에 적용된 Snort 3 버전이 활성화되어 디바이스를 통과하는 모든 트래픽에 적용됩니다.

필요한 경우 Snort 버전을 전환할 수 있습니다. Snort 2와 Snort 3 침입 규칙은 매핑되며, 이 매핑은 시스템에서 제공됩니다. 그러나 Snort 2 및 Snort 3에서는 모든 침입 규칙의 일대일 매핑을 찾을 수 없습니다. Snort 2에서 규칙에 대한 규칙 작업을 변경한 경우 Snort 3로 전환하면 해당 변경 사항이 유지되지 않습니다. 변경 사항을 유지하려면 Snort 2를 Snort 3와 동기화해야 합니다. 동기화에 대한 자세한 내용은 Snort 2 규칙과 Snort 3 동기화 , 6 페이지 항목을 참조하십시오.

네트워크 분석 및 침입 정책 사전 요건

Snort 검사기 엔진이 침입 및 악성코드 분석을 위해 트래픽을 처리하도록 허용하려면 Threat Defense 디바이스에 대해 활성화된 IPS 라이선스가 있어야 합니다.

네트워크 분석, 침입 정책을 관리하고 마이그레이션 작업을 수행하려면 관리자 사용자여야 합니다.

Snort 2에서 Snort 3로 마이그레이션하는 방법

Snort 2에서 Snort 3로 마이그레이션하려면 Threat Defense 디바이스의 검사 엔진을 Snort 2에서 Snort 3로 전환해야 합니다.

다음 테이블에는 요구 사항에 따라 Snort 2에서 Snort 3로 디바이스를 마이그레이션하는 작업이 나열되어 있습니다.

단계	작업	절차 링크
1	Sntit 3 활성화	• 개별 디바이스에서 Snort 3 활성화, 3 페이지 • 여러 디바이스에서 Snort 3 활성화, 3 페이지
2	Snort 2 사용자 지정 규칙을 Snort 3로 변환	• 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 4 페이지 • 단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 5 페이지
3	Snort 2 규칙과 Snort 3 동기화	Snort 2 규칙과 Snort 3 동기화 , 6 페이지

Snort 2에서 Snort 3로 마이그레이션하기 위한 사전 요건

다음은 디바이스를 Snort 2에서 Snort 3로 마이그레이션하기 전에 고려해야 할 권장 사전 요건입니다.

- 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.
- 침입 정책을 복제합니다. 이를 위해서 침입 정책의 복사본을 생성하기 위한 기본 정책으로 기존 정책을 사용할 수 있습니다. **Intrusion Policies(**침입 정책**)** 페이지에서 **Create Policy(**정책 생성**)**를 클릭하고 **Base Policy(**기본 정책**)** 드롭다운 목록에서 기존 침입 정책을 선택합니다.

개별 디바이스에서 Snort 3 활성화

중요 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 디바이스를 클릭하여 디바이스 홈 페이지로 이동합니다.

참고 디바이스가 Snort 2 또는 Snort 3로 나타나 디바이스의 현재 버전을 표시합니다.

단계 3 **Device(**디바이스**)** 탭을 클릭합니다.

단계 4 Inspection Engine(검사 엔진) 섹션에서 **Upgrade(**업그레이드**)**를 클릭합니다.

참고 Snort 3을 비활성화하려면 Inspection Engine(검사 엔진) 섹션에서 **Revert to Snort 2(Snort 2**로 되돌리기**)**를 클릭합니다.

단계 5 **Yes(**예**)**를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 참고, 구성 변경 사항 구축, 7 페이지.

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

여러 디바이스에서 Snort 3 활성화

여러 디바이스에서 Snort 3를 활성화하려면 모든 필수 Threat Defense 디바이스가 버전 7.0 이상인지 확인하십시오.

중요 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 Snort 3를 활성화하거나 비활성화할 모든 디바이스를 선택합니다.

참고 디바이스가 Snort 2 또는 Snort 3로 나타나 디바이스의 현재 버전을 표시합니다.

단계 3 **Select Bulk Action(**대량 작업 선택**)** 드롭다운 목록을 클릭하고 **Upgrade to Snort 3(Snort 3**로 업그레이드**)**를 선택합니다.

단계 4 **Yes(예)**를 클릭합니다.

다음에 수행할 작업

디바이스에서 변경 사항을 구축합니다. 참고, 구성 변경 사항 구축, 7 페이지.

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

Snort 2 사용자 지정 IPS 규칙을 Snort 3로 변환

서드파티 벤더의 규칙 집합을 사용하는 경우 해당 벤더에 연락하여 규칙이 Snort 3로 성공적으로 변환되는지 확인하거나 기본적으로 Snort 3용으로 작성된 대체 규칙 집합을 얻으십시오. 직접 작성한 사용자 지정 규칙이 있는 경우 변환 전에 Snort 3 규칙을 작성하는 방법을 숙지하여 변환 후 Snort 3 탐지를 최적화하도록 규칙을 업데이트할 수 있습니다. Snort 3의 규칙 작성에 대해 자세히 알아보려면 아래 링크를 참조하십시오.

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Snort 3 규칙에 대해 자세히 알아보려는 경우 https://blog.snort.org/에서 다른 블로그를 참조할 수 있습니다.

시스템에서 제공하는 툴을 사용하여 Snort 2 규칙을 Snort 3 규칙으로 변환하려면 다음 절차를 참조하십시오.

- 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 4 페이지
- 단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 5 페이지

중요 Snort 2 NAP(네트워크 분석 정책) 설정은 Snort3에 자동으로 복사될 수 없습니다. NAP 설정은 Snort 3에서 수동으로 복제해야 합니다.

모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 변환

단계 1 **Objects(개체)** > **Intrusion Rules(침입 규칙)**를 선택합니다.

단계 2 **Snort 3 All Rules(Snort 3 모든 규칙)** 탭을 클릭합니다.

단계 3 왼쪽 창에 **All Rules(모든 규칙)**가 선택되어 있는지 확인합니다.

단계 4 **Tasks(작업)** 드롭다운 목록을 클릭하고 다음을 선택합니다.

- **Convert Snort 2 rules and import(Snort 2 규칙 변환 및 가져오기)** - 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 자동 변환하고 Management Center에 Snort 3 사용자 지정 규칙으로 가져옵니다.

- **Convert Snort 2 rules and download(Snort 2** 규칙 변환 및 다운로드**)** - 모든 침입 정책의 모든 Snort 2 사용자 지정 규칙을 Snort 3로 자동 변환하고 로컬 시스템에 다운로드합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

참고
- 앞 단계에서 **Convert and import(**변환 및 가져오기**)**를 선택한 경우 변환된 모든 규칙은 **Local Rules(**로컬 규칙**)** 아래 새로 생성된 규칙 그룹 **All Snort 2 Converted Global(**모든 **Snort 2** 변환 전역**)**에 저장됩니다.
- 앞 단계에서 **Convert and download(**변환 및 다운로드**)**를 선택한 경우 규칙 파일을 로컬에 저장합니다. 다운로드한 파일에서 변환된 규칙을 검토하고 나중에 규칙 그룹에 사용자 지정 규칙 추가의 단계에 따라 업로드할 수 있습니다.

추가 지원 및 정보는 Snort 2 규칙을 Snort 3로 변환 비디오를 참조하십시오.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 7 페이지를 참고하십시오.

단일 침입 정책의 Snort 2 사용자 지정 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.

단계 **3** 침입 정책의 **Sync(**동기화**)** 아이콘( )을 클릭합니다.

참고 Snort 2 버전과 Snort 3 버전의 침입 정책이 동기화된 경우 **Sync(**동기화**)** 아이콘이 녹색( )으로 표시됩니다. 이는 변환할 사용자 지정 규칙이 없음을 나타냅니다.

단계 **4** 요약을 읽고 **Custom Rules(**사용자 지정 규칙**)** 탭을 클릭합니다.

단계 **5** 다음을 선택합니다.

- **Import converted rules to this policy(**변환된 규칙을 이 정책으로 가져오기**)** - 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환하고 Management Center에 Snort 3 사용자 지정 규칙으로 가져옵니다.
- **Download converted rules(**변환된 규칙 다운로드**)** - 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환하고 로컬 시스템에 다운로드합니다. 다운로드한 파일에서 변환된 규칙을 검토하고 나중에 업로드 아이콘을 클릭하여 파일을 업로드할 수 있습니다.

단계 **6** **Re-Sync(**재동기화**)**를 클릭합니다.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 7 페이지를 참고하십시오.

Snort 2 및 Snort 3 기본 정책 매핑 보기

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

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

단계 3 **IPS Mapping(IPS** 매핑**)**을 클릭합니다.

단계 4 **IPS Policy Mapping(IPS** 정책 매핑**)** 대화 상자에서 **View Mappings(**매핑 보기**)**를 클릭하여 Snort 3에서 Snort 2로의 침입 정책 매핑을 확인합니다.

단계 5 **OK(**확인**)**를 클릭합니다.

Snort 2 규칙과 Snort 3 동기화

Snort 2 버전 설정과 사용자 지정 규칙이 유지되고 Snort 3에 전달되도록 하기 위해 Management Center는 동기화 기능을 제공합니다. 동기화는 Snort 2 규칙 재정의 설정 및 사용자 지정 규칙에 도움이 됩니다. 이는 지난 몇 개월 또는 몇 년간 Snort 3 버전에서 복제하도록 변경되거나 추가되었을 수 있습니다. 이 유틸리티를 사용하면 Snort 2 버전 정책 구성을 Snort 3 버전과 동기화하여 비슷한 커버리지로 시작할 수 있습니다.

Management Center를 6.7 이하 버전에서 7.0 이상 버전으로 업그레이드하는 경우, 시스템에서 구성을 동기화합니다. Management Center가 7.0 이상 버전인 경우 상위 버전으로 업그레이드할 수 있으며, 업그레이드 중에는 콘텐츠가 동기화되지 않습니다.

디바이스를 Snort 3로 업그레이드하기 전에, Snort 2 버전을 변경하는 경우 이 유틸리티를 통해 Snort 2 버전에서 Snort 3 버전으로의 최신 동기화를 수행하여 유사한 커버리지로 시작할 수 있습니다.

참고 Snort 3로 전환한 후에는 정책의 Snort 3 버전을 독립적으로 관리하고 이 유틸리티를 일반 작업으로 사용하지 않는 것이 좋습니다.

중요

- Snort 2 규칙 재정의와 사용자 지정 규칙이 Snort 3에 복사되기만 하며 그 반대로는 복사되지 않습니다. Snort 2 및 Snort 3에서는 모든 침입 규칙의 일대일 매핑을 찾을 수 없습니다. 다음 절차를 수행할 때 두 버전에 있는 규칙에 대한 규칙 작업의 변경 사항이 동기화됩니다.
- 동기화 시 사용자 지정 규칙 또는 시스템 제공 규칙의 임계값 및 억제 설정이 Snort 2에서 Snort 3로 마이그레이션되지 않습니다.

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

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

단계 **3** **Snort 3** 동기화 상태 표시를 클릭합니다.

단계 **4** 동기화되지 않은 침입 정책을 식별합니다.

단계 **5** **Sync(**동기화**)** 아이콘( )을 클릭합니다.

참고 Snort 2 버전과 Snort 3 버전의 침입 정책이 동기화된 경우 **Sync(**동기화**)** 아이콘이 녹색( )으로 표시됩니다.

단계 **6** 요약을 읽고 필요한 경우 요약 사본을 다운로드합니다.

단계 **7** **Re-Sync(**재동기화**)**를 클릭합니다.

참고
- 동기화된 설정은 Snort 3 침입 엔진이 디바이스에 적용되고 구축이 성공한 경우에만 적용됩니다.
- Snort 2 사용자 지정 규칙은 시스템 제공 툴을 사용하여 Snort 3로 변환할 수 있습니다. Snort 2 사용자 지정 규칙이 있는 경우 Custom Rules(사용자 지정 규칙) 탭을 클릭하고 화면의 지침에 따라 규칙을 변환합니다. 자세한 내용은 단일 침입 정책의 Snort 2 사용자 지정 규칙을 Snort 3로 변환, 5 페이지를 참고하십시오.

다음에 수행할 작업

구성 변경사항을 구축합니다. 구성 변경 사항 구축, 7 페이지를 참고하십시오.

구성 변경 사항 구축

컨피그레이션을 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 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** 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** 컨피그레이션 변경 사항을 구축할 디바이스를 식별하여 선택합니다.

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

  디바이스 옆의 확인란을 선택하면 디바이스에 대해 수행되고 디바이스 아래에 나열된 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(구축하면 Threat Defense 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 컨피그레이션을 재구축합니다.

다음에 수행할 작업

구축 중에 구축 장애가 발생하는 경우 해당 장애가 트래픽에 영향을 미칠 수 있습니다. 그러나 특정 조건에 따라 달라집니다. 구축에 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.