정책 관리

다음 주제는 Firepower Management Center의 다양한 정책을 관리하는 방법에 대해 설명합니다.

정책 관리를 위한 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- Network Admin(네트워크 관리자)
- 보안 승인자

정책 구축

구축 설정을 완료하거나 구성을 변경한 뒤 영향받는 디바이스에 변경 사항을 구축해야 합니다. 메시지 센터에서 배포 상태를 확인할 수 있습니다.

다음 구성 요소 업데이트를 배포합니다.

- 디바이스 및 인터페이스 컨피그레이션
- 장치 관련 정책: NAT, VPN, QoS, 플랫폼 설정
- 액세스 제어 및 관련 정책: DNS, 파일, ID, 침입, 네트워크 분석, SSL
- 네트워크 검색 정책
- 침입 규칙 업데이트
- 설정 및 해당 요소와 관련된 개체

배포 작업을 예약하거나 침입 규칙 업데이트를 가져올 때 시스템 배포로 설정하여 자동으로 구축 시스템을 구성할 수 있습니다. 자동화 정책을 구축하는 것은 특히 침입 및 네트워크 분석에 대한 시스템 제공 기본 정책을 수정하는 침입 규칙 업데이트를 허용하는 경우에 유용합니다. 또한 침입 규칙 업데이트는 액세스 제어 정책의 고급 전처리 및 성능 옵션에 대한 기본값을 변경할 수 있습니다.

다중 도메인 구축에서 사용자 계정에 속해있는 모든 도메인에 대한 변경 사항을 구축할 수 있습니다.

- 상위 도메인이 모든 하위 도메인에 동시에 변경 사항을 구축하도록 전환합니다.
- 리프 도메인이 해당 도메인에만 변경 사항을 구축하도록 전환합니다.

구성 변경 사항 구축을 위한 모범 사례

다음은 컨피그레이션 변경 사항 구축을 위한 지침입니다.

인라인 구축과 패시브 구축 비교

수동으로 구축된 디바이스에 인라인 컨피그레이션을 적용하거나 인라인으로 구축된 디바이스에 수동 컨피그레이션을 적용하지 마십시오.

구축 시간 및 메모리 제한

구축 소요 시간은 다음을 비롯한 여러 요인에 따라 달라집니다.

- 디바이스로 전송하는 컨피그레이션. 예를 들어 차단할 보안 인텔리전스 항목의 수를 크게 늘리면 구축이 더 오래 걸릴 수 있습니다.
- 디바이스 모델 및 메모리. 메모리가 적은 디바이스에서는 구축이 더 오래 걸릴 수 있습니다. 예를 들어 Firepower 7010, 7020 또는 7030 디바이스 구축은 최대 5분이 소요될 수 있습니다.

디바이스의 기능을 초과하는 작업을 수행하지 마십시오. 대상 디바이스에서 지원하는 최대 규칙 또는 정책 수를 초과하면 경고가 표시됩니다. 최대치는 디바이스의 프로세서 수와 메모리뿐 아니라 정책 및 규칙의 복잡성과 같은 여러 가지 요인에 따라 달라집니다. 정책 및 규칙 최적화에 대한 정보는 액세스 제어 규칙 순서에 대한 모범 사례를 참조하십시오.

구축 중에 트래픽 흐름 및 검사 중단

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. Snort® 재시작 트래픽 동작, 17 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 20 페이지의 내용을 참조하십시오.

주의 중단의 영향이 가장 적은 시간이나 유지 보수 기간에 구축을 수행하는 것이 좋습니다.

애플리케이션 탐지기 자동 활성화

애플리케이션 제어를 수행할 때 필요한 탐지기를 비활성화할 경우 정책 구축 시 적절한 시스템 제공 탐지기가 자동으로 활성화됩니다. 시스템 제공 탐지기가 없으면 애플리케이션에 대해 가장 최근에 수정된 사용자 정의 탐지기가 활성화됩니다.

네트워크 검색 정책 변경이 있는 자산 재검색

네트워크 검색 정책에 대한 변경 사항을 구축할 때는 시스템이 모니터링되는 네트워크의 호스트에 대한 네트워크 맵에서 MAC 주소, TTL 및 홉 정보를 삭제한 후 다시 검색합니다. 또한, 영향을 받는 매니지드 디바이스는 아직 Firepower Management Center로 전송되지 않은 검색 데이터를 모두 삭제합니다.

관련 항목

Snort® 재시작 시나리오, 15 페이지

구축 상태

Deployment(구축) 페이지에서 **Status(**상태**)** 열은 각 디바이스의 구축 상태를 제공합니다. 구축이 진행 중인 경우 구축 진행률의 라이브 상태가 표시됩니다. 그렇지 않으면 다음 상태 중 하나가 표시됩니다.

- Pending(보류 중) - 구축할 디바이스에 변경 사항이 있음을 나타냅니다.
- Warnings or errors(경고 또는 오류) - 사전 구축 확인에서 구축에 대한 경고 또는 오류를 식별했으며 구축을 진행하지 않았음을 나타냅니다. 경고가 있는 경우 구축을 계속할 수 있지만 오류가 있는 경우에는 구축을 계속할 수 없습니다.

  참고 상태 열은 구축 페이지의 단일 사용자 세션에 대해서만 경고 또는 오류 상태를 제공합니다. 페이지에서 다른 페이지로 이동하거나 페이지를 새로 고치면 상태가 보류 중으로 변경됩니다.

- Failed(실패) - 이전 구축 시도가 실패했음을 나타냅니다. 세부 사항을 보려면 상태를 클릭합니다.
- In queue(대기열) - 구축이 시작되었으며 시스템이 아직 구축 프로세스를 시작하지 않았음을 나타냅니다.

• Completed(완료됨) - 구축이 성공적으로 완료되었음을 나타냅니다.

구축 견적

디바이스, 정책 또는 구성을 선택한 후에는 구축 페이지에서가 가견적 링크를 사용할 수 있습니다. 가견적 링크를 클릭하여 구축 기간의 가견적을 확인합니다. 소요 시간은 대략적인 가견적(약 70% 정확도)이며 구축에 소요되는 실제 시간은 몇 가지 시나리오에서 달라질 수 있습니다. 일부 FTD에 대한 구축은 예상 구축 기간을 참조하십시오. 가견적은 최대 20개의 FTD 디바이스를 구축할 때 신뢰할 수 있습니다.

가견적을 사용할 수 없으면 선택한 디바이스에서 첫 번째로 성공한 구축이 보류 중이므로 데이터를 사용할 수 없음을 나타냅니다. 이 상황은 FMC 버전 업그레이드 후 또는 새로 설치한 후에 발생할 수 있습니다.

참고 가견적은 휴리스틱 기술을 기반으로 하므로 대량 정책 변경(대량 정책 마이그레이션의 경우) 및 선택적 구축에 대한 가견적이 올바르지 않으며 신뢰할 수 없습니다.

구축 미리보기

미리보기에서는 디바이스에 구축할 모든 정책 및 개체 변경 사항의 스냅샷을 제공합니다. 정책 변경 사항에는 새 정책, 기존 정책의 변경 사항 및 삭제된 정책이 포함됩니다. 개체 변경 사항에는 정책에 사용되는 추가 및 수정된 개체가 포함됩니다. 사용되지 않는 개체 변경 사항은 디바이스에 구축되지 않으므로 표시되지 않습니다.

Deployment(구축) 페이지에서 Preview(미리보기) 열은 나열된 각 디바이스에 대한 미리보기( ) 아이콘을 제공합니다. 미리보기 아이콘을 클릭하면 FMC에서 모든 정책 및 개체 변경 사항을 나열하는 UI 페이지를 표시합니다. 미리보기 페이지의 왼쪽 창에는 디바이스에서 변경된 모든 정책 유형이 트리 구조로 구성되어 있습니다. 오른쪽 창에는 정책의 모든 추가, 변경 또는 삭제된 항목이나 왼쪽 창에서 선택한 개체가 나열됩니다. 오른쪽 창에 있는 2개의 열은 마지막으로 구축한 구성 설정(**Version on Device(**디바이스 버전**)** 열)과 구축 예정인 변경 사항(**Version on FMC(FMC** 버전**)** 열)을 제공합니다. 마지막으로 구축된 구성 설정은 디바이스가 아니라 FMC에 마지막으로 저장된 구축의 스냅샷에서 가져옵니다. 설정의 배경색은 페이지 오른쪽 상단에 있는 범례에 따라 색상으로 구분됩니다.

참고

- 구축 변경 사항을 미리 보려면 Firepower REST API에서 Firepower Management Center에 액세스해야 합니다. REST API 액세스를 활성화하려면 REST API 액세스 활성화의 단계를 수행합니다.
- 미리보기에는 여러 정책 간 규칙의 재정렬이 표시되지 않습니다.
- 변경되지 않은 경우에도 인터페이스 또는 플랫폼 설정 정책을 처음 추가할 때 구성된 다른 설정과 함께 모든 기본값이 미리보기에 표시됩니다. 마찬가지로, 설정에 대한 고가용성 관련 정책 및 기본값은 변경되지 않은 경우에도 고가용성 쌍이 설정되거나 중단된 후 첫 번째 미리보기에 표시됩니다.
- 일부 개체의 경우, 미리보기가 지원되지 않습니다.
- 개체가 디바이스 또는 인터페이스와 연결된 경우에만 개체 추가 및 속성 변경 사항이 미리보기에 표시됩니다. 개체 삭제는 표시되지 않습니다.
- 다음 정책에 대해서는 미리보기가 지원되지 않습니다.
  - 고가용성
  - 네트워크 검색
  - 네트워크 분석
  - 디바이스 설정
  - Flex 설정

선택적 정책 구축

FMC를 사용하면 구축할 예정인 디바이스의 모든 변경 사항 목록에서 특정 정책을 선택하고 선택한 정책만 구축할 수 있습니다. 선택적으로, 다음 정책에 대해서만 구축을 사용할 수 있습니다.

- 액세스 제어 정책
- 침입 정책
- 악성코드 및 파일 정책
- DNS 정책
- ID 정책
- SSL 정책
- QoS 정책
- 사전 필터 정책
- 네트워크 검색
- NAT 정책

- 라우팅 정책

구축 페이지에서 디바이스별 설정 변경 사항을 보려 확장 화살표( )를 클릭하면 정책 선택( ) 아이콘이 표시됩니다. 정책 선택 아이콘을 사용하면 나열된 나머지 변경 사항을 구축하지 않고 보류하면서 구축할 개별 정책 또는 설정을 선택할 수 있습니다. 이 옵션은 FTD에만 사용할 수 있으며 센서에는 사용할 수 없습니다. 이 옵션을 통해 특정 정책 또는 설정에 대한 상호 의존적인 변경 사항을 볼 수도 있습니다. FMC는 정책 간(예: 액세스 제어 정책과 침입 정책 간), 공유 개체와 정책 간의 종속성을 동적으로 탐지합니다. 상호 의존적인 변경 사항은 상호 의존적인 구축 변경 사항을 식별할 수 있도록 색상 코드 태그를 사용하여 표시됩니다. 구축 변경 사항 중 하나를 선택하면 상호 의존적인 변경 사항이 자동으로 선택됩니다.

참고

- 공유 개체의 변경 사항을 구축할 때는 영향을 받는 정책도 함께 구축해야 합니다. 구축 중에 공유 개체를 선택하면 영향을 받는 정책이 자동으로 선택됩니다.
- 예약된 구축 및 REST API를 사용하는 구축의 경우에는 선택적 구축이 지원되지 않습니다. 이때는 모든 변경 사항을 완전히 구축하도록 선택할 수만 있습니다.
- 경고 및 오류에 대한 사전 구축 검사는 선택한 정책뿐만 아니라 오래된 모든 정책에 대해서도 수행됩니다. 따라서 경고 또는 오류 목록에는 선택 취소된 정책도 표시됩니다.
- 마찬가지로 Deployment(구축) 페이지의 **Inspect Interruption(**검사 중단**)** 열 표시는 선택한 정책뿐 아니라 모든 오래된 정책을 고려합니다. **Inspect Interruption(**검사 중단**)** 열에 대한 자세한 내용은 Firepower Threat Defense 디바이스의 재시작 경고의 내용을 참조하십시오.

선택적으로 정책을 구축하는 데는 몇 가지 제한 사항이 있습니다. 아래 테이블의 내용에 따라 선택적 정책 구축을 사용할 수 있는 시점을 파악하십시오.

표 *1:* 선택적 구축에 대한 제한 사항

유형	설명	시나리오
전체 구축	전체 구축은 특정 구축 시나리오에 필요하며, FMC는 이러한 시나리오에서 선택적 구축을 지원하지 않습니다. 이러한 시나리오에서 오류가 발생하는 경우, 디바이스에서 구축할 모든 변경 사항을 골라서 진행하도록 선택할 수 있습니다.	전체 구축이 필요한 시나리오는 다음과 같습니다. • FTD 또는 FMC를 업그레이드한 후 첫 번째 구축 • FTD를 복원한 후의 첫 번째 구축 • FTD 인터페이스 설정 수정 후 첫 번째 구축 • 가상 라우터 설정 수정 후 첫 번째 구축 • FTD 디바이스가 새 도메인(전역에서 하위 도메인으로 또는 하위 도메인에서 전역으로)으로 이전하는 경우

유형	설명	시나리오
연결된 정책 구축	FMC는 서로 연결된 상호 의존적인 정책을 식별합니다. 상호 연결된 정책 중 하나를 선택하면 나머지 상호 연결된 정책이 자동으로 선택됩니다.	연결된 정책이 자동으로 선택되는 시나리오는 다음과 같습니다. • 새 개체가 기존 정책과 연결된 경우 • 기존 정책의 개체가 수정된 경우 여러 정책이 자동으로 선택되는 시나리오는 다음과 같습니다. • 새 개체가 기존 정책과 연결되어 있고 동일한 개체가 이미 다른 정책과 연결되어 있으면 연결된 모든 정책이 자동으로 선택됩니다. • 공유 개체가 수정되면 연결된 모든 정책이 자동으로 선택됩니다.
상호 의존적 정책 변경(색상으로 구분된 태그를 사용하여 표시)	FMC는 정책 간 및 공유 개체와 정책 간의 종속성을 동적으로 탐지합니다. 개체 또는 정책의 상호 종속성은 색상으로 구분된 태그를 사용하여 표시됩니다.	색상으로 구분된 상호 의존적 정책 또는 개체가 자동으로 선택되는 시나리오는 다음과 같습니다. • 모든 오래된 정책에 상호 의존적인 변경 사항이 있는 경우 예를 들어, 액세스 제어 정책, 침입 정책 및 NAT 정책이 오래된 경우입니다. 액세스 제어 정책과 NAT 정책은 개체를 공유하므로 구축을 위해 모든 정책이 함께 선택됩니다. • 모든 오래된 정책이 하나의 개체를 공유하고 해당 개체가 수정된 경우

유형	설명	시나리오
액세스 정책 그룹 사양	액세스 정책 그룹 정책은 정책 표시 또는 숨기기( )를 클릭하면 **Access Policy Group(**액세스 정책 그룹**)** 아래의 미리보기 창에 함께 나열됩니다.	액세스 정책 그룹 정책에 대한 시나리오 및 예상되는 동작은 다음과 같습니다. • 액세스 제어 정책이 만료된 경우, 파일 그룹 및 침입 정책을 제외하고 이 그룹에 속한 다른 모든 오래된 정책은 액세스 제어 정책이 구축하도록 선택될 때 설정됩니다. 단, 액세스 제어 정책이 만료된 경우, 종속적인 변경이 없는 한 액세스 제어 정책의 선택 여부와 관계없이 침입 및 파일 정책을 개별적으로 선택하거나 선택을 취소할 수 있습니다. 예를 들어, 새 침입 정책이 액세스 제어 규칙에 할당된 경우, 종속 변경 사항이 있음을 나타내며, 둘 중 하나를 선택하면 액세스 제어 정책과 침입 정책이 모두 자동으로 선택됩니다. • 만료된 액세스 제어 정책이 없는 경우, 이 그룹의 다른 만료된 정책을 개별적으로 선택하여 구축할 수 있습니다.

컨피그레이션 변경 사항 구축

컨피그레이션을 변경한 후 해당하는 디바이스에 구축합니다. 컨피그레이션 변경 사항은 트래픽 흐름 및 검사 중단의 영향이 가장 적은 시간이나 유지 보수 기간에 구축하는 것이 좋습니다.

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. Snort® 재시작 트래픽 동작, 17 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 20 페이지의 내용을 참조하십시오.

시작하기 전에

- 구성 변경 사항 구축을 위한 모범 사례, 2 페이지에 설명되어 있는 지침을 검토합니다.
- 모든 매니지드 디바이스가 동일한 수정 버전의 보안 영역 개체를 사용하는지 확인합니다. 보안 영역 개체를 수정한 경우 동기화하려는 모든 디바이스에서 인터페이스에 대한 영역 설정을 수정하기 전에는 구성 변경 사항을 디바이스에 구축하지 마십시오. 모든 매니지드 디바이스에 동시에 구축해야 합니다. 보안 영역 개체의 수정 버전 동기화의 내용을 참조하십시오.

프로시저

단계 **1** Firepower Management Center 메뉴 모음에서 **Deploy(구축)**를 클릭한 다음 **Deployment(구축)**를 선택합니다.

GUI 페이지에는 오래된 상태의 구성이 보류중인 디바이스가 나열됩니다.

- **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 구성을 마지막으로 변경한 시간을 나타냅니다.
- **Preview(미리보기)** 열에서는 다음 구축에 대한 변경 사항을 미리 볼 수 있습니다. 자세한 내용은 구축 미리보기, 4 페이지를 참고하십시오.
- **Status(상태)** 열은 각 구축의 상태를 제공합니다. 자세한 내용은 구축 상태, 3 페이지를 참고하십시오.

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 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 구성을 선택할 수 있습니다. 자세한 내용은 선택적 정책 구축, 5 페이지 섹션을 참조해 주십시오.

선택적으로, 수정되지 않은 관련 정책을 선택적으로 보거나 숨기는 데 정책 표시 또는 숨기기( )을(를) 사용할 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** (선택 사항) 대략적인 구축 기간을 확인하려면 **Estimate(견적)**를 클릭합니다.

자세한 내용은 구축 견적, 4 페이지를 참조하십시오.

단계 **4** **Deploy(**구축**)**를 클릭합니다.

단계 **5** 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

- (선택 사항) 구축 상태를 모니터링합니다. 구축 메시지 보기를 참조하십시오.
- 구축에 실패하는 경우 구성 변경 사항 구축을 위한 모범 사례, 2 페이지를 참조하십시오.

관련 항목

Snort® 재시작 시나리오, 15 페이지

디바이스에 기존 구성을 재구축하십시오

관리되는 단일 디바이스에 기존의 (변경되지 않은) 구성을 강제 구축할 수 있습니다. 컨피그레이션 변경 사항은 트래픽 흐름 및 검사 중단의 영향이 가장 적은 시간이나 유지 보수 기간에 구축하는 것이 좋습니다.

⚠

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. Snort® 재시작 트래픽 동작, 17 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 20 페이지의 내용을 참조하십시오.

시작하기 전에

구성 변경 사항 구축을 위한 모범 사례, 2 페이지에 설명되어 있는 지침을 검토합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**을(를) 선택합니다.

단계 **2** 강제 구축을 원하는 디바이스 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 디바이스를 클릭합니다.

단계 **4** **General(**일반**)** 섹션 옆에 있는 수정( )을 클릭합니다.

단계 **5** 강제 구축( ) 버튼을 클릭합니다.

참고 강제 구축은 FTD에 구축할 정책 규칙의 완전한 생성을 포함하므로 일반 구축보다 시간이 더 오래 걸립니다.

단계 **6** **Deploy(**구축**)**를 클릭합니다.

시스템은 구축하려는 설정과 관련된 모든 오류나 경고를 식별합니다. 경고 상황을 해결하지 않고 계속하려면 **Proceed(**진행**)**를 클릭합니다. 그러나 시스템이 오류를 식별하는 경우 계속 진행할 수 없습니다.

다음에 수행할 작업

- (선택 사항) 구축 상태를 모니터링합니다. 구축 메시지 보기를 참조하십시오.
- 구축에 실패하는 경우 구성 변경 사항 구축을 위한 모범 사례, 2 페이지를 참조하십시오.

관련 항목

Snort® 재시작 시나리오, 15 페이지

구축 히스토리 보기

프로시저

단계 **1** Firepower Management Center 메뉴 표시줄에서 **Deploy(**구축**)**를 클릭한 다음 **Deployment History(**구축 기록**)**를 선택합니다.

모든 이전 구축 및 롤백 작업의 목록이 역순으로 표시됩니다.

단계 **2** 필요한 구축 작업 옆의 확장 화살표( )를 클릭하여 작업에 포함된 디바이스 및 구축 상태를 확인합니다.

단계 **3** (선택 사항) 디바이스로 전송된 명령 및 수신된 응답을 보려면 대화 내용 상세정보( )를 클릭합니다.

기록은 다음 섹션으로 구성되어 있습니다.

- **Snort Apply(Snort** 적용**)** - Snort 관련 정책에서 장애 또는 응답이 발생하는 경우, 이 섹션에 메시지가 표시됩니다. 일반적으로 이 섹션은 비어 있습니다.
- **CLI Apply(CLI** 적용**)** - 이 섹션에서는 디바이스로 전송되는 명령을 사용하여 설정한 기능에 대해 설명합니다.

참고 롤백 작업의 기록은 CLI 명령 정보를 제공하지 않습니다. 롤백 명령을 보려면 구축 롤백 기록 보기, 15 페이지의 내용을 참조하십시오.

- **Infrastructure Messages(**인프라 메시지**)** - 이 섹션에는 여러 구축 모듈의 상태가 표시됩니다.

CLI Apply(CLI 적용**)** 섹션의 구축 기록에는 디바이스로 전송된 명령과 디바이스에서 반환된 응답이 포함되어 있습니다. 이러한 응답은 정보 메시지 또는 오류 메시지일 수 있습니다. 장애가 발생한 구축의 경우 명령 오류를 나타내는 메시지를 확인합니다. FlexConfig 정책을 사용하여 맞춤화된 기능을 구성하는 경우 이러한 오류를 검사하면 특히 유용할 수 있습니다. 이 오류를 확인하여 명령을 구성하려는 FlexConfig 개체의 스크립트를 수정할 수 있습니다.

참고 관리 기능에 대해 전송된 명령과 FlexConfig 정책에서 생성된 명령이 기록에서 구분되지는 않습니다.

예를 들어, 다음 시퀀스는 Firepower Management Center(FMC)가 외부에서 논리적 이름으로 GigabitEthernet0/0을 설정하기 위해 명령을 전송했음을 보여줍니다. 디바이스에서 보안 수준을 0으로 자동 설정했다고 응답했습니다. FTD에서는 어떠한 경우에도 보안 수준을 사용하지 않습니다.

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

구축 롤백

롤백은 FTD 디바이스에서 기존 구축을 지우고 이전에 구축한 구성으로 디바이스를 재구성하기 위해 제공되는 구축 기능입니다.

주의 롤백은 베타 기능입니다. 그러나 이 기능은 완전히 지원됩니다.

정책 구축 후 FTD를 통과하는 트래픽이 의도하지 않은 방식으로 영향을 받는 경우 롤백이 디바이스를 결함 있는 구축 이전의 상태로 되돌릴 수 있는 옵션을 제공합니다.

구축이 잘못되어 의도하지 않은 방식으로 트래픽이 중단된 경우에는 구축의 변경 사항을 확인하여 문제를 해결하는 것이 좋습니다. 이전 구축의 변경 사항을 확인하려면 **Deploy(**구축**)** > **Deployment History(**구축 기록**)**로 이동하여 마지막 구축의 기록을 확인합니다. 이전 구축과 관련된 추가 변경 사항은 감사 레코드를 참조하십시오(감사 기록 참조). 문제를 일으키는 변경 사항을 식별한 후 구성을 수정하고 디바이스에 다시 구축합니다. 이것이 권장되는 접근 방식입니다. 그러나 문제를 일으킨 변경 사항을 식별할 수 없는 경우 디바이스에서 마지막으로 구축된 안정적인 버전으로 롤백합니다.

롤백 작업이 정상적으로 완료되면 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 롤백된 디바이스 옆의 **Preview(**미리보기**)** 아이콘을 클릭합니다. 롤백 구성과 FMC의 현재 변경 사항 간의 변경 사항을 확인합니다. 문제를 일으킨 변경 사항을 식별하고 수정합니다.

롤백은 일부를 제외하고 디바이스의 모든 구성을 되돌립니다. 자세한 내용은 아래 표를 참조하십시오.

롤백 중에 복귀되는 구성	롤백 중에 복귀되지 않은 구성
• 모든 정책 구성 • 인터페이스 구성 • SRU 구성 • VDB 구성 • VPN 구성 • FXOS 구성	• Snort 이진 • Geo DB

중요

- 롤백은 중단 작업입니다. 이 작업을 수행하는 동안 모든 기존 연결 및 경로가 삭제되고 트래픽이 중단됩니다. 롤백은 선택한 모든 FTD 디바이스에서 현재 구성을 제거하고 선택한 롤백 버전으로 재구성합니다.
- 최적의 성능을 위해 낮은 트래픽 조건에서 롤백을 시작합니다.
- 특정 버전으로의 롤백은 한 번만 수행할 수 있습니다.
- 현재 구축된 버전 직전 버전으로만 롤백할 수 있습니다. 이전 버전으로의 롤백은 지원되지 않습니다. 지원되지 않는 버전의 경우 롤백 아이콘이 회색으로 표시됩니다.
- 2회 연속 롤백 작업은 허용되지 않습니다. 그러나 구축 후에는 다시 롤백할 수 있습니다.
- 롤백은 선택한 FTD에서만 설정을 되돌립니다. FMC는 모든 변경 사항을 유지합니다. FMC에서 구성 변경 사항이 유지되면 롤백 작업 후 디바이스가 FMC에서 오래된 것으로 표시됩니다. 디바이스의 구성과 FMC에서 유지되는 변경 사항을 보려면 **Deploy(**구축**)** > **Deployment(**구축**)**으로 이동하고 롤백된 디바이스 옆에 있는 **Preview(**미리 보기**)** 아이콘을 클릭합니다.
- 전체 구축이므로 롤백한 후 첫 번째 구축에서 구축할 변경 사항에 유의해야 합니다. 그러면 롤백된 버전으로 다시 롤백할 수 없습니다.
- **Object Group Search(**개체 그룹 검색**)** 설정이 비활성화된 경우 큰 액세스 목록이 있는 FTD에 대해서는 롤백 작업을 완료하는 데 더 오래 걸릴 수 있습니다. 이 **Object Group Search(**개체 그룹 검색**)** 설정을 확인하려면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**로 이동하여 디바이스를 선택하고 **Edit Advanced Settings(**고급 설정 편집**)**을 클릭합니다.

참고

- 롤백은 FTD 버전 6.7.0 이상에서만 지원됩니다.
- 롤백은 FTD 클러스터 및 NGIPS 디바이스에서 지원되지 않습니다.
- FMC와 FTD 간의 연결 인터페이스가 관리에서 데이터로 또는 그 반대로 변경되는 경우 롤백이 지원되지 않습니다.
- Firepower 4100/9300에서는 이전 구축의 FCM(Firepower Chassis Manager)에서 인터페이스를 변경한 다음 FCM을 사용하여 인터페이스를 동기화한 후 롤백을 시작합니다. 이렇게 하지 않으면 트래픽이 중단될 수 있습니다.
- 독립 인증서 등록도 Deployment History(구축 기록) 페이지에 구축 작업으로 나열됩니다. 그러나 이러한 버전으로 롤백할 수는 없습니다. 인증서 등록 이후에 생성된 구축 버전의 롤백은 인증서 연결도 되돌립니다. 롤백 후 다음 구축에서는 구축을 진행하기 전에 인증서를 수동으로 연결합니다.
- FMC 또는 FTD 업그레이드 후 첫 번째 버전에서는 롤백이 지원되지 않습니다. 예를 들어 FMC가 6.7.0에서 6.7.0.1로 업그레이드된 경우 6.7.0과 연결된 구축 패키지로 롤백할 수 없습니다.
- 구축 빈도가 **Once(**한 번**)**로 설정된 상태로 구성된 FlexConfig 개체가 있는 디바이스에 대한 구축이 롤백되는 경우, Preview (미리보기) 페이지에서 해당 객체가 오래된 것으로 표시되더라도 해당 구축을 재구축할 수 없습니다. 롤백 후에는 다음 구축 전에 FlexConfig 개체를 수동으로 할당 해제한 다음 디바이스에 다시 할당해야합니다.

HA 시나리오의 롤백

다음 HA 시나리오에서는 롤백이 지원되지 않습니다.

- 롤백하려는 버전에 FTD HA 부트 스트랩 구성이 포함된 경우.
- 롤백하려는 버전에 FTD HA 중단 구성이 포함된 경우.
- 현재 독립형 모드인 FTD가 이전 구축 버전에서 HA 또는 클러스터의 일부인 경우.

디바이스에서 구축 롤백

프로시저

단계 **1** Firepower Management Center 메뉴 표시줄에서 **Deploy(**구축**)** > **Deployment History(**구축 기록**)**를 선택합니다.

모든 이전 구축 작업 목록이 역순으로 표시됩니다.

단계 **2** 필요한 구축 작업 옆의 롤백 아이콘()을 클릭하여 작업에 포함된 디바이스 및 구축 상태를 확인합니다.

단계 **3** 롤백할 디바이스를 선택합니다.

단계 **4** **Rollback(**롤백**)**을 클릭합니다.

다음에 수행할 작업

롤백 상태를 확인하려면 **Deploy(**구축**)** > **Deployment(**구축**)**를 클릭합니다. 디바이스 옆의 롤백 상태를 볼 수 있습니다.

구축 롤백 기록 보기

롤백 기록은 디바이스에서 반환되는 응답과 함께 디바이스로 전송되는 명령이 작성된 버전입니다. 롤백 작업이 실패한 경우, **Deploy(**구축**)** > **Deployment History(**구축 기록**)** 페이지의 기록에 실패 이유가 표시됩니다. 단, 롤백 작업을 성공적으로 수행하기 위해 실행된 CLI 명령을 확인하려면 롤백 작업이 완료된 후 아래 단계를 수행하십시오. 이 정보는 다음 구축까지만 확인할 수 있습니다.

참고 CLI 명령 정보는 롤백이 완료된 후에 확인할 수 있으며, 다음 구축까지만 살펴볼 수 있습니다. 롤백 작업 후 첫 번째 구축에서는 모든 롤백 관련 정보가 지워집니다.

프로시저

단계 **1** Firepower Management Center 메뉴 표시줄에서 **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** 왼쪽 창에서 롤백된 디바이스를 선택합니다.

단계 **3** **View System & Troubleshooting Details(**시스템 및 문제 해결 세부 사항 보기**)** 링크를 클릭합니다.

단계 **4** **Advanced Troubleshooting(**고급 문제 해결**)**을 클릭하십시오.

단계 **5** **Threat Defense CLI(**위협 방어 **CLI)**를 클릭합니다.

단계 **6** **Command(**명령**)** 드롭다운 상자에서 **show**를 클릭합니다.

단계 **7** **Parameter(**매개변수**)** 필드에 **`running`**을 입력합니다.

단계 **8** **Execute(**실행**)**를 클릭합니다.

Snort® 재시작 시나리오

Snort 프로세스라는 트래픽 검사 엔진이 매니지드 디바이스에서 재시작되면, 프로세스가 다시 시작될 때까지 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 17 페이지을 참고하십시오. 또한, 구축 시에는 Snort 프로세스가 재시작되는지와 관계없이 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다.

다음 표의 시나리오 중 하나가 발생하는 경우 Snort 프로세스가 재시작됩니다.

표 *2: Snort* 재시작 시나리오

시나리오 다시 시작	추가 정보
Snort 프로세스를 재시작해야 하는 특정 설정을 구축합니다.	구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 20 페이지
즉시 Snort 프로세스를 재시작해야 하는 특정 설정을 수정합니다.	즉시 Snort 프로세스를 재시작시키는 변경 사항, 23 페이지
현재 구축된 자동 애플리케이션 우회(AAB) 설정을 활성화하는 트래픽을 활성화합니다.	AAB(Automatic Application Bypass) 구성

관련 항목

액세스 제어 정책 고급 설정

구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 20 페이지

정책 적용 중에 트래픽 검사

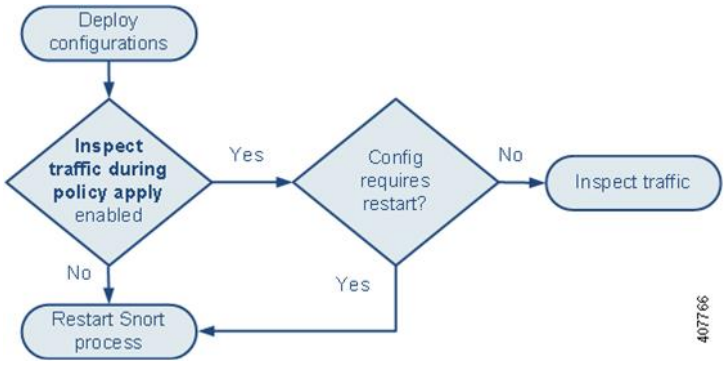
정책 적용 중 트래픽 검사는 고급 액세스 제어 정책 일반 설정으로서 설정 변경이 구축되는 동안 관리되는 디바이스가 트래픽을 검사하도록 허용합니다. 단 구축하려는 설정이 Snort 프로세스를 재시작할 필요가 없는 경우에 한정됩니다. 이 옵션은 다음과 같이 구성할 수 있습니다.

- 활성화 — 재시작 시 특정 설정이 Snort 프로세스를 요구하지 않는 한 구축 시 트래픽을 검사합니다.

  구축하려는 구성이 Snort 재시작을 요구하지 않는 경우 시스템은 현재 구축된 액세스 제어 정책을 사용해 트래픽을 검사하고 구축 시 구축하려는 액세스 제어 정책으로 전환합니다.

- 비활성화 — 구축 중 트래픽을 검사하지 않습니다. 구축 시 항상 Snort 프로세스를 재시작합니다.

다음 그래픽은 정책 적용 중 트래픽 검사 활성화에 따라 Snort가 재시작되는 방식을 나타냅니다.



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. Snort® 재시작 트래픽 동작, 17 페이지 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션, 20 페이지의 내용을 참조하십시오.

Snort® 재시작 트래픽 동작

다음 표에서는 Snort 프로세스가 재시작될 때 각 디바이스가 트래픽을 처리하는 방법을 설명합니다.

표 ***3: FTD*** 및 ***FTD*** 가상 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음
라우팅, Transparent(EtherChannel, 이중화, Transparent 포함)	차단

표 ***4: 7000*** 및 ***8000, NGIPSv*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음
라우팅, 스위칭 (7000 및 8000 Series 전용)	차단

표 *5: ASA FirePOWER* 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
라우팅 또는 fail-open 상태의 Transparent	검사 없이 통과됨
라우팅 또는 fail-close 상태의 Transparent	차단

표 *6: FTD* 및 *FTD* 가상 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Snort Fail Open: Down(Snort Fail-Open:** 중단**)**: 활성화	검사 없이 통과됨
인라인: **Snort Fail Open: Down(Snort Fail-Open:** 중단**)**: 비활성화	차단
라우팅, Transparent(EtherChannel, 이중화, 하위 인터페이스 포함) 버전 6.2.2에서는 **configure snort preserve-connection {enable | disable}** CLI 명령을 지원하지 않으며 이 명령이 활성화되어 있을 때(기본값) 검사 없이 통과하도록 기존 TCP/UDP 연결을 허용했습니다. 버전 6.2.2 기준으로, FMC 및 FTD 모두 버전 6.2.0.2 또는 후속 6.2.0.x 패치를 실행하고 있지 않으면 패킷이 삭제됩니다. 자세한 내용은 Cisco Firepower Threat Defense 명령 참조의 내용을 참고하십시오.	차단
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음

표 *7: 7000* 및 *8000, NGIPSv* 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음

인터페이스 컨피그레이션	재시작 트래픽 동작
라우팅, 스위칭 (7000 및 8000 Series 전용)	차단

표 ***8: ASA FirePOWER*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
라우팅 또는 fail-open 상태의 Transparent	검사 없이 통과됨
라우팅 또는 fail-close 상태의 Transparent	차단

표 ***9: FTD*** 및 ***FTD*** 가상 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Snort Fail Open: Down(Snort Fail-Open: 중단)**: 비활성화	차단
인라인: **Snort Fail Open: Down(Snort Fail-Open: 중단)**: 활성화	검사 없이 통과됨
라우팅, Transparent(EtherChannel, 이중화, 하위 인터페이스 포함): **preserve-connection** 활성화 (**configure snort preserve-connection enable**, 기본값) 자세한 내용은 Cisco Firepower Threat Defense 명령 참조의 내용을 참고하십시오.	기존 TCP / UDP 플로우 : Snort가 중단된 상태에서 하나 이상의 패킷이 도착하는 한 검사 없이 통과됨 새 TCP/UDP 플로우와 모든 비TCP/UDP 플로우: 삭제됨 다음 트래픽은 **preserve-connection** 활성화 시에도 삭제됩니다. • **Analyze** 규칙 작업 또는 **Analyze all tunnel traffic** 기본 정책 작업과 일치하는 plaintext, passthrough prefilter 터널 트래픽 • 연결은 액세스 제어 규칙과 일치하지 않으며 대신 기본 작업에 의해 처리됩니다. • 암호 해독된 TLS/SSL 트래픽 • 안전한 검색 흐름 • 캡티브 포털 흐름
라우팅, Transparent(EtherChannel, 이중화, 하위 인터페이스 포함): **preserve-connection** 비활성화 (**configure snort preserve-connection disable**)	차단
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회

인터페이스 컨피그레이션	재시작 트래픽 동작
패시브	중단되지 않음, 검사되지 않음

표 ***10: NGIPSv*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인: **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인: 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
패시브	중단되지 않음, 검사되지 않음

표 ***11: ASA FirePOWER*** 재시작 트래픽의 영향

인터페이스 컨피그레이션	재시작 트래픽 동작
라우팅 또는 fail-open 상태의 Transparent	검사 없이 통과됨
라우팅 또는 fail-close 상태의 Transparent	차단

참고 Snort 프로세스가 재시작되는 동안 중단되는 경우의 트래픽 처리 이외에 Failsafe 옵션의 컨피그레이션에 따라 Snort 프로세스가 사용 중인 경우에도 트래픽이 검사 없이 통과하거나 삭제될 수 있습니다. Firepower System의 인라인 집합의 내용을 참조하십시오.

참고 컨피그레이션 구축 중에 Snort 프로세스가 사용 중이지만 중단되지는 않은 경우, 총 CPU 로드가 50%를 초과하면 라우팅, 스위칭 또는 Transparent 인터페이스에서 일부 패킷이 삭제될 수 있습니다.

구축 또는 활성화 시 **Snort** 프로세스를 재시작하는 컨피그레이션

AAB를 제외한 다음 구성을 구축할 때는 설명대로 Snort 프로세스가 재시작됩니다. AAB를 구축할 때는 프로세스가 재시작되지 않지만, 과도한 패킷 레이턴시로 인해 현재 구축된 AAB 컨피그레이션이 활성화되어 Snort 프로세스가 부분적으로 재시작됩니다.

액세스 제어 정책 고급 설정

- **Inspect Traffic During Policy Apply(**정책 적용 중에 트래픽 검사**)**가 비활성화되었을 때 구축합니다.

- SSL 정책을 추가하거나 제거합니다.

보안 인텔리전스

여러 보안 인텔리전스 화이트리스트 또는 블랙리스트 네트워크나 네트워크 개체를 추가 또는 삭제합니다. 변경 사항은 맞춤형 목록 또는 시스템 제공 목록이 될 수 있으며 Snort 프로세스의 재시작 여부는 검사에 사용할 수 있는 메모리에 따라 디바이스별로 달라질 수 있습니다.

파일 정책

다음 컨피그레이션 중 하나의 첫 번째 또는 마지막 항목을 구축합니다. 이러한 파일 정책 컨피그레이션을 다른 방식으로 구축할 때는 프로세스가 재시작되지 않지만, 비 파일 정책 컨피그레이션을 구축할 때는 프로세스가 재시작될 수 있습니다.

- **Inspect Archives(**아카이브 검사**)**를 활성화하거나 비활성화합니다.
- 다음 작업 중 하나를 수행합니다.
  - 구축된 액세스 컨트롤 정책에 파일 정책이 하나 이상 포함되어 있으면 **Inspect Archives(**아카이브 검사**)**를 활성화하거나 비활성화합니다.
  - **Inspect Archives(**아카이브 검사**)**가 활성화되어 있으면 첫 번째 정책 규칙을 추가하거나 마지막 파일 정책을 제거합니다. **Inspect Archives(**아카이브 검사**)**가 적용되려면 규칙이 하나 이상 필요합니다.
- **Detect Files(**파일 탐지**)** 또는 **Block Files(**파일 차단**)** 규칙에서 **Store Files(**파일 저장**)**를 활성화하거나 해제합니다.
- **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 규칙 작업을 분석 옵션(**Spero Analysis or MSEXE(Spero** 분석 또는 **MSEXE)**, **Dynamic Analysis(**동적 분석**)**, **Local Malware Analysis(**로컬 악성코드 분석**)**) 또는 파일 저장 옵션(**Malware(**악성코드**)**, **Unknown(**알 수 없음**)**, **Clean(**정상**)**, **Custom(**맞춤형**))**과 결합하는 첫 번째 활성 파일 규칙을 추가하거나 마지막 활성 파일 규칙을 제거합니다.

이러한 파일 정책 컨피그레이션을 보안 영역이나 터널 영역에 구축하는 액세스 컨트롤 규칙의 경우 컨피그레이션이 다음 조건을 충족할 때만 프로세스가 재시작됩니다.

- 액세스 컨트롤 규칙의 소스 또는 대상 보안 영역이 대상 디바이스의 인터페이스와 연결된 보안 영역과 일치해야 합니다.
- 액세스 컨트롤 규칙의 대상 영역이 *any*(임의)가 아니면 규칙의 소스 터널 영역은 사전 필터 정책의 터널 규칙에 할당된 터널 영역과 일치해야 합니다.

ID 정책

- SSL 암호 해독이 비활성화되어 있으면(액세스 제어 정책에 SSL 정책이 포함되지 않음) 첫 번째 활성 인증 규칙을 추가하거나 마지막 활성 인증 규칙을 제거합니다.

활성 인증 규칙에는 **Active Authentication(**활성 인증**)** 규칙 작업 또는 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)**가 선택된 **Passive Authentication(**패시브 인증**)** 규칙 작업이 있습니다.

네트워크 검색

- 네트워크 검색 정책을 사용하여 HTTP, FTP 또는 MDNS 프로토콜을 통한 신뢰할 수 없는 트래픽 기반 사용자 탐지를 활성화하거나 비활성화합니다.

디바이스 관리

- 라우팅: 7000 또는 8000 Series 디바이스에 라우팅된 인터페이스 쌍 또는 가상 라우터를 추가합니다.
- VPN: 7000 또는 8000 Series 디바이스에서 VPN을 추가하거나 제거합니다.

  주의 7000 또는 8000 Series 디바이스에서 VPN을 추가하거나 제거할 때는 Snort 프로세스가 재시작된다는 경고가 표시되지 않습니다.

- MTU: 디바이스의 모든 비 관리 인터페이스 중에서 가장 높은 MTU 값을 변경합니다.
- 7000/8000 시리즈 고가용성: 고가용성 상태 공유 옵션을 변경합니다. 기본 디바이스와 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고가 표시되지 않습니다.
- AAB(자동 애플리케이션 바이패스): Snort 프로세스 오작동 또는 잘못된 디바이스 컨피그레이션으로 인해 단일 패킷이 과도한 처리 시간을 사용하면 현재 구축되어 있는 AAB 컨피그레이션이 활성화됩니다. 이 경우 매우 긴 레이턴시를 완화하거나 완전한 트래픽 정지를 방지하기 위해 Snort 프로세스가 부분적으로 재시작됩니다. 이처럼 프로세스가 부분적으로 재시작되면 디바이스가 트래픽을 처리하는 방법에 따라 일부 패킷이 검사 없이 통과되거나 삭제됩니다.

업데이트

- 시스템 업데이트: Snort 이진 또는 데이터 획득 라이브러리(DAQ)의 새 버전을 포함하는 소프트웨어 업데이트 후에 처음으로 구성을 구축합니다.
- VDB: 매니지드 디바이스에 적용 가능한 변경 사항을 포함하는 VDB(취약성 데이터베이스) 업데이트를 설치한 후 처음으로 구성을 구축하려면 탐지 엔진 재시작이 필요하며 그러면 일시적인 트래픽 중단이 발생할 수 있습니다. 이러한 경우, 설치를 시작하기 위해 Firepower Management Center를 선택하면 경고 메시지가 표시됩니다. VDB 변경 사항이 보류 중인 경우 구축 대화 상자에서 Firepower Threat Defense 디바이스에 대한 추가 경고를 제공합니다. Firepower Management Center에만 적용되는 VDB 업데이트로는 탐지 엔진이 재시작되지 않으므로 해당 업데이트는 구축할 수 없습니다.

관련 항목

컨피그레이션 변경 사항 구축, 8 페이지
Snort® 재시작 시나리오, 15 페이지

즉시 Snort 프로세스를 재시작시키는 변경 사항

다음 변경 사항은 구축 단계를 거치지 않고 즉시 Snort 프로세스를 재시작합니다. 재시작으로 인해 어떻게 트래픽이 영향을 받는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작, 17 페이지을 참고하십시오.

- 애플리케이션 또는 애플리케이션 탐지기와 관련된 다음 작업 중 하나를 수행합니다.
  - 시스템 또는 사용자 정의 애플리케이션 탐지기를 활성화하거나 비활성화합니다.
  - 활성화된 사용자 정의 탐지기를 삭제합니다.
  - 활성화된 사용자 정의 탐지기를 저장하고 다시 활성화합니다.
  - 사용자 정의 애플리케이션 생성

  Snort 프로세스를 재시작한다는 경고 메시지가 표시되며 진행을 취소할 수 있습니다. 현재 도메인 또는 하위 도메인의 관리되는 디바이스가 재시작됩니다.
- Firepower Threat Defense 고가용성 쌍을 생성하거나 중단 - 고가용성 쌍을 생성하면 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지가 표시되며 사용자가 취소할 수 있습니다.
- 7000 또는 8000 Series 유저 인터페이스(시스템 > 설정 > 프로세스)에서 Snort 프로세스를 재시작 - 시스템이 사용자의 승인 여부를 확인하며 사용자는 취소할 수 있습니다.

정책 비교

조직의 표준 규정을 준수하는지에 대한 정책 변경을 검토하고 시스템 성능을 최적화하기 위해 두 정책 또는 저장된 정책과 실행 설정 간 차이를 검토할 수 있습니다.

다음 정책 유형을 비교할 수 있습니다.

- DNS
- 파일
- 상태
- ID
- 침입
- 네트워크 분석
- SSL

비교 보기는 옵션 요약 비교 형식으로 두 정책을 표시합니다. 두 정책 간 차이점은 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.

- 녹색은 강조 표시된 설정이 한 정책에서는 나타나지만 다른 정책에서는 나타나지 않음을 표시합니다.

정책 비교

특정 정책에 대한 액세스 권한 및 필요한 라이선스가 있고 정책을 구성하기 위한 올바른 도메인에 있는 경우에만 정책을 비교할 수 있습니다.

프로시저

단계 **1** 비교할 정책의 관리 페이지에 액세스합니다.

- DNS—**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**
- 파일 — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Malware & File(**악성코드 및 파일**)**
- 상태 — **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)**
- ID — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)**
- 침입 — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**
- 네트워크 분석 — **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**

  참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

- SSL — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**

단계 **2** **Compare Policies(**정책 비교**)**를 클릭합니다.

단계 **3** **Compare Against(**비교 대상**)** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 가지의 서로 다른 정책을 비교하려면, **Other Policy(**다른 정책**)**를 선택합니다.
- 동일한 정책의 두 가지 수정 버전을 비교하려면, **Other Revision(**다른 수정 버전**)**을 선택합니다.
- 현재 활성화된 정책과 다른 정책을 비교하려면, **Running Configuration(**실행 중인 컨피그레이션**)**을 선택합니다.

단계 **4** 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 가지 서로 다른 정책을 비교하는 경우 **Policy A(**정책 **A)** 및 **Policy B(**정책 **B)** 드롭다운 목록에서 비교할 정책을 각각 선택합니다.
- 실행 중인 컨피그레이션을 다른 정책과 비교하는 경우 **Policy B(**정책 **B)** 드롭다운 목록에서 두 번째 정책을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** 비교 결과를 검토합니다.

- 비교 뷰어—비교 뷰어를 사용하여 정책 차이점을 개별적으로 탐색하려면 제목 바 위의 **Previous(**이전**)** 또는 **Next(**다음**)**를 클릭합니다.

- 비교 보고서 — 두 정책 간의 차이점을 나열하는 PDF 보고서를 생성하려면 **Comparison Report(**비교 보고서**)**를 클릭합니다.

정책 보고서

대부분의 정책에 대해 두 종류의 보고서를 생성할 수 있습니다. 보고서 목록은 두 정책 간 차이를 비교하는 반면, 단일 정책에 대한 보고서는 정책에 현재 저장된 설정의 세부 정보를 제공합니다. 상태를 제외한 모든 정책 유형에 대한 단일 정책 보고서를 생성할 수 있습니다.

참고 침입 정책 보고서는 기본 정책 설정과 정책 레이어의 설정을 결합하며 기본 정책 또는 정책 레이어 중 기반이 되는 설정이 무엇인지 구분하지 않습니다.

현재 정책 보고서 생성

특정 정책에 대한 액세스 권한 및 필요한 라이선스가 있고 정책을 설정하기 위한 올바른 도메인에 있는 경우에만 정책을 생성할 수 있습니다.

프로시저

단계 **1** 보고서를 생성할 정책의 관리 페이지에 액세스합니다.

- 액세스 제어 —**Policies(**정책**)** > **Access Control(**액세스 제어**)**
- DNS—**Policies(**정책**)** > **Access Control(**액세스 제어**)** > **DNS**
- 파일 — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Malware & File(**악성코드 및 파일**)**
- 상태 — **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)**
- ID — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Identity(ID)**
- 침입 — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**
- 7000 및 8000 Series 디바이스용 NAT — **Devices(**디바이스**)** > **NAT**
- 네트워크 분석 — **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)** 또는 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Intrusion(**침입**)**으로 이동한 다음 **Network Analysis Policy(**네트워크 분석 정책**)**

  참고 맞춤형 사용자 역할이 여기 나와 있는 첫 번째 경로에 대한 액세스를 제한하는 경우에는 두 번째 경로를 사용하여 정책에 액세스합니다.

- SSL — **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**

단계 **2** 보고서를 생성하려는 정책 옆에 있는 보고서( )를 클릭합니다.

만료된 정책

The Firepower System marks out-of-date policies with red status text that indicates how many of its targeted devices need a policy update. 이 상태를 지우려면 다시 디바이스에 정책을 구축 해야 합니다.

Configuration changes that require a policy re-deploy include:

- 액세스 제어 정책을 수정하는 경우: 액세스 제어 규칙, 기본 작업, 정책 대상, 보안 인텔리전스 필터링, 전처리를 포함한 고급 옵션 등의 모든 변경 사항
- 액세스 제어 정책이 호출하는 모든 정책을 변경하는 경우: SSL 정책, 네트워크 분석 정책, 침입 정책, 파일 정책, ID 정책 또는 DNS 정책
- 액세스 제어 정책 또는 호출 정책에 사용된 재사용 가능한 개체 또는 구성의 변경:
  - 네트워크, 포트, VLAN 태그, URL 및 지리위치 개체
  - 보안 인텔리전스 목록 및 피드
  - 애플리케이션 필터 또는 탐지기
  - 침입 정책 변수 집합
  - 파일 목록
  - 암호 해독 관련 개체 및 보안 영역
- 시스템 소프트웨어, 침입 규칙 또는 취약성 데이터베이스(VDB)의 업데이트

웹 인터페이스 내 여러 위치에서 이러한 구성 중 일부를 변경할 수 있다는 점에 주의하십시오. 예를 들어, 개체 관리자(**Objects(**개체**)** > **Object Management(**개체 관리**)**)를 사용하여 보안 영역을 수정할 수 있습니다. 그러나, 디바이스의 구성(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**)에서 인터페이스 유형을 수정하면 영역도 변경될 수 있으며 정책 재구축이 필요합니다.

참고로 다음 업데이트에는 정책 재구축이 필요하지 않습니다.

- 보안 인텔리전스 피드에 대한 자동 업데이트 그리고 컨텍스트 메뉴를 사용하여 보안 인텔리전스 차단 또는 차단 금지 목록에 추가
- URL 필터링 데이터에 대한 자동 업데이트
- 예약된 GeoDB(지정학적 위치 데이터베이스) 업데이트

제한된 구축에 대한 성능 고려 사항

호스트, 애플리케이션, 사용자 검색 데이터는 시스템이 네트워크 전체의 최신 프로파일을 생성하도록 허용합니다. 또한 시스템은 침입 및 공격 네트워크 트래픽을 분석하고 선택적으로 공격 패킷을 제거하는 침입 탐지 및 예방 시스템(IPS)으로 작용합니다.

검색 및 IPS를 결합하면 네트워크 활동에 대한 컨텍스트를 제공하며 다음과 같은 다양한 기능을 활용할 수 있습니다.

- 영향 플래그 및 보안 침해 지표는 특정 익스플로잇, 공격, 악성코드에 취약한 호스트가 무엇인지 나타냅니다
- 적응형 프로파일 Firepower 권장 사항은 대상 호스트에 따라 트래픽을 다른 방법으로 검사할 수 있습니다
- 상관관계는 영향을 받은 호스트에 따라 침입(및 기타 이벤트)에 다른 방식으로 대응합니다

그러나 조직이 IPS 수행 또는 검색 수행에만 관심이 있는 경우 다음 설정으로 시스템의 설정을 최적화할 수 있습니다.

침입 방지 없이 검색

검색 기능은 네트워크 트래픽을 모니터링하고 네트워크의 (네트워크 디바이스를 포함한) 호스트 유형 개수 및 운영 시스템, 활성 애플리케이션, 해당 호스트에 개방된 포트 정보를 확인할 수 있습니다. 또한 네트워크의 사용자 활동을 모니터링하도록 관리되는 디바이스를 구성할 수 있습니다. 검색 데이터를 사용해 트래픽 프로파일링을 수행하고 네트워크 규정 준수를 평가하고 정책 위반에 대응할 수 있습니다.

기본 구축(검색 및 단순한 네트워크 기반 액세스 제어만 수행)의 경우 액세스 제어 정책을 구성할 때 몇 가지 중요 지침을 따름으로서 디바이스의 성능을 향상할 수 있습니다.

참고 모든 트래픽을 허용하는 경우에도 액세스 제어 정책을 사용해야 합니다. 네트워크 검색 정책은 액세스 제어 정책이 통과를 허용하는 트래픽에 한해서만 검사할 수 있습니다.

우선 액세스 제어 정책에 복잡한 프로세스가 필요하지 않으며 단순한 네트워크 기반 조건을 사용하여 네트워크 트래픽을 처리할 수 있는지 확인합니다. 다음 지침을 모두 시행해야 합니다. 이런 옵션 중 하나의 구성 오류가 발생할 경우 성능 이점이 사라집니다.

- 보안 인텔리전스 기능을 사용하지 마십시오. 정책의 보안 인텔리전스 설정에서 생성된 전역 차단 또는 차단 금지 목록을 제거합니다.
- 차단 활동을 모니터링하거나 상호 작용과 관련된 액세스 제어 규칙을 포함하지 마십시오. 허용되고 신뢰할 수 있는 차단 규칙만 사용합니다. 허용된 트래픽은 검색을 통해서만 검사할 수 있으며 신뢰할 수 있는 차단된 트래픽은 검사할 수 없습니다.
- 애플리케이션, 사용자, URL, ISE 속성, 위치 정보에 기반한 네트워크 조건과 관련된 제어 규칙을 포함하지 않습니다. 단순한 네트워크 기반 조건인 영역, IP 주소, VLAN 태그, 포트만 사용합니다.
- 파일, 악성코드, 침입 검사를 수행하는 액세스 제어 규칙을 포함하지 않습니다. 즉 파일 또는 침입 정책을 액세스 제어 규칙과 연결하지 마십시오.

- 액세스 제어 정책의 Advanced(고급) 설정에서 **Access Control(**액세스 제어**)** 규칙이 결정되기 전에 사용되는 Intrusion Policy(침입 정책)가 **No Rules Active(**활성 규칙 없음**)**로 설정되어 있는지 확인합니다.
- **Network Discovery Only(**네트워크 검색만**)**를 정책의 기본 활동으로 선택합니다. 침입 검사를 수행하는 정책을 기본 활동으로 선택하지 않습니다.

액세스 제어 정책을 결합하면 시스템이 세그먼트, 포트, 영역에서 발견된 검색 데이터, 호스트, 애플리케이션, 사용자에 대한 검색을 수행하는 네트워크 세그먼트, 포트, 영역을 특정하는 네트워크 검색 정책을 설정하고 구축할 수 있습니다.

관련 항목

트래픽이 식별되기 전에 통과하는 패킷 검사

검색 없이 침입 방지

필요하지 않을 경우 (IPS 전용 구축 등) 검색을 비활성화하면 성능을 향상시킬 수 있습니다. 검색을 비활성화하려면 다음의 모든 변경 사항을 구현해야 합니다.

- 네트워크 검색 정책의 모든 규칙을 삭제합니다.
- 영역, IP 주소, VLAN 태그, 포트의 액세스 제어를 수행하는 단순한 네트워크 기반 조건만 사용합니다.

  모든 유형의 어플리케이션, 사용자, URL, 지리 위치 제어, 보안 인텔리전스를 수행하지 마십시오. 검색 데이터의 스토리지를 비활성화할 수 있지만 시스템은 이런 기능을 수행하기 위해 수집 및 검사를 수행합니다.
- 기본 전역 목록을 포함해 액세스 제어 정책의 보안 인텔리전스 설정에서 모든 차단 및 차단 안 함 목록을 삭제하면 네트워크 및 URL 기반 보안 인텔리전스를 비활성화합니다.
- DNS 규칙에 대해 DNS 및 전역 차단 목록에 대한 기본 전역 차단 안 함 목록을 포함해 DNS 정책과 관련된 모든 규칙을 삭제 또는 비활성화하여 DNS 기반 보안 인텔리전스를 비활성화합니다.

구축 후 대상 디바이스에서 새 검색을 중지합니다. 시스템은 시간 초과 환경 설정에 따라 네트워크 맵에서 점진적으로 정보를 삭제합니다. 또는 사용자가 모든 데이터를 즉시 제거할 수 있습니다.

정책 관리 히스토리

기능	버전	세부 사항
FTD 디바이스의 롤백 구축	6.7	롤백은 FTD 디바이스에서 기존 구축을 제거하고 이전에 구축한 구성으로 디바이스를 재구성하기 위해 제공되는 구축 기능입니다. New/modified(신규 / 수정) 페이지: **Deploy(**구축**)** > **Deployment History(**구축 히스토리**)** 페이지에 롤백 아이콘이 있는 새로운 롤백 열이 제공됩니다. 작업이 확장되어도 디바이스 레벨에서 롤백을 시작하기 위해 유사한 롤백 아이콘을 찾을 수 있습니다. 지원되는 플랫폼: Firepower Management Center

기능	버전	세부 사항
Firepower Management Center의 구축 섹션을 개정합니다.	6.6	

기능	버전	세부 사항
		FMC 메뉴 모음의 **Deploy(**구축**)** 버튼이 **Deploy(**구축**)** 메뉴로 변경됩니다. 그 아래에는 2개의 새로운 하위 메뉴 옵션이 있습니다. 이들은 **Deployment(**구축**)** 및 **Deployment History(**구축 히스토리**)**입니다. 새로 구축된 기능과 함께 구축 페이지가 개선되었으며, 새로운 구축 히스토리 페이지에서는 모든 이전 구축의 범례를 제공합니다. 구축 페이지에는 다음과 같은 기능이 새로 추가되었습니다. • 구축 상태-구축 페이지의 Status(상태) 열에서 각 디바이스의 구축 상태를 제공합니다. • 구축 견적-디바이스, 정책 또는 구성을 선택한 후 구축 페이지에서 견적 링크를 사용할 수 있습니다. 견적 링크를 한 번 클릭하면 구축 기간의 견적이 제공됩니다. • 구축 미리보기-미리보기는 디바이스에 구축할 모든 정책 및 개체 변경 사항의 스냅샷을 제공합니다. 정책 변경 사항에는 새 정책, 기존 정책의 변경 사항 및 삭제된 정책이 포함됩니다. 개체 변경 사항에는 정책에 사용되는 추가 및 수정된 개체가 포함됩니다. • 선택적 정책 구축-FMC를 사용하면 구축해야 하는 디바이스의 모든 변경 사항 목록에서 특정 정책을 선택하고 선택한 정책만 구축할 수 있습니다. 지원되는 플랫폼: Firepower

기능	버전	세부 사항
		Management Center