구성 가져오기 및 내보내기

다음 항목에서는 가져오기/내보내기 기능 사용 방법을 설명합니다.

컨피그레이션 가져오기/내보내기 정보

가져오기/내보내기 기능을 사용하여 어플라이언스 간에 구성을 복사할 수 있습니다. 구성 가져오기 및 내보내기는 백업 도구용이 아니지만 새로운 어플라이언스를 추가하는 프로세스를 간소화하는 데 사용될 수 있습니다.

단일 구성을 내보내거나 단일 동작으로 같은 유형 또는 다른 유형의 구성 집합을 내보낼 수 있습니다. 나중에 패키지를 다른 어플라이언스로 가져올 때 패키지의 어떤 구성을 가져올지 선택할 수 있습니다.

내보낸 패키지에는 해당 구성에 대한 개정 정보가 들어 있으며, 해당 구성을 다른 어플라이언스로 가져올 수 있는지 여부를 결정합니다. 어플라이언스 호환 되는 경우 패키지에 중복 구성, 시스템은 해결 옵션을 제공 합니다.

참고 가져오기 및 내보내기 어플라이언스는 동일한 버전의 Firepower System을 실행해야 합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다. 버전이 일치하지 않으면 가져오기가 실패합니다. 침입 규칙 업데이트 가져오기/내보내기 기능을 사용할 수 없습니다. 대신 최신 규칙 업데이트 버전을 다운로드하고 적용합니다.

가져오기/내보내기를 지원하는 구성

가져오기/내보내기는 다음 구성을 지원합니다.

- 액세스 제어 정책 및 이 정책에서 호출하는 정책: 네트워크 분석, 침입, SSL, 파일, Threat Defense Service Policy
- 액세스 제어와 무관한 침입 정책
- NAT 정책(Firepower Threat Defense만 해당)
- FlexConfig 정책. 그러나 정책을 내보내는 경우 모든 비밀 키 변수의 내용이 지워집니다. 비밀 키를 사용하는 FlexConfig 정책을 가져온 후 모든 비밀 키의 값을 수동으로 편집해야 합니다.
- 플랫폼 설정
- 상태 정책
- 알림 응답
- 애플리케이션 탐지기(사용자 정의 및 Cisco Professional Services 제공 모두)
- 대시보드
- 맞춤형 테이블
- 맞춤형 워크플로
- 저장된 검색
- 맞춤형 사용자 역할
- 보고서 템플릿
- 서드파티 제품 및 취약성 매핑

구성 가져오기/내보내기에 대한 특별 고려 사항

구성을 내보내는 경우 시스템도 다른 필수 구성을 내보냅니다. 예를 들어, 액세스 제어 정책 내보내기는 해당 정책이 호출하는 하위 정책, 해당 정책이 사용하는 개체 및 개체 그룹, 상위 정책 (다중 도메인 구축의 경우) 등을 내보냅니다. 또 다른 예로, 외부 인증이 활성화된 플랫폼 설정 정책을 내보내는 경우 인증 개체도 내보내게 됩니다. 그러나 몇 가지 예외가 있습니다.

- 시스템 제공 데이터베이스 및 피드— 시스템은 URL 필터링 카테고리 및 평판 데이터, Cisco Intelligence Feed 데이터 또는 GeoDB(지리위치 데이터베이스)를 내보내지 않습니다. 구축에 있는 모든 어플라이언스가 Cisco의 최신 정보를 받는지 확인하십시오.
- 전역 보안 인텔리전스 목록—시스템은 내보낸 구성과 관련된 전역 보안 인텔리전스 차단 리스트 및 차단 안 함 목록을 내보냅니다. (다중 도메인 구축에서 이는 현재 도메인과 상관없이 발생합니다.) 시스템은 하위 도메인 목록을 내보내지 않습니다.) 가져오기 프로세스는 이들 목록을 사용자가 생성한 목록으로 전환한 다음 가져온 구성으로 새 목록을 사용합니다. 이렇게 하면 가져온 목록이 기존의 전역 차단 목록 및 차단 안 함 목록과 충돌하지 않습니다. 가져오는 Firepower Management Center에서 가져온 구성으로 전역 목록을 사용하려면 목록을 수동으로 추가하십시오.

- 침입 정책 공유 계층 - 내보내기 프로세스가 침입 정책 공유 계층을 끊습니다. 이전에 공유된 계층은 패키지에 포함되며, 가져온 침입 정책에는 공유 계층이 포함되지 않습니다.
- 침입 정책 기본 변수 집합 - 내보내기 패키지에는 맞춤형 변수 및 시스템 제공 변수가 포함된 기본 변수 집합과 사용자 정의 값이 포함됩니다. 가져오기 프로세스는 기본 변수 집합을 가져오는 Firepower Management Center에서 가져온 값으로 업데이트합니다. 그러나 가져오기 프로세스는 내보내기 패키지에 없는 사용자 지정 변수를 삭제하지 않습니다. 가져오기 프로세스는 또한 내보내기 패키지에서 설정되지 않은 값에 대해 가져오는 Firepower Management Center에서 사용자 정의 값을 되돌리지 않습니다. 따라서 가져오는 Firepower Management Center이 기본 변수를 다르게 구성한 경우, 가져온 침입 정책이 예상과 다르게 작동할 수 있습니다.
- 맞춤형 사용자 개체—맞춤형 사용자 그룹 또는 개체를 Firepower Management Center에 생성한 경우 그리고 그러한 맞춤형 사용자 개체가 액세스 정책에 있는 어느 규칙의 일부인 경우, 내보내기 파일(.sfo)은 사용자 개체 정보를 전달하지 않습니다. 따라서 그러한 정책을 가져오는 경우, 그러한 맞춤형 사용자 개체에 대한 참조는 제거되며 대상 Firepower Management Center로 가져올 수 없습니다. 누락된 사용자 그룹으로 인한 탐지 문제를 방지하려면, 맞춤형 사용자 개체를 새 Firepower Management Center에 수동으로 추가하고 가져오기 후 액세스 제어 정책을 다시 구성합니다.

가져올 때 개체 및 개체 그룹:

- 일반적으로 가져오기 프로세스는 개체 및 그룹을 새 항목으로 가져 오며 기존 개체 및 그룹을 대체할 수 없습니다. 그러나 가져온 구성의 네트워크 및 포트 개체 또는 그룹이 기존 개체 또는 그룹과 일치하는 경우, 가져온 구성은 새 개체/그룹을 생성하는 대신 기존 개체/그룹을 다시 사용합니다. 시스템은 이름(자동 생성된 숫자 제외)과 각 네트워크 및 포트 개체/그룹의 내용을 비교하여 일치하는 항목을 결정합니다.
- 가져온 개체의 이름이 가져오는 Firepower Management Center에서 기존 개체와 일치하는 경우, 시스템이 가져온 개체 및 그룹 이름에 자동 생성된 번호를 추가하여 고유하게 만듭니다.
- 가져온 구성에서 사용되는 보안 영역 을 가져오는 Firepower Management Center에 의해 관리되는 매칭 유형 영역 에 매핑해야 합니다.
- 개인 키를 포함하는 PKI 개체를 사용하는 구성을 내보내는 경우, 시스템은 내보내기 전에 개인 키를 암호 해독합니다. 가져올 때 시스템은 무작위로 생성된 키로 해당 키를 암호화합니다.

구성 가져오기/내보내기 요구 사항 및 사전 요건

모델 지원

Any(모든 상태)

지원되는 도메인

모든

사용자 역할

- 관리자

컨피그레이션 내보내기

내보내는 구성 수 및 그러한 구성이 참조하는 개체의 수에 따라 내보내기 프로세스가 몇 분 정도 걸릴 수 있습니다.

팁 Firepower System의 많은 목록 페이지에는 목록 항목 옆에 **YouTube EDU**( )이 있습니다. 이 아이콘이 있으면 내보내기 절차의 빠른 대안으로서 사용할 수 있습니다.

시작하기 전에

- 가져오기 및 내보내기 어플라이언스에서 동일한 버전의 Firepower System 실행 중인지 확인합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Tools(**툴**)** > **Import/Export(**가져오기/내보내기**)**을(를) 선택합니다.

단계 **2** 축소( ) 및 확장( ) 아이콘을 클릭하여 사용 가능한 설정 목록을 축소하고 확대합니다.

단계 **3** 내보내려는 구성을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **4** 웹 브라우저의 프롬프트에 따라 내보낸 패키지를 컴퓨터에 저장합니다.

컨피그레이션 가져오기

가져오는 구성의 수 및 해당 구성이 참조하는 개체의 수에 따라 가져오기 절차에는 몇 분 정도 걸릴 수 있습니다.

참고 시스템에서 로그아웃하거나 다른 도메인으로 변경한 경우 또는 **Import(**가져오기**)**를 클릭한 후 사용자 세션이 시간 초과된 경우, 가져오기 프로세스가 완료될 때까지 백그라운드에서 계속 진행됩니다.

시작하기 전에

- 가져오기 및 내보내기 어플라이언스에서 동일한 버전의 Firepower System 실행 중인지 확인합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다.
- 가져오는 Firepower Management Center에 보안 영역을 생성합니다. 이 영역의 유형이 가져오는 액세스 제어 정책의 영역 유형과 일치해야 합니다. 자세한 내용은 보안 영역를 참조하십시오.

프로시저

단계 **1** 가져오는 어플라이언스에서 **System(**시스템**)** > **Tools(**툴**)** > **Import/Export(**가져오기/내보내기**)**을 선택합니다.

단계 **2** **Upload Package(**패키지 업로드**)**를 클릭합니다.

단계 **3** 내보내기한 패키지의 경로를 입력하거나 해당 위치를 찾은 다음 **Upload(**업로드**)**를 클릭합니다.

단계 **4** 버전 불일치 또는 기타 문제가 없는 경우 가져오려는 구성을 선택한 다음 **Import(**가져오기**)**를 클릭합니다.
충돌 해결 또는 보안 영역 매핑을 수행할 필요가 없는 경우, 가가져오기가 완료되고 성공 메시지가 나타납니다. 이 절차의 나머지 부분을 건너뜁니다.

단계 **5** 메시지가 나타나면, Access Control Import Resolution(액세스 제어 가져오기 해결) 페이지에서 영역으로 가져온 구성에서 사용된 보안 영역를 가져오는 Firepower Management Center이 관리하는 매칭된 인터페이스 유형과 매핑합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

단계 **7** 메시지가 나타나면, Import Resolution(가져오기 해결) 페이지에서 가져오기 충돌 해결, 5 페이지에 설명된 대로 각 구성을 확장하고 적절한 옵션을 선택합니다.

단계 **8** **Import(**가져오기**)**를 클릭합니다.

단계 **9** 모든 피드를 업데이트합니다.

예를 들어, **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Security Intelligence(**보안 인텔리전스**)**로 이동하여 URL, Network(네트워크), DNS Lists(DNS 목록) 및 Feeds(피드) 페이지에서 **Update Feed(**피드 업데이트**)** 버튼을 클릭합니다.

가져온 정책은 피드 내용을 포함하지 않습니다.

단계 **10** 디바이스에 정책을 구축하기 전에 모든 피드 업데이트가 완료될 때까지 기다리십시오.

가져오기 충돌 해결

구성 가져오기를 시도하는 경우, 시스템에서 동일한 이름 및 유형의 구성이 이미 어플라이언스에 존재하는지 여부를 확인합니다. 다중 도메인 구축에서 시스템은 구성이 현재 도메인이나 상위 도메인 또는 하위 도메인에 정의 된 구성의 복제인지 여부도 결정합니다. (하위 도메인의 구성은 볼 수 없지만, 하위 도메인에 중복된 이름이 있는 구성이 존재하는 경우 시스템이 충돌을 알립니다.) 가져오기에 중복 구성이 포함된 경우, 시스템은 다음 중 구축에 적합한 해결 옵션을 제공합니다.

- 기존 항목 유지

  시스템이 해당 구성을 가져오지 않습니다.

- 기존 항목 교체

  시스템이 가져오기에서 선택된 구성으로 현재 구성을 덮어씁니다.

- 최신 항목 유지

  타임 스탬프가 어플라이언스의 현재 구성에 대한 타임 스탬프보다 최근인 경우에만 시스템이 선택된 구성을 가져옵니다.

- 새 항목으로 가져오기

  시스템이 선택된 중복 구성을 가져오고 시스템 생성 번호를 이름에 추가하여 고유하게 만듭니다. (가져오기 프로세스를 완료하기 전에 이 이름을 변경할 수 있습니다.) 어플라이언스의 원래 구성이 변경되지 않습니다.

시스템에서 제공하는 해결 옵션은 구축에서 도메인을 사용하는지 여부, 가져온 구성이 현재 도메인에 정의된 구성과 중복되는지 여부 또는 현재 도메인의 상위 또는 하위 도메인에 정의된 구성인지 여부에 따라 달라집니다. 다음 표는 시스템에서 해결 옵션을 제공하거나 제공하지 않는 경우를 나열합니다.

해결 옵션	**Firepower Management Center**		매니지드 디바이스
	현재 도메인에서 중복	상위 또는 하위 도메인의 중복	
기존 항목 유지	예	예	예
기존 항목 교체	예	아니요	예
최신 항목 유지	예	아니요	예
새 항목으로 가져오기	예	예	예

사용자가 정상 또는 맞춤형 검색 파일 목록을 사용하는 파일 정책으로 액세스 제어 정책을 가져오고 파일 목록에는 중복 이름 충돌이 나타나는 경우, 시스템에서 위의 표에 설명된 대로 충돌 해결 옵션을 제공합니다. 그러나 시스템이 정책 및 파일 목록에 대해 수행하는 작업은 아래 표에 설명된 대로 다양합니다.

해결 옵션	시스템 작업	
	액세스 제어 정책 및 관련 파일 정책을 새 항목으로 가져오고 파일 목록을 병합합니다.	기존 액세스 제어 정책, 관련 파일 정책 및 파일 목록이 그대로 유지됩니다.
기존 항목 유지	아니요	예
기존 항목 교체	예	아니요

해결 옵션	시스템 작업	
	액세스 제어 정책 및 관련 파일 정책을 새 항목으로 가져오고 파일 목록을 병합합니다.	기존 액세스 제어 정책, 관련 파일 정책 및 파일 목록이 그대로 유지됩니다.
새 항목으로 가져오기	예	아니요
Keep newest(최신 상태로 유지**)**하고 가져오는 액세스 제어 정책이 최신 항목이 됩니다.	예	아니요
Keep newest(최신 상태로 유지**)**하고 기존 액세스 제어 정책이 최신 항목이 됩니다.	아니요	예

어플라이언스에서 가져온 구성을 수정하고 나중에 해당 어플라이언스로 해당 구성을 다시 가져 오는 경우, 유지할 구성 버전을 선택해야 합니다.