Cisco ASA-Firepower Threat Defense 마이그레이션 가이드 버전 6.2

초판: 2017년 01월 23일

최종 변경: 2017년 02월 08일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

텍스트 부품 번호:

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이센스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이센스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

목 차

1 장

Cisco ASA-Firepower Threat Defense 마이그레이션 소개

이 가이드에서는 Cisco의 마이그레이션 툴을 사용하여 방화벽 정책 설정을 사용자 Cisco ASA에서 Firepower Threat Defense 디바이스로 마이그레이션하는 방법을 설명합니다.

고급 스테이트풀 방화벽 및 VPN 집선 장치 기능을 제공하는 Cisco ASA는 오랫동안 방화벽의 업계 표준으로 사용되어 왔습니다. 이 제품에 대한 자세한 내용은 http://www.cisco.com/go/asa를 참조하십시오.

한 단계 발전된 방화벽 제품인 Firepower Threat Defense는 유니파이드 차세대 방화벽 및 차세대 IPS 기능을 제공합니다. 이 제품에는 Firepower Software 모델에서 제공되는 IPS 기능뿐 아니라 사이트 대 사이트 VPN, 강력한 라우팅, NAT, 클러스터링, 애플리케이션 가시성 및 액세스 제어와 관련된 기타 최적화 등의 방화벽 및 플랫폼 기능이 포함되어 있습니다. 또한, Firepower Threat Defense는 AMP(Advanced Malware Protection) 및 URL 필터링도 지원합니다. 이 제품에 대한 자세한 내용은 http://www.cisco.com/go/ngfw를 참조하십시오.

Cisco의 마이그레이션 툴을 사용하면 ASA 컨피그레이션의 특정 기능을 Firepower Threat Defense 컨피그레이션의 동등 기능으로 변환할 수 있습니다. 이 변환을 수행한 후 사용자가 변환된 정책을 조정하고 추가 Firepower Threat Defense 정책을 구성하여 마이그레이션을 수동으로 완료하는 것이 좋습니다.

새 Firepower Threat Defense 디바이스 또는 Firepower Threat Defense 디바이스로 초기화된 원래 ASA 디바이스로 ASA 컨피그레이션을 마이그레이션할 수 있습니다.

• 설명서 표기 규칙, 6 페이지

마이그레이션 툴

ASA 컨피그레이션을 Firepower Threat Defense 컨피그레이션 Firepower Management Center로 마이그레이션하려면 ASA-Firepower Threat Defense 마이그레이션 툴 이미지를 사용하여 전용 Firepower Management Center Virtual for VMware를 준비합니다. 이 전용 Management Center는 디바이스와 통신하지 않습니다. 대신, 마이그레이션 툴에서 .cfg 또는 .txt 형식의 ASA 컨피그레이션 파일을 .sfo 형식의 Firepower 가져오기 파일로 변환한 다음 프로덕션Management Center에서 이 파일을 가져올 수 있습니다.

마이그레이션 툴은 ASA 컨피그레이션 형식의 데이터, 즉 적절한 순서가 지정된 ASA CLI 명령의 플랫 파일만 변환할 수 있습니다. 마이그레이션 툴을 사용하는 경우 시스템이 파일 형식을 검증합니다. 예를 들어 파일에 ASA 버전 명령이 포함되어야 합니다. 시스템이 파일을 검증할 수 없으면 변환에서 장애가 발생합니다.

ASA 디바이스 요건

마이그레이션 툴은 다음 ASA 디바이스에서 컨피그레이션 데이터를 마이그레이션할 수 있습니다.

표 *1:* 지원되는 플랫폼 및 환경

지원되는 플랫폼	지원되는 환경
Any(모두)	ASA 버전 9.7/ASDM 버전 7.7 ASA 버전 9.6/ASDM 버전 7.6 ASA 버전 9.5/ASDM 버전 7.5 ASA 버전 9.4/ASDM 버전 7.4 ASA 버전 9.3/ASDM 버전 7.3 ASA 버전 9.2/ASDM 버전 7.2 ASA 버전 9.1/ASDM 버전 7.1

또한, ASA 디바이스는 다음 요건을 충족해야 합니다.

- 단일 상황 모드에서 실행 중이어야 합니다.
- 페일오버 쌍의 일부인 경우 액티브 유닛이어야 합니다.
- 클러스터의 일부인 경우 마스터 유닛이어야 합니다.

ASA 디바이스는 Transparent 모드 또는 라우팅 모드에서 실행할 수 있습니다.

Firepower 디바이스 요건

이 문서에서 설명하는 마이그레이션 프로세스를 수행하려면 다음 Firepower 디바이스가 필요합니다.

- 전용 Firepower Management Center Virtual for VMware에서 실행되는 마이그레이션 툴
- 프로덕션Firepower Management Center. 지원되는 플랫폼에서 지원되는 환경을 실행해야 합니다.

지원되는 **Firepower Management Center** 플랫폼	지원되는 **Firepower Management Center** 환경
Firepower Management Center: FS750, FS1500, FS2000, FS3500, FS4000, Virtual	마이그레이션 툴과 동일한 버전이어야 합니다.

- 프로덕션Firepower Threat Defense 디바이스(이미지로 다시 설치된 ASA 디바이스일 수 있음). Firepower Threat Defense용으로 지원되는 플랫폼 및 환경의 목록은 *Firepower System* 호환성 가이드를 참조하십시오.

라이센스 요건

이 문서에서 설명하는 마이그레이션된 컨피그레이션을 사용하려면 기본 Firepower Threat Defense 라이센스가 있어야 합니다. 자세한 내용은 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html를 참조하십시오.

ASA 디바이스에는 Firepower Threat Defense 디바이스와 다른 라이센스가 필요하므로 마이그레이션 툴은 라이센스 정보를 마이그레이션하지 않습니다. Firepower Threat Defense 디바이스용으로 새 라이센스를 구매해야 합니다. 마이그레이션 상황의 라이센스 가격에 대해 궁금한 점이 있으면 영업 팀에 문의하십시오.

마이그레이션이 지원되는 ASA 기능

마이그레이션 툴은 다음 ASA 기능을 마이그레이션할 수 있습니다.

- 확장 액세스 규칙(인터페이스에 할당하고 글로벌로 할당할 수 있음)
- Twice NAT 및 네트워크 개체 NAT 규칙
- 툴이 변환하는 확장 액세스 규칙 및 NAT 규칙과 연결된 모든 네트워크 개체/그룹 또는 서비스 개체/그룹

툴이 ASA 컨피그레이션을 Firepower Threat Defense 컨피그레이션으로 변환하는 방법에 대한 설명은 변환 매핑 개요, 17 페이지를 참조하십시오.

마이그레이션 제한

ASA 컨피그레이션을 마이그레이션할 때는 다음 제한 사항에 유의하십시오.

ASA 컨피그레이션만 해당

마이그레이션 툴은 ASA 컨피그레이션만 변환하고 기존 ASA FirePOWER 컨피그레이션은 변환하지 않습니다. 따라서 기존 ASA FirePOWER 컨피그레이션은 Firepower Threat Defense 컨피그레이션으로 수동 변환해야 합니다.

ACL 및 **ACE** 제한

마이그레이션 툴은 최대 2백만 개의 총 액세스 규칙 요소를 포함하는 ASA 컨피그레이션 파일을 지원할 수 있습니다. 변환된 컨피그레이션 파일이 이 제한을 초과하면 마이그레이션에서 장애가 발생합니다.

단일 ACL의 요소 수가 아닌 ASA 컨피그레이션 파일의 모든 액세스 규칙 요소 합계를 고려해야 합니다. 단일 ACL의 요소를 보려면 ASA CLI 명령 `show access-list | i elements`를 사용합니다.

적용된 규칙 및 개체만 해당

마이그레이션 툴은 인터페이스에 적용된 ACL만 변환합니다. 즉, ASA 컨피그레이션 파일에 페어링된 **access-list** 및 **access-group** 명령이 포함되어야 합니다.

마이그레이션 툴은 활성 상태로 적용된 ACL 또는 NAT 규칙과 연결된 개체만 변환합니다. 즉, ACL 컨피그레이션 파일에 적절하게 연결된 **object**, **access-list**, **access-group** 및 **nat** 명령이 포함되어야 합니다. 네트워크 및 서비스 개체만 마이그레이션할 수는 없습니다.

지원되지 않는 **ACL** 및 **NAT** 컨피그레이션

마이그레이션 툴은 대부분의 ACL 및 NAT 컨피그레이션을 지원하지만, 특정 예외가 있습니다. 지원되지 않는 ACL 및 NAT 컨피그레이션은 다음과 같이 처리됩니다.

변환하되 비활성화 - 마이그레이션 툴은 다음을 사용하는 ACE를 완벽하게 변환할 수 없습니다.

- 시간 범위 개체
- FQDN(Fully Qualified Domain Name)
- 로컬 사용자 또는 사용자 그룹
- SGT(보안 그룹) 개체
- 소스 및 목적지 포트 둘 다에서 중첩된 서비스 그룹

  지원되지 않는 요소에는 동등한 Firepower 개체가 없으므로 마이그레이션 툴은 이러한 규칙의 특정 요소를 변환할 수 없습니다. 이러한 경우 툴은 소스 네트워크 등 동등한 Firepower 개체가 있는 규칙 요소를 변환하고, 시간 범위 등 동등한 Firepower 개체가 없는 규칙 요소를 제외한 다음 생성하는 새 액세스 제어 또는 사전 필터 정책의 규칙을 비활성화합니다.

  또한, 비활성화되는 각 규칙에 대해 규칙 이름에 `(unsupported)`가 추가되고 시스템이 마이그레이션 중에 규칙을 비활성화한 이유를 나타내는 코멘트가 규칙에 추가됩니다. 사용자Firepower Management Center에서 비활성화된 규칙을 가져온 후 Firepower System에서 정상적으로 수행된 구축에 대한 규칙을 수동으로 수정하거나 교체할 수 있습니다.

제외 - 마이그레이션 툴은 생성하는 정책에서 EtherType 또는 WebType ACL, **name** 명령으로 지정된 호스트 주소 이름 별칭을 사용하는 ACE, 그리고 사전 정의된(기본) 서비스 개체를 사용하는 ACE 컨피그레이션을 제외합니다. 이러한 제외되는 컨피그레이션에 대한 자세한 내용은 *CLI* 설명서 *2: Cisco ASA Series* 방화벽 *CLI* 환경 설정 가이드 또는 *ASDM* 설명서 *2: Cisco ASA Series* 방화벽 *ASDM* 환경 설정 가이드를 참조하십시오.

기타 지원되지 않는 **ASA** 컨피그레이션

마이그레이션 툴은 이 문서에 지정된 기능 이외의 ASA 기능에 대해 마이그레이션을 지원하지 않습니다. 툴은 ASA 컨피그레이션 파일을 처리할 때 지원되지 않는 기능에 대한 컨피그레이션 데이터를 무시합니다.

마이그레이션 체크리스트

마이그레이션 툴을 사용하기 전에 다음 사항을 확인하십시오.

- ASA 디바이스가 모든 마이그레이션 요건을 충족해야 합니다. ASA 디바이스 요건, 2 페이지를 참조하십시오.
- ASA 컨피그레이션 파일이 .cfg 또는 txt 형식이어야 합니다.
- ASA 컨피그레이션 파일이 지원되는 컨피그레이션만 포함하고 마이그레이션에 필요한 제한을 충족해야 합니다. 마이그레이션 제한, 4 페이지를 참조하십시오.

- ASA 컨피그레이션 파일이 유효한 ASA CLI 컨피그레이션만 포함해야 합니다. 계속 진행하기 전에 잘못되었거나 불완전한 명령을 모두 수정하십시오. 파일에 잘못된 컨피그레이션이 포함되어 있으면 마이그레이션에서 장애가 발생합니다.
- 변환된 ASA 컨피그레이션 파일을 가져오려면 Firepower Management Center가 컨피그레이션을 변환하는 마이그레이션 툴과 동일한 버전을 실행해야 합니다. 이러한 제한은 주 릴리스와 부 릴리스에 둘 다 적용됩니다. 예를 들어 마이그레이션 툴은 버전 6.2를 실행하는데 파일을 가져오려는 Firepower Management Center는 버전 6.1.0.2를 실행하는 경우에는 Firepower Management Center 6.2.0으로 업그레이드해야 변환된 ASA 컨피그레이션 파일을 가져올 수 있습니다.

설명서 표기 규칙

이 문서에서는 Firepower Threat Defense 컨피그레이션으로 변환된 ASA 컨피그레이션의 예를 제공합니다. 이러한 예에 포함된 대부분의 열은 Firepower Management Center의 개체 관리자 또는 관련 규칙 편집기에 있는 구성 요소에 직접 매핑됩니다. 아래 표에는 Firepower UI 구성 요소에 직접 매핑되지 않는 열이 나와 있습니다.

표 ***2:*** 간접 값을 사용하는 열

열	값	설명
Enabled(활성화됨)	True/False	액세스 제어 규칙 또는 사전 필터 규칙에서 **Enabled(**활성화됨**)** 체크 박스를 선택할지 아니면 선택하지 않을지를 지정합니다.
Action(작업)	Permit(허용) 동등 항목	변환 중에 선택하는 항목에 따라 결정되는 값을 다음과 같이 지정합니다. • 액세스 규칙을 액세스 제어 규칙으로 변환하도록 선택하는 경우 이 값이 **Allow(**허용**)**인지 아니면 **Trust(**신뢰**)**인지도 선택합니다. • 액세스 규칙을 사전 필터 규칙으로 변환하도록 선택하는 경우 이 값이 **Fastpath(**빠른 경로**)**인지 아니면 **Analyze(**분석**)**인지도 선택합니다.
Domain(도메인)	없음	변환 시점에 이 필드는 비어 있습니다. 프로덕션Firepower Management Center에서 도메인을 가져올 때까지는 시스템이 도메인을 할당하지 않기 때문입니다. 가져오기를 수행하면 변환된 컨피그레이션을 가져오는 도메인을 기준으로 도메인이 할당됩니다.
Override(재정의)	True/False	개체에서 **Allow Overrides(**재정의 허용**)** 체크 박스를 선택할지 아니면 선택하지 않을지를 지정합니다.

2 장

ASA 컨피그레이션을 Firepower Threat Defense 컨피그레이션으로 마이그레이션

마이그레이션을 위해 ASA 준비

단계 **1** ASA 디바이스가 컨피그레이션 마이그레이션 요건을 충족하는지 확인합니다. ASA 디바이스 요건, 2 페이지를 참조하십시오.

단계 **2** 내보낼 ACL(Access Control List) 및 NAT 정책을 확인합니다.

단계 **3** ACL에 있는 항목 수를 확인합니다.

```
show access-list acl_name | i elements
```

단계 **4** 컨피그레이션에 포함된 요소가 2백만 개보다 많을 경우 불필요한 요소를 최대한 많이 정리하십시오.

마이그레이션 툴 설치

주의 프로덕션 Firepower Management Center에는 마이그레이션 툴을 설치하지 마십시오. 프로덕션 디바이스에서는 이 툴을 사용할 수 없습니다. 마이그레이션 툴을 설치한 후에는 지정된 Firepower Management Center를 이미지로 다시 설치하는 방법으로만 툴을 제거할 수 있습니다.

단계 **1** 지원 서비스에서 다음 이미지 중 하나를 다운로드합니다.

- Firepower Management Center Virtual for VMware
- Firepower Management Center Virtual for KVM

단계 **2** 해당 가이드에 설명된 대로 이미지 파일을 사용하여 전용 Firepower Management Center Virtual을 설치합니다.

- *VMware* 구축용 *Cisco Firepower Management Center Virtual* 빠른 시작 가이드
- *KVM* 구축용 *Cisco Firepower Management Center Virtual* 빠른 시작 가이드

단계 **3** `admin` 사용자 이름을 사용하여 `ssh`를 통해 Firepower Management Center에 연결합니다.

단계 **4** root 셸에 로그인합니다.

```
sudo su -
```

단계 **5** 다음 명령을 실행합니다.

```
enableMigrationTool.pl
```

참고 프로세스가 완료된 후 마이그레이션 툴을 사용하려면 Firepower Management Center에서 실행 중인 웹 인터페이스 세션을 모두 새로 고칩니다.

ASA 컨피그레이션 파일 저장

마이그레이션 툴은 .cfg 또는 .txt 형식의 ASA 컨피그레이션 파일을 변환할 수 있습니다.

단계 **1** 컨피그레이션을 저장합니다.
이 컨피그레이션을 저장하는 데 사용하는 명령은 ASA 디바이스의 버전에 따라 다를 수 있습니다. 자세한 내용은 http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html#pgfId-126642의 ASA 문서 로드맵에 나와 있는 버전별 ASA 환경 설정 가이드를 참조하십시오.

단계 **2** 저장한 컨피그레이션 파일을 마이그레이션 툴에서 액세스할 수 있는 위치(예: 로컬 컴퓨터 또는 네트워크의 공유 드라이브)로 전송합니다.

ASA 컨피그레이션 파일 변환

ASA 컨피그레이션 파일(.cfg 또는 .txt)을 Firepower 컨피그레이션 파일(.sfo)로 변환하려면 아래 단계를 수행합니다.

주의 마이그레이션 툴 UI는 Firepower Management Center UI의 확장입니다. 그러나 이 절차에서 설명하는 기능만 실행할 수 있습니다.

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

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

단계 **3** **Browse(**찾아보기**)**를 클릭하고 ASA에서 내보낸 컨피그레이션 파일을 선택합니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** 액세스 규칙을 변환할 때 시스템에서 사용할 정책을 선택합니다.

- **Prefilter Policy(**사전 필터 정책**)** - 액세스 규칙을 사전 필터 규칙으로 변환합니다.
- **Access Control Policy(**액세스 제어 정책**)** - 액세스 규칙을 액세스 제어 규칙으로 변환합니다.

단계 **6** **Prefilter Policy(**사전 필터 정책**)**를 선택한 경우 시스템에서 Permit(허용) 작업과 함께 액세스 규칙에 대해 할당할 작업을 선택합니다.

- **Fastpath(**빠른 경로**)** - 액세스 제어, ID 요건, 속도 제한 등의 모든 이후 검사와 제어에서 일치하는 트래픽을 제외합니다. 터널을 빠른 경로로 지정하면 캡슐화된 모든 연결이 빠른 경로로 지정됩니다.
- **Analyze(**분석**)** - 나머지 액세스 제어를 통해 트래픽을 계속 분석할 수 있습니다. 트래픽이 액세스 제어 및 관련 심층 검사에서 통과하는 경우 트래픽 속도도 제한할 수 있습니다.

단계 **7** **Access Control Policy(**액세스 제어 정책**)**를 선택한 경우 시스템에서 Permit(허용) 작업과 함께 규칙에 대해 할당할 작업을 선택합니다.

- **Trust(**신뢰**)** - 심층 검사 또는 네트워크 검색 없이 트래픽이 통과할 수 있도록 허용합니다. ID 정책에 의해 적용된 인증 요건 및 속도 제한은 신뢰할 수 있는 트래픽에도 계속 적용됩니다.
- **Allow(**허용**)** - 일치하는 트래픽이 통과할 수 있도록 허용합니다. ID 정책에 의해 적용된 인증 요건, 속도 제한 및 심층 검사(구성된 경우)는 허용되는 트래픽에도 계속 적용됩니다.

단계 **8** 시스템에서 지원되지 않는 규칙을 처리하는 방법을 지정합니다.

- **Convert as disabled rules(**비활성화된 규칙으로 변환**)**
- **Do not convert and add to migration report(**변환하지 않고 마이그레이션 보고서에 추가**)**

단계 **9** 로깅이 활성화된 액세스 규칙을 변환할 때 시스템이 할당해야 하는 작업을 선택합니다.

- **At the start of connection**(연결 시작 시)
- **At the end of connection**(연결 종료 시)
- **Both**(둘 다)

단계 **10** **Next**(다음)를 선택합니다.
마이그레이션이 작업으로 큐에 추가됩니다. 메시지 센터에서 작업 상태를 확인할 수 있습니다.

단계 **11** 시스템 상태 아이콘을 클릭하여 메시지 센터를 표시합니다.

단계 **12** **Tasks**(작업) 탭을 클릭합니다.
중간 Firepower Management Center에서는 마이그레이션 툴 작업만 실행할 수 있으므로, 마이그레이션 작업이 맨 위 메시지로 목록에 표시됩니다.

단계 **13** 마이그레이션 중 장애가 발생하면 해당하는 로그에서 오류 메시지를 검토합니다. 변환 장애 트러블슈팅, 11 페이지를 참조하십시오.

단계 **14** 마이그레이션이 정상적으로 완료되면 다음을 수행합니다.

- **Download .sfo(.sfo** 다운로드)를 클릭하여 변환된 파일을 로컬 컴퓨터에 복사합니다.
- **Migration Report**(마이그레이션 보고서)를 클릭하여 마이그레이션 보고서를 확인합니다.

단계 **15** 마이그레이션 보고서를 검토합니다.
마이그레이션 보고서에는 마이그레이션 툴이 Firepower Threat Defense 컨피그레이션으로 변환했거나 변환하지 못한 ASA 컨피그레이션이 요약되어 있습니다. 정상적으로 변환되지 않는 컨피그레이션은 다음과 같습니다.

- Firepower System에서 지원되지 않는 ASA 컨피그레이션
- Firepower System에서 지원은 되지만(동등한 Firepower 항목이 있음) 마이그레이션 툴이 변환하지 않는 ASA 컨피그레이션

정상적으로 변환되지 않았으며 동등한 Firepower 항목이 있는 컨피그레이션은 프로덕션Firepower Management Center에 변환된 정책을 가져온 후에 수동으로 추가할 수 있습니다.

변환 장애 트러블슈팅

전용 Firepower Management Center에서 변환 장애가 발생하는 경우 마이그레이션 툴은 로컬 컴퓨터에 다운로드할 수 있는 트러블슈팅 파일에 오류 데이터를 기록합니다.

단계 **1** **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** 어플라이언스 목록의 **Appliance(**어플라이언스**)** 열에서 전용 Firepower Management Center의 이름을 클릭합니다.

단계 **3** **Generate Troubleshooting Files(**트러블슈팅 파일 생성**)**를 클릭합니다.

단계 **4** **All Data(**모든 데이터**)** 체크 박스를 선택합니다.

단계 **5** **Generate(**생성**)**를 클릭합니다.
트러블슈팅 파일 생성이 작업으로 큐에 추가됩니다.

단계 **6** 메시지 센터에서 작업의 진행 상황을 확인하여 추적합니다.

단계 **7** 시스템이 트러블슈팅 파일을 생성하고 작업 상태가 `Completed(완료)`로 변경된 후 **Click to retrieve generated files(**생성된 파일을 검색하려면 클릭**)**를 클릭합니다.

단계 **8** TAC의 지침에 따라 트러블슈팅 파일을 Cisco로 전송합니다.

변환된 **ASA** 컨피그레이션 가져오기

Firepower Management Center의 다중 도메인 구축에서 시스템은 변환된 ASA 컨피그레이션을 가져오는 도메인에 해당 컨피그레이션을 할당합니다. 가져오기를 수행할 때 변환된 개체의 **Domains(**도메인**)** 필드가 채워집니다.

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

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

단계 **3** **Choose File(**파일 선택**)**을 클릭하고 Browse(찾아보기)를 사용하여 로컬 컴퓨터에 있는 적절한 .sfo 파일을 선택합니다.

단계 **4** **Upload(**업로드**)**를 클릭합니다.

단계 **5** 가져올 정책을 선택합니다. 이전 마이그레이션에서 선택한 항목에 따라 정책에 액세스 제어 정책, 사전 필터 정책 또는 NAT 정책이 포함될 수 있습니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.
파일이 분석되고 Import Conflict(가져오기 충돌) 페이지가 표시됩니다.

단계 **7** Import Conflict(가져오기 충돌) 페이지에서 다음을 수행합니다.

- 컨피그레이션의 충돌을 해결합니다. *Firepower Management Center* 환경 설정 가이드에서 가져오기 충돌 해결을 참조하십시오.
- 원본 ASA 컨피그레이션에서 인터페이스별로 규칙이 그룹화된 방식을 복제하거나 해당 그룹 연결을 새 연결로 교체합니다. 이렇게 하려면 다음과 같이 액세스 제어 규칙을 보안 영역에 할당하고, 사전 필터 또는 NAT 규칙을 인터페이스 그룹에 할당해야 합니다.

유형	소스	이 영역이나 그룹을 선택하는 경우
시스템 생성 보안 영역/인터페이스 그룹	마이그레이션 툴이 변환 중에 이 보안 영역/인터페이스 그룹을 자동으로 생성합니다.	원본 ASA 컨피그레이션에서 인터페이스별로 규칙이 그룹화된 방식을 복제하려는 경우
변환된 ASA 컨피그레이션을 가져오기 전에 생성된 보안 영역/인터페이스 그룹	변환된 ASA 컨피그레이션을 가져오기 전에 이 보안 영역/인터페이스 그룹을 생성합니다.	Firepower Management Center에 이미 있는 보안 영역/인터페이스 그룹과 규칙을 연결하려는 경우
가져오기 프로세스 중 즉시 생성되는 보안 영역/인터페이스 그룹	규칙 집합 옆에 있는 드롭다운 목록에서 New... (새로 만들기)를 선택하여 이 보안 영역/인터페이스 그룹을 생성합니다.	Firepower Management Center에서 새 보안 영역/인터페이스 그룹과 규칙을 연결하려는 경우

팁 규칙 집합 옆에 있는 화살표를 사용하여 해당 집합에 대한 추가 정보를 확장합니다.

참고 마이그레이션 툴은 인터페이스 컨피그레이션을 변환하지 않습니다. 따라서 변환된 ASA 컨피그레이션을 가져온 후에 디바이스를 수동으로 추가하고 해당 디바이스에서 인터페이스를 구성해야 합니다. 그러나 이 가져오기 단계에서는 새 Firepower Threat Defense 디바이스의 인터페이스와 빠르게 연결할 수 있는 단일 엔티티(보안 영역 또는 인터페이스 그룹)와 ACL 또는 NAT 정책 간의 연결을 유지할 수 있습니다. 보안 영역/인터페이스 그룹을 인터페이스와 연결하는 방법에 대한 자세한 내용은 마이그레이션 정책 구성, 13 페이지를 참조하십시오.

단계 **8** **Import**(가져오기)를 클릭합니다.
가져오기가 완료되면 메시지 센터로 이동하라는 메시지가 표시됩니다.

단계 **9** 시스템 상태 아이콘을 클릭하여 메시지 센터를 표시합니다.

단계 **10** **Tasks**(작업) 탭을 클릭합니다.

단계 **11** 가져오기 작업의 링크를 클릭하여 가져오기 보고서를 다운로드합니다.

Firepower Threat Defense 설치

아래 표에 나와 있는 적절한 빠른 시작 가이드를 사용하여 Firepower Threat Defense를 설치합니다.

참고 빠른 시작 가이드 절차에는 디바이스에 새 이미지를 설치하는 방법이 포함되어 있으므로 새 디바이스에 Firepower Threat Defense를 설치할 때나 원본 ASA를 이미지로 Firepower Threat Defense에 다시 설치할 때 동일한 절차를 사용할 수 있습니다.

플랫폼	빠른 시작 가이드
Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html
FirePOWER 4100 Series with Threat Defense: 4110, 4120, 4140	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp4100/ftd-4100-qsg.html
FirePOWER 9300 with Threat Defense	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp9300/ftd-9300-qsg.html
FirePOWER Threat Defense Virtual: VMware	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html
Firepower Threat Defense Virtual: AWS Cloud	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-qsg.html

마이그레이션 정책 구성

이 절차에서는 Firepower Management Center에서 마이그레이션한 정책을 구성하는 단계를 대략적으로 설명합니다. 각 단계에 대한 자세한 내용은 *Firepower Management Center* 환경 설정 가이드에서 관련 절차를 참조하십시오.

단계 **1** 변환 프로세스 중에 생성된 보안 영역 또는 인터페이스 그룹에 Firepower Threat Defense 디바이스의 인터페이스를 할당합니다.

단계 **2** ASA 액세스 규칙을 액세스 제어 정책으로 마이그레이션한 경우 다음 작업을 수행합니다.

- 필요한 경우 비활성화된 규칙을 활성화 또는 수정하고, 규칙을 추가 및 제거하고, 규칙 순서를 변경하여 정책의 규칙을 조정합니다. 예를 들어 서로 다른 소스 및 대상 프로토콜이나 여러 프로토콜을 지정하는 규칙을 수정할 수 있습니다. 여러 프로토콜을 지정하는 액세스 규칙, 28 페이지를 참조하십시오.
- 필요한 경우 툴이 변환하지 않는 ASA 파라미터와 동등한 Firepower 항목을 다음과 같이 구성합니다.

액세스 규칙 파라미터	액세스 제어 규칙 파라미터
사용자	선택한 사용자 조건
보안 그룹(소스)	맞춤형 SGT 조건
로깅 활성화	연결 시작 시 로깅 및/또는 연결 종료 시 로깅 옵션
로깅 레벨	연결 이벤트 로깅
로깅 간격	연결 이벤트 로깅

- 액세스 제어 정책을 Firepower Threat Defense 디바이스에 할당합니다.

단계 **3** ASA 액세스 규칙을 사전 필터 정책으로 마이그레이션한 경우 다음 작업을 수행합니다.

- 필요한 경우 비활성화된 규칙을 활성화 또는 수정하고, 규칙을 추가 및 제거하고, 규칙 순서를 변경하여 정책의 규칙을 조정합니다. 예를 들어 서로 다른 소스 및 대상 프로토콜이나 여러 프로토콜을 지정하는 규칙을 수정할 수 있습니다. 여러 프로토콜을 지정하는 액세스 규칙, 28 페이지를 참조하십시오.
- 필요한 경우 툴이 변환하지 않는 ASA 파라미터와 동등한 Firepower 항목을 다음과 같이 구성합니다.

액세스 규칙 파라미터	사전 필터 규칙 파라미터
로깅 활성화	연결 시작 시 로깅 및/또는 연결 종료 시 로깅 옵션
로깅 레벨	연결 이벤트 로깅
로깅 간격	연결 이벤트 로깅

- 시스템이 변환 중에 생성한 새 액세스 제어 정책을 구성하거나 다른 액세스 제어 정책과 사전 필터 정책을 연결합니다.
- 연결된 액세스 제어 정책을 Firepower Threat Defense 디바이스에 할당합니다.

단계 **4** NAT 정책을 마이그레이션한 경우 다음 작업을 수행합니다.

- 필요한 경우 비활성화된 규칙을 활성화 또는 수정하고, 규칙을 추가 및 제거하고, 규칙 순서를 변경하여 정책의 규칙을 조정합니다.

- NAT 정책을 Firepower Threat Defense 디바이스에 할당합니다.

단계 **5** 필요한 경우 애플리케이션 가시성 및 제어, 침입 차단, URL 필터링 및 AMP(Advanced Malware Protection)를 비롯한 차세대 방화벽 기능을 구성합니다.

단계 **6** 컨피그레이션 변경 사항을 구축합니다. 컨피그레이션 변경 사항 구축, 15 페이지를 참조하십시오.

컨피그레이션 변경 사항 구축

마이그레이션한 컨피그레이션을 구축하려면 다음 단계를 수행합니다. 구축 프로세스에 대한 자세한 내용은 *Firepower Management Center* 환경 설정 가이드에서 컨피그레이션 변경 사항 구축을 참조하십시오.

단계 **1** Firepower Management Center 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다.
Deploy Policies(정책 구축) 대화 상자에 컨피그레이션이 오래된 디바이스가 나열됩니다. 대화 상자 맨 위의 **Version(**버전**)**에는 컨피그레이션을 마지막으로 변경한 시간이 표시됩니다. 디바이스 테이블의 **Current Version(**현재 버전**)** 열에는 각 디바이스에 변경 사항을 마지막으로 구축한 시간이 표시됩니다.

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

- Sort(정렬) - 열 제목을 클릭하여 디바이스 목록을 정렬합니다.
- Expand(확장) - 디바이스 목록을 확장하여 구축할 컨피그레이션 변경 사항을 확인하려면 더하기 아이콘 ( )을 클릭합니다. 색인( ) 아이콘이 있는 오래된 정책이 표시됩니다.
- Filter(필터) - 디바이스 목록을 필터링합니다. 디스플레이에서 임의 열 머리글의 오른쪽 위에 있는 화살표를 클릭하고 **Filter(**필터**)** 텍스트 상자에 텍스트를 입력한 다음 Enter 키를 누릅니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

단계 **4** 시스템이 구축할 변경 사항에서 오류나 경고를 식별하는 경우에는 다음 옵션 중에서 선택할 수 있습니다.

- Proceed(계속) - 경고 조건을 해결하지 않고 구축을 계속합니다.시스템에서 오류를 식별하는 경우에는 계속 진행할 수 없습니다.
- Cancel(취소) - 구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 다시 구축합니다.

A 부 록

변환 매핑

다음 항목에서는 마이그레이션 툴이 ASA 컨피그레이션을 Firepower Threat Defense 컨피그레이션으로 변환하는 방법을 설명합니다.

변환 매핑 개요

마이그레이션 툴은 ASA 컨피그레이션을 다음과 같이 Firepower Threat Defense 컨피그레이션으로 변환합니다.

표 *3:* 변환 매핑 요약

엔티티	**ASA** 컨피그레이션	**Firepower Threat Defense** 컨피그레이션
네트워크 개체	네트워크 개체 네트워크 개체 그룹 중첩된 네트워크 개체 그룹	네트워크 개체 네트워크 개체 그룹 중첩된 네트워크 개체 그룹

엔티티	**ASA** 컨피그레이션	**Firepower Threat Defense** 컨피그레이션
서비스 개체	서비스 개체 서비스 개체 그룹 중첩된 서비스 개체 그룹	포트 개체 포트 개체 그룹 일반 포트 개체 그룹
액세스 규칙	액세스 규칙	액세스 제어 정책 또는 사전 필터 정책 중 선택한 항목
NAT 규칙	Twice NAT 규칙 네트워크 개체 NAT 규칙	수동 NAT 규칙 자동 NAT 규칙

변환된 컨피그레이션의 명명 규칙

마이그레이션 툴은 ASA 액세스 규칙, NAT 규칙 및 관련 개체를 동등한 Firepower Threat Defense 항목으로 변환할 때 아래에 설명된 명명 규칙을 사용합니다.

개체 및 개체 그룹 이름

마이그레이션 툴은 개체 및 개체 그룹을 변환할 때 ASA 컨피그레이션 파일의 개체 및 그룹 이름을 유지합니다.

예를 들면 다음과 같습니다.

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
```

툴은 이 컨피그레이션을 `obj1` 및 `obj2`로 명명된 네트워크 개체와 `obj_group1`로 명명된 네트워크 개체 그룹으로 변환합니다.

서비스 개체 및 서비스 그룹을 포트 개체 및 포트 개체 그룹으로 변환할 때 툴은 특정 경우에 다음 확장자를 원래 개체 또는 그룹 이름에 추가할 수 있습니다.

표 ***4:*** 변환된 서비스 개체 및 그룹에 대한 확장자

확장자	추가 이유
`_dst`	소스 및 목적지 포트가 포함된 서비스 개체를 포트 개체 2개로 분할합니다. 변환된 목적지 포트 데이터를 저장하는 데 사용되는 서비스 개체에 이 확장자가 추가됩니다. 자세한 내용은 소스 및 목적지 포트가 포함된 서비스 개체, 36 페이지를 참조하십시오.

확장자	추가 이유
_src	소스 및 목적지 포트가 포함된 서비스 개체를 포트 개체 2개로 분할합니다. 변환된 소스 포트 데이터를 저장하는 데 사용되는 서비스 개체에 이 확장자가 추가됩니다. 자세한 내용은 소스 및 목적지 포트가 포함된 서비스 개체, 36 페이지를 참조하십시오.
_#	중첩된 서비스 그룹을 변환합니다. 중첩된 서비스 그룹 변환, 38 페이지를 참조하십시오.

정책 이름

ASA 컨피그레이션 파일에는 ASA의 호스트 이름을 지정하는 `hostname` 파라미터가 포함되어 있습니다. 마이그레이션 툴은 이 값을 사용하여 파일을 변환할 때 생성하는 정책의 이름을 지정합니다.

- 액세스 제어 정책 - *hostname*-AccessPolicy-*conversion_date*
- 사전 필터 정책 - *hostname*-PrefilterPolicy-*conversion_date*
- NAT 정책 - *hostname*-NATPolicy-*conversion_date*

규칙 이름

변환된 액세스 제어, 사전 필터 및 NAT 규칙에 대해 시스템은 다음 형식을 사용하여 각 새 규칙의 이름을 지정합니다.

ACL_name-#rule_index

여기서 각 항목은 다음을 나타냅니다.

- *ACL_name* - 규칙이 속한 ACL의 이름
- *rule_index* - ACL의 다른 규칙을 기준으로 규칙이 변환되는 순서를 지정하는 시스템 생성 정수

예를 들면 다음과 같습니다.

```
acl1#1
```

서비스 개체를 변환하는 동안 단일 액세스 규칙을 여러 규칙으로 확장해야 하는 경우 다음 확장자가 추가됩니다.

ACL_name#rule_index_sub_index

여기서 추가되는 #은 확장된 시퀀스에서 새 규칙의 위치를 나타냅니다.

예를 들면 다음과 같습니다.

```
acl1#1_1
acl1#1_2
```

규칙 이름이 30자보다 긴 것으로 확인되면 ACL 이름이 단축되고 축약된 이름의 끝에 물결표(~)가 추가됩니다.

```
ACL Name~#rule index
```

예를 들어 원래 ACL 이름이 `accesslist_for_outbound_traffic`인 경우 ACL 이름이 다음과 같이 잘립니다.

```
accesslist_for_outbound_tr~#1
```

보안 영역 및 인터페이스 그룹 이름

마이그레이션 툴은 ASA 컨피그레이션 파일에서 `access-group` 명령을 변환할 때 변환 중에 선택한 항목에 따라 보안 영역 또는 인터페이스 그룹을 생성하여 명령의 인그레스 및 이그레스 정보를 캡처합니다. 이때 툴은 다음 형식을 사용하여 새 보안 영역 또는 인터페이스 그룹의 이름을 지정합니다.

*ACL_name_interface_name_direction_keyword*_zone

여기서 각 항목은 다음을 나타냅니다.

- *ACL_name* - `access-group` 명령의 ACL 이름
- *interface_name* - `access-group` 명령의 인터페이스 이름
- *direction_keyword* - `access-group` 명령의 방향 키워드(`in` 또는 `out`)

예를 들면 다음과 같습니다.

```
access-list acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

툴은 이 컨피그레이션을 `acp1_outside_in_zone`로 명명된 보안 영역 또는 인터페이스 그룹으로 변환합니다.

Firepower 개체 및 개체 그룹 관련 필드

Firepower 네트워크 및 포트 개체/그룹은 ASA 개체 및 그룹에 없는 소수의 필드를 포함합니다. 마이그레이션 툴은 변환된 네트워크 및 포트 개체/그룹에 있는 이러한 Firepower 관련 필드에 다음 기본값을 채웁니다.

표 ***5: Firepower*** 개체/그룹 관련 필드의 기본값

Firepower 개체/그룹의 필드	변환된 **ASA** 개체/그룹의 기본값
도메인	없음
재정의	False

이러한 기본값에 대한 자세한 내용은 설명서 표기 규칙, 6 페이지를 참조하십시오.

액세스 규칙 변환

마이그레이션 툴은 마이그레이션 중에 선택하는 항목에 따라 ASA 제어 규칙을 액세스 제어 규칙 또는 사전 필터 규칙으로 변환할 수 있습니다.

액세스 규칙을 액세스 제어 규칙으로 변환

ASA 액세스 규칙을 Firepower Threat Defense 액세스 제어 규칙으로 변환하도록 선택하는 경우 다음과 같은 작업이 수행됩니다.

- 변환된 규칙이 액세스 제어 정책의 **Default(**기본**)** 규칙 섹션에 추가됩니다.
- Description(설명) 필드의 내용이 규칙의 **Comment History(**코멘트 내역**)** 내 항목으로 유지됩니다.
- 규칙을 변환된 규칙으로 식별하는 항목이 **Comment History(**코멘트 내역**)**에 추가됩니다.
- 액세스 제어 규칙의 **Action(**작업**)**이 다음과 같이 설정됩니다.

액세스 규칙의 작업	액세스 제어 규칙의 작업
Permit(허용**)**	마이그레이션 중에 선택하는 항목에 따라 **Allow(**허용**)** 또는 **Trust(**신뢰**)**
Deny(거부**)**	**Block(**차단**)**

- 액세스 제어 규칙의 **Source Zones(**소스 영역**)** 및 **Destination Zones(**대상 영역**)**이 다음과 같이 설정됩니다.

ACL 유형	소스 영역	대상 영역
글로벌 - `Any(모두)` 인터페이스에 적용됨	`Any(모두)`	`Any(모두)`
특정 인터페이스에 적용됨	가져오기 중에 선택하는 보안 영역	`Any(모두)`

- 액세스 규칙이 비활성 상태이면 툴은 해당 규칙을 비활성화된 액세스 제어 규칙으로 변환합니다.

마이그레이션 툴은 다음 기본 파라미터를 사용하여 변환된 규칙을 액세스 제어 정책에 할당합니다.

- 새 액세스 제어 정책의 기본 작업이 **Block All Traffic(**모든 트래픽 차단**)**으로 설정됩니다.
- 액세스 제어 정책이 기본 사전 필터 정책과 연결됩니다.

액세스 규칙 필드 및 이 필드가 매핑되는 액세스 제어 규칙 필드

마이그레이션 툴은 아래 표에 설명된 대로 ASA 액세스 규칙의 필드를 Firepower Threat Defense 액세스 제어 규칙의 필드로 변환합니다.

참고:

- 열 1(ASA 액세스 규칙 필드)의 필드 이름은 ASDM 인터페이스의 필드 레이블에 해당합니다.
- 열 2(Firepower 액세스 제어 규칙 필드)의 필드 이름은 Firepower Management Center 인터페이스의 필드 레이블에 해당합니다.

표 ***6: ASA*** 액세스 규칙 필드 및 이 필드가 매핑되는 ***Firepower*** 액세스 제어 규칙 필드

ASA 액세스 규칙 필드	**Firepower** 액세스 제어 규칙 필드
인터페이스	동등 필드 없음
작업	조치
소스	소스 네트워크
사용자	변환하지 않음(선택한 사용자 조건과 동일함)
보안 그룹(소스)	변환하지 않음(맞춤형 SGT 조건과 동일함)
대상	대상 네트워크
보안 그룹(대상)	동등 필드 없음
서비스	선택한 목적지 포트(사전 정의된 서비스 개체를 지정하는 경우 변환하지 않음)
설명	코멘트
로깅 활성화	변환하지 않음(연결 시작 시 로깅 또는 연결 종료 시 로깅과 동일함)
로깅 레벨	변환하지 않음(연결 이벤트 로깅과 동일함)
규칙 활성화	활성화됨
트래픽 방향	동등 필드 없음
소스 서비스	선택한 소스 포트(사전 정의된 서비스 개체를 지정하는 경우 변환하지 않음)
로깅 간격	변환하지 않음(연결 이벤트 로깅과 동일함)
시간 범위	동등 필드 없음

액세스 제어 규칙 관련 필드

Firepower Threat Defense 액세스 제어 규칙은 ASA 액세스 규칙에 없는 소수의 필드를 포함합니다. 마이그레이션 툴은 변환된 액세스 제어 규칙에 있는 이러한 Firepower 관련 필드에 다음 기본값을 채웁니다.

표 *7:* 액세스 제어 규칙 관련 필드의 기본값

액세스 제어 규칙 필드	변환된 액세스 규칙의 기본값
이름	시스템 생성(변환된 컨피그레이션의 명명 규칙, 18 페이지 참조)
소스 영역	• ACL이 글로벌로 적용되는 경우 `Any(모두)` • ACL이 특정 인터페이스에 적용되는 경우 변환 중에 툴이 생성하는 보안 영역
대상 영역	`Any(모두)`(모든 액세스 제어 규칙의 기본값)
선택한 VLAN 태그	기본값 없음(가져오기 후에 수동으로 조건을 추가할 수 있음)
선택한 애플리케이션 및 필터	기본값 없음(가져오기 후에 수동으로 조건을 추가할 수 있음)
선택한 URL	기본값 없음(가져오기 후에 수동으로 조건을 추가할 수 있음)

액세스 규칙을 사전 필터 규칙으로 변환

ASA 액세스 규칙을 Firepower Threat Defense 사전 필터 규칙으로 변환하도록 선택하는 경우 다음과 같은 작업이 수행됩니다.

- Description(설명) 필드의 내용이 규칙의 **Comment History(**코멘트 내역**)** 내 항목으로 유지됩니다.
- 규칙을 변환된 규칙으로 식별하는 항목이 **Comment History(**코멘트 내역**)**에 추가됩니다.
- 사전 필터 규칙의 **Action(**작업**)**이 다음과 같이 설정됩니다.

액세스 규칙의 작업	사전 필터 규칙의 작업
Permit(허용**)**	마이그레이션 중에 선택하는 항목에 따라 **Fastpath(**빠른 경로**)** 또는 **Analyze(**분석**)**

액세스 규칙의 작업	사전 필터 규칙의 작업
Deny(거부**)**	**Block(**차단**)**

- 사전 필터 규칙의 **Source Interface Objects(**소스 인터페이스 개체**)** 및 **Destination Interface Objects(**대상 인터페이스 개체**)**가 다음과 같이 설정됩니다.

ACL 유형	소스 인터페이스 개체	대상 인터페이스 개체
글로벌 - `Any(모두)` 인터페이스에 적용됨	`Any(모두)`	`Any(모두)`
특정 인터페이스에 적용됨	가져오기 중에 선택하는 인터페이스 그룹	`Any(모두)`

- 액세스 규칙이 비활성 상태이면 툴은 해당 규칙을 비활성화된 사전 필터 규칙으로 변환합니다.

마이그레이션 툴은 다음 기본 파라미터를 사용하여 변환된 규칙을 사전 필터 정책에 할당합니다.

- 새 사전 필터 정책의 기본 작업이 **Analyze All Tunnel Traffic(**모든 터널 트래픽 분석**)**으로 설정됩니다.
- 사전 필터 정책과 같은 이름의 액세스 제어 정책이 생성된 다음 사전 필터 정책이 해당 액세스 제어 정책과 연결됩니다. 새 액세스 제어 정책의 기본 작업이 **Block All Traffic(**모든 트래픽 차단**)**으로 설정됩니다.

액세스 규칙 필드 및 이 필드가 매핑되는 사전 필터 규칙 필드

마이그레이션 툴은 아래 표에 설명된 대로 ASA 액세스 규칙의 필드를 Firepower Threat Defense 사전 필터 규칙의 필드로 변환합니다.

참고:

- 열 1(ASA 액세스 규칙 필드)의 필드 이름은 ASDM 인터페이스의 필드 레이블에 해당합니다.
- 열 2(Firepower 사전 필터 규칙 필드)의 필드 이름은 Firepower Management Center 인터페이스의 필드 레이블에 해당합니다.

표 ***8: ASA*** 액세스 규칙 필드 및 이 필드가 매핑되는 ***Firepower*** 사전 필터 규칙 필드

ASA 액세스 규칙 필드	**Firepower** 사전 필터 규칙 필드
인터페이스	동등 필드 없음
규칙 활성화	활성화됨

ASA 액세스 규칙 필드	**Firepower** 사전 필터 규칙 필드
작업	조치
소스	소스 네트워크
사용자	동등 필드 없음
보안 그룹(소스)	동등 필드 없음
대상	대상 네트워크
보안 그룹(대상)	동등 필드 없음
서비스	선택한 소스 포트 선택한 목적지 포트
설명	코멘트
로깅 활성화	변환하지 않음(연결 시작 시 로깅 또는 연결 종료 시 로깅과 동일함)
로깅 레벨	변환하지 않음(연결 이벤트 로깅과 동일함)
트래픽 방향	동등 필드 없음
소스 서비스	선택한 소스 포트(사전 정의된 서비스 개체를 지정하는 경우 변환하지 않음)
로깅 간격	변환하지 않음(연결 이벤트 로깅과 동일함)
시간 범위	동등 필드 없음

Firepower 사전 필터 규칙 관련 필드

Firepower Threat Defense 사전 필터 규칙은 ASA 액세스 규칙에 없는 소수의 필드를 포함합니다. 마이그레이션 툴은 변환된 사전 필터 제어 규칙에 있는 이러한 Firepower 관련 필드에 다음 기본값을 채웁니다.

표 ***9: Firepower*** 사전 필터 규칙 관련 필드의 기본값

사전 필터 규칙 필드	변환된 액세스 규칙의 기본값
이름	시스템 생성(변환된 컨피그레이션의 명명 규칙, 18 페이지 참조)

사전 필터 규칙 필드	변환된 액세스 규칙의 기본값
소스 인터페이스 개체	• ACL이 글로벌로 적용되는 경우 Any(모두) • ACL이 특정 인터페이스에 적용되는 경우 변환 중에 툴이 생성하는 인터페이스 그룹
대상 인터페이스 개체	Any(모두)(모든 사전 필터 규칙의 기본값)
선택한 VLAN 태그	기본값 없음(가져오기 후에 수동으로 조건을 추가할 수 있음)

액세스 규칙의 포트 인수 연산자

확장 액세스 규칙은 서비스 개체에서 사용된 것과 동일한 연산자를 사용하는 port_argument 요소를 포함할 수 있습니다. 마이그레이션 툴은 액세스 규칙에 포트 인수 연산자가 하나 포함되어 있는지 아니면 포트 인수 연산자가 여러 개 포함되어 있는지에 따라 서비스 개체를 변환할 때와 약간 다른 방식으로 액세스 규칙의 이러한 연산자를 변환합니다.

아래 표에는 포함될 수 있는 연산자와 단일 연산자 사용 예가 나와 있습니다.

표 ***10:*** 액세스 규칙의 포트 인수 연산자

연산자	설명	예
lt	보다 작음	access-list acp1 extended permit tcp any lt 300
gt	보다 큼	access-list acp2 extended permit tcp any gt 300
eq	같음	access-list acp3 extended permit tcp any eq 300
neq	같지 않음	access-list acp4 extended permit tcp any neq 300
range	값의 범위(경계값 포함). 이 연산자를 사용할 때는 range 100 200과 같이 포트 번호 2개를 지정합니다.	access-list acp5 extended permit tcp any range 9000 12000

액세스 규칙에 단일 포트 인수 연산자가 포함되어 있으면 마이그레이션 툴은 다음과 같이 액세스 규칙을 단일 액세스 제어 또는 사전 필터 규칙으로 변환합니다.

표 ***11:*** 단일 포트 인수 연산자가 포함된 액세스 규칙 및 이 규칙이 변환되는 액세스 제어 또는 사전 필터 규칙

연산자	이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
`lt`	acp1#1	모든	모든	모든	모든	1~299	모두	Permit(허용) 동등 항목	True
`gt`	acp2#1	모든	모든	모든	모든	301~65535	모두	Permit(허용) 동등 항목	True
`eq`	acp3#1	모든	모든	모든	모든	300	모두	Permit(허용) 동등 항목	True
`neq`	acp4#1	모든	모든	모든	모든	1~299, 301~65535	모두	Permit(허용) 동등 항목	True
`range`	acp5#1	모든	모든	모든	모든	9000~2000	모두	Permit(허용) 동등 항목	True

이 표에 나와 있는 원본 연산자(연산자) 열은 명확한 설명을 위해 제공되며 액세스 제어 규칙의 필드를 나타내지는 않습니다.

액세스 제어 규칙에 `access-list acp6 extended permit tcp any neq 300 any neq 400`과 같이 여러 포트 연산자가 포함되어 있으면 마이그레이션 툴은 다음과 같이 단일 액세스 규칙을 여러 액세스 제어 또는 사전 필터 규칙으로 변환합니다.

표 ***12:*** 여러 포트 인수 연산자가 포함된 액세스 규칙 및 이 규칙이 변환되는 액세스 제어 규칙

연산자	이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
`neq`	acp6#1_1	모든	모든	모든	모든	1~299	1~399	Permit(허용) 동등 항목	True
`neq`	acp6#1_2	모든	모든	모든	모든	301~65535	1~399	Permit(허용) 동등 항목	True
`neq`	acp6#1_3	모든	모든	모든	모든	1~299	401~65535	Permit(허용) 동등 항목	True
`neq`	acp6#1_4	모든	모든	모든	모든	301~65535	401~65535	Permit(허용) 동등 항목	True

이 표에 나와 있는 원본 연산자(연산자) 열은 명확한 설명을 위해 제공되며 액세스 제어 규칙의 필드를 나타내지는 않습니다.

여러 프로토콜을 지정하는 액세스 규칙

ASA에서는 TCP와 UDP 등 여러 프로토콜을 지정하는 프로토콜 서비스 개체를 사용하도록 액세스 규칙의 소스 및 목적지 포트를 구성할 수 있습니다. 예를 들면 다음과 같습니다.

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list acp1 extended permit object-group TCPUDP any any
```

그러나 Firepower System에서는 다음과 같은 방식으로만 액세스 제어 또는 사전 필터 규칙을 구성할 수 있습니다.

- 소스 및 목적지 포트 둘 다에서 동일한 프로토콜을 지정해야 합니다.
- 목적지 포트는 여러 프로토콜을 지정할 수 있지만 소스 포트는 None(없음)을 지정해야 합니다.

프로토콜 개체 그룹 TCP 및 UDP를 포함하는 액세스 규칙은 지원되지 않는 규칙으로 마이그레이션됩니다. 따라서 규칙은 **Object Group Protocol containing both tcp and udp is not supported(TCP** 및 **UDP**를 둘 다 포함하는 개체 그룹 프로토콜은 지원되지 않습니다**.)**라는 코멘트와 함께 비활성화됩니다.

NAT 규칙 변환

ASA용 NAT와 Firepower Threat Defense용 NAT는 아래 표에 요약되어 있는 것처럼 동일한 기능을 지원합니다.

표 ***13: ASA NAT*** 정책 및 이 정책이 매핑되는 ***Firepower Threat Defense NAT*** 정책

ASA NAT 정책	**Firepower Threat Defense NAT** 정책	특성 정의
Twice NAT	수동 NAT	• 단일 규칙에서 소스 및 대상 주소를 둘 다 지정합니다. • 직접 구성됩니다. • 네트워크 개체 그룹을 사용할 수 있습니다. • NAT 테이블에서 수동으로 순서가 지정됩니다(자동 NAT 규칙 앞이나 뒤).

ASA NAT 정책	Firepower Threat Defense NAT 정책	특성 정의
네트워크 개체 NAT	자동 NAT	• 소스 또는 대상 주소 중 하나를 지정합니다. • 네트워크 개체의 파라미터로 구성됩니다. • 네트워크 개체 그룹을 사용할 수 없습니다. • NAT 테이블에서 자동으로 순서가 지정됩니다.

마이그레이션 툴은 ASA NAT 컨피그레이션을 Firepower Threat Defense NAT 컨피그레이션으로 변환합니다. 그러나 지원되지 않는 네트워크 개체를 사용하는 ASA NAT 컨피그레이션은 변환할 수 없으며, 이러한 경우 변환에서 장애가 발생합니다.

ASA NAT 규칙 필드 및 이 필드가 매핑되는 Firepower Threat Defense 규칙 필드

마이그레이션 툴은 아래 표에 설명된 대로 ASA NAT 규칙의 필드를 Firepower Threat Defense NAT 규칙의 필드로 변환합니다.

참고:

- 열 1(ASA NAT 규칙 필드)의 필드 이름은 ASDM 인터페이스의 필드 레이블에 해당합니다.
- 열 2(Firepower Threat Defense 규칙 필드)의 필드 이름은 Firepower Management Center 인터페이스의 필드 레이블에 해당합니다.

표 ***14: ASA NAT*** 규칙 필드 및 이 필드가 매핑되는 ***Firepower Threat Defense NAT*** 규칙 필드

ASA NAT 규칙 필드	Firepower Threat Defense 규칙 필드
원본 패킷 - 소스 인터페이스	인터페이스 개체 - 소스 인터페이스 개체
원본 패킷 - 소스 주소	원본 패킷 - 원본 소스
원본 패킷 - 대상 인터페이스	인터페이스 개체 - 대상 인터페이스 개체
원본 패킷 - 대상 주소	원본 패킷 - 원본 대상 - 주소 유형 원본 패킷 - 원본 대상 - 네트워크
원본 패킷 - 서비스	원본 패킷 - 원본 소스 포트 원본 패킷 - 원본 목적지 포트

ASA NAT 규칙 필드	**Firepower Threat Defense** 규칙 필드
변환된 패킷 - 소스 NAT 유형	유형
변환된 패킷 - 소스 주소	변환된 패킷 - 변환된 소스 - 주소 유형 변환된 패킷 - 변환된 소스 - 네트워크
변환된 패킷 - 대상 주소	변환된 패킷 - 변환된 대상
변환된 패킷 - 서비스	변환된 패킷 - 변환된 소스 포트 변환된 패킷 - 변환된 목적지 포트
일대일 주소 변환 사용	고급 - 네트워크 대 네트워크 매핑
PAT 풀 변환된 주소	PAT 풀 - PAT - 주소 유형 PAT 풀 - PAT - 네트워크
라운드 로빈	PAT 풀 - 라운드 로빈 할당 사용
인터페이스가 아닌 대상별로 PAT 고유성 확장	PAT 풀 - 확장된 PAT 테이블
TCP 및 UDP 포트를 균일 범위 1024~65535로 변환	PAT 풀 - 균일 포트 범위
범위 1~1023 포함	PAT 풀 - 예약 포트 포함
블록 할당 활성화	동등 항목 없음
소스 인터페이스 PAT에 IPv6 사용	동등 항목 없음
대상 인터페이스 PAT에 IPv6 사용	고급 - IPv6
규칙 활성화	활성화
이 규칙과 일치하는 DNS 회신 변환	고급 - 이 규칙과 일치하는 DNS 회신 변환
이그레스 인터페이스에서 프록시 ARP 비활성화	고급 - 대상 인터페이스에서 ARP 프록시 설정 안 함
라우트 테이블을 조회하여 이그레스 인터페이스 찾기	동등 항목 없음
방향	고급 - 단방향
설명	설명

네트워크 개체 및 네트워크 개체 그룹 변환

네트워크 개체와 네트워크 개체 그룹은 IP 주소 또는 호스트 이름을 식별합니다. ASA 및 Firepower Threat Defense 둘 다에서 이러한 개체와 그룹을 액세스 규칙 및 NAT 규칙에 모두 사용할 수 있습니다.

ASA에서 네트워크 개체는 호스트, 네트워크 IP 주소, IP 주소의 범위 또는 FQDN(Fully Qualified Domain Name)을 포함할 수 있습니다. Firepower System에서 네트워크 개체는 FQDN을 제외하고 이와 동일한 값을 지원합니다.

마이그레이션 툴은 개체가 여러 액세스 규칙 또는 NAT 규칙에서 사용되는지 여부에 관계없이 ASA 네트워크 개체 또는 그룹을 한 번 변환합니다.

네트워크 개체 변환

마이그레이션 툴은 변환하는 각 ASA 네트워크 개체에 대해 Firepower 네트워크 개체를 생성합니다.

마이그레이션 툴은 ASA 네트워크 개체의 필드를 다음과 같이 Firepower 네트워크 개체의 필드로 변환합니다.

표 ***15: ASA*** 네트워크 개체 필드 및 이 필드가 매핑되는 ***Firepower*** 네트워크 개체 필드

ASA 네트워크 개체 필드	**Firepower** 네트워크 개체 필드
이름	시스템 생성. 참조 항목: 변환된 컨피그레이션의 명명 규칙, 18 페이지
유형	유형
IP 버전	동등 필드 없음
IP 주소	값
넷마스크	값(CIDR 표기법에 포함됨)
설명	설명
개체 NAT 주소	동등 필드 없음

예**: ACL(Access Control List)**의 네트워크 개체

ASA 컨피그레이션 파일에 다음 명령이 있는 경우

```
object network obj1
 host 1.2.3.4
```

```
object network obj2
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
access-list sample_acl extended permit ip object obj1 object obj2
access-list sample_acl extended permit ip object obj3 object obj1
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

이러한 개체가 다음과 같이 변환됩니다.

이름	도메인	값(네트워크)	유형	재정의
obj1	없음	1.2.3.4	호스트	False
obj2	없음	1.2.3.7~1.2.3.10	주소 범위	False
obj3	없음	10.83.0.0/16	네트워크	False

예: **NAT** 규칙의 네트워크 개체

ASA 컨피그레이션 파일에 다음 명령이 있는 경우

```
nat (gigabitethernet1/1,gigabitethernet1/2) source static obj1 obj1
```

위의 액세스 규칙 예에 나와 있는 `obj1` 개체를 변환하는 것과 동일한 방식으로 이 규칙의 `obj1` 개체가 변환됩니다.

네트워크 개체 그룹 변환

마이그레이션 툴은 변환하는 각 ASA 네트워크 개체 그룹에 대해 Firepower 네트워크 개체 그룹을 생성합니다. 또한, 그룹에 포함된 개체가 아직 변환되지 않았으면 변환합니다.

마이그레이션 툴은 ASA 네트워크 개체 그룹의 필드를 다음과 같이 Firepower 네트워크 개체 그룹의 필드로 변환합니다.

표 ***16: ASA*** 네트워크 개체 그룹 필드 및 이 필드가 매핑되는 ***Firepower*** 네트워크 개체 그룹 필드

ASA 네트워크 개체 그룹 필드	**Firepower** 네트워크 개체 그룹 필드
그룹 이름	이름
설명	설명
그룹 구성원	값(선택한 네트워크)

예: **ACL(Access Control List)**의 네트워크 개체 그룹

ASA 컨피그레이션 파일에 다음 명령이 있는 경우

```
object network obj1
 host 1.2.3.4
object network obj2
```

```
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
 network-object object obj3
access-list sample_acl extended permit ip object-group obj_group1 any
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

다음 네트워크 그룹이 생성됩니다.

이름	도메인	값(네트워크)	유형	재정의
obj_group1	없음	obj1 obj2 obj3	그룹	False

관련 개체가 아직 변환되지 않은 경우 네트워크 개체 변환, 31 페이지에 설명된 대로 해당 개체가 변환됩니다.

예: **NAT** 규칙의 네트워크 개체 그룹

ASA 컨피그레이션 파일에 다음 명령이 있는 경우

```
nat (interface1,interface2) source static obj_group1 obj_group1
```

위의 액세스 규칙 예에 나와 있는 `obj_group1`을 변환하는 것과 동일한 방식으로 이 규칙의 `obj_group1`이 변환됩니다.

서비스 개체 및 서비스 그룹 변환

ASA에서 서비스 개체 및 서비스 그룹은 프로토콜과 포트를 지정하고 해당 포트를 소스 또는 목적지 포트로 지정합니다. 액세스 규칙과 NAT 규칙 둘 다에서 서비스 개체 및 그룹을 사용할 수 있습니다.

Firepower System에서 포트 개체 및 포트 개체 그룹은 프로토콜과 포트를 지정하지만 액세스 제어, 사전 필터 또는 NAT 규칙에 해당 개체를 추가하는 경우에만 이러한 포트가 소스 또는 목적지 포트로 지정됩니다. 마이그레이션 툴은 Firepower System에서 서비스 개체를 동등한 기능으로 변환하기 위해 서비스 개체를 포트 개체 또는 그룹으로 변환하고 관련 액세스 제어, 사전 필터 또는 NAT 규칙을 특정한 방식으로 변경합니다. 따라서 변환 중에 마이그레이션 툴이 단일 보안 개체 및 관련된 액세스 규칙이나 NAT 규칙을 여러 포트 개체/그룹 및 관련된 액세스 제어, 사전 필터 또는 NAT 규칙으로 확장할 수 있습니다.

서비스 개체 변환

마이그레이션 툴은 하나 이상의 포트 개체와 이러한 포트 개체를 참조하는 하나 이상의 액세스 제어 또는 사전 필터 규칙을 생성하여 ASA 서비스 개체를 변환합니다.

마이그레이션 툴은 다음 서비스 개체 유형을 변환할 수 있습니다.

- 프로토콜
- TCP/UDP
- ICMP/ICMPv6

마이그레이션 툴은 ASA 서비스 개체의 필드를 다음과 같이 Firepower 포트 개체의 필드로 변환합니다.

표 ***17: ASA*** 서비스 개체 필드 및 이 필드가 매핑되는 ***Firepower*** 포트 개체 필드

ASA 서비스 개체 필드	**ASA** 서비스 개체 유형	**Firepower** 포트 개체 필드
이름	모두	시스템 생성(변환된 컨피그레이션의 명명 규칙, 18 페이지 참조)
서비스 유형	TCP/UDP, ICMP/ICMPv6	프로토콜
프로토콜	프로토콜 전용	프로토콜
설명	모두	동등 항목 없음. 콘텐츠가 삭제됨
목적지 포트/범위	TCP/UDP 전용	포트
소스 포트/범위	TCP/UDP 전용	포트
ICMP 유형	ICMP/ICMPv6 전용	Type(유형)
ICMP 코드	ICMP/ICMPv6 전용	코드

서비스 개체의 포트 리터럴 값

ASA 서비스 개체는 포트 번호가 아닌 포트 리터럴 값을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
object service http
 service tcp destination eq www
```

Firepower System은 이러한 포트 리터럴 값을 지원하지 않으므로 마이그레이션 툴은 포트 리터럴 값을 해당 값이 나타내는 포트 번호로 변환합니다. 툴은 위의 예를 다음 포트 개체로 변환합니다.

이름	유형	도메인	값(프로토콜/포트)	재정의
HTTP	개체	없음	TCP(6)/80	False

포트 리터럴 값 및 연결된 포트 번호의 전체 목록은 *CLI* 설명서 *1: Cisco ASA Series* 일반 작업 *CLI* 환경 설정 가이드에서 TCP 및 UDP 포트를 참조하십시오.

서비스 개체의 포트 인수 연산자

ASA 서비스 개체는 포트 인수에 다음 연산자를 사용할 수 있습니다.

표 ***18:*** 서비스 개체의 포트 인수 연산자

연산자	설명	예
`lt`	보다 작음	`object service testOperator` ` service tcp source lt 100`
`gt`	보다 큼	`object service testOperator` ` service tcp source gt 100`
`eq`	같음	`object service http-proxy` ` service tcp source eq 8080`
`neq`	같지 않음	`object service testOperator` ` service tcp source neq 200`
`range`	값의 범위(경계값 포함)	`object service http-proxy` ` service tcp source range 9000 12000`

마이그레이션 툴은 이러한 연산자를 다음과 같이 변환합니다.

표 ***19:*** 포트 인수 연산자가 포함된 서비스 개체 및 이 개체가 변환되는 포트 개체/그룹

연산자	변환 대상	예제 포트 개체 값(프로토콜/포트)
`lt`	지정한 숫자보다 작은 포트 번호 범위를 지정하는 단일 포트 개체	`TCP(6)/1-99`
`gt`	지정한 숫자보다 큰 포트 번호 범위를 지정하는 단일 포트 개체	`TCP(6)/101-65535`
`eq`	단일 포트 번호를 지정하는 단일 포트 개체	`TCP(6)/8080`

`neq`	포트 개체 2개와 포트 개체 그룹 하나. 첫 번째 포트 개체는 지정한 포트보다 작은 범위를 지정합니다. 두 번째 포트 개체는 지정한 포트보다 큰 범위를 지정합니다. 포트 개체 그룹은 두 포트 개체를 모두 포함합니다.	첫 번째 개체(`testOperator_src_1`):
		`TCP(6)/1-199`
		두 번째 개체(`testOperator_src_2`):
		`TCP(6)/201-65535`
		개체 그룹(`testOperator_src`):
		`testOperator_src_1`
		`testOperator_src_2`

`range`	값의 범위(경계값 포함)를 지정하는 단일 포트 개체	`TCP(6)/9000-12000`

소스 및 목적지 포트가 포함된 서비스 개체

ASA에서는 단일 서비스 개체가 소스 및 목적지 포트를 둘 다 지정할 수 있습니다. Firepower System에서는 포트 개체가 포트 값만 지정합니다. 액세스 제어 또는 사전 필터 규칙에 포트 개체를 사용할 때까지 포트가 소스 또는 목적지로 지정되지 않습니다.

마이그레이션 툴은 이러한 차이를 고려하여 소스 및 목적지를 둘 다 지정하는 ASA 서비스 개체를 변환할 때 단일 개체를 두 포트 개체로 확장합니다. 그리고 원본 지정을 나타내기 위해 개체 이름에 확장자를 추가합니다. 소스 포트의 경우 *_src*, 목적지 포트의 경우 *_dst*가 추가됩니다.

예

```
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
```

툴은 이 서비스 개체를 다음 포트 개체로 변환합니다.

이름	유형	도메인	값(프로토콜/포트)	재정의
http-proxy_src	개체	없음	TCP(6)/9000-12000	False
http-proxy_dst	개체	없음	TCP(6)/8080	False

예: 프로토콜 서비스 개체 변환

ASA 컨피그레이션:

```
object service protocolObj1
 service snp
 description simple routing
```

변환 대상:

표 ***20:*** 포트 개체

이름	유형	도메인	값(프로토콜)	재정의
protocolObj1	개체	없음	SNP(109)	False

예: TCP/UDP 서비스 개체 변환

ASA 컨피그레이션:

```
object service servObj1
 service tcp destination eq ssh
```

변환 대상:

표 ***21:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
servObj1	개체	없음	TCP(6)/22	False

예: **ICMP/ICMPv6** 서비스 개체 변환

ICMP

ASA 컨피그레이션:

```
object service servObj1
 service icmp alternate-address 0
```

변환 대상:

표 ***22:*** 포트 개체

이름	유형	도메인	값(프로토콜/유형: 코드)	재정의
servObj1	개체	없음	ICMP(1)/대체 호스트 주소: 호스트의 대체 주소	False

ICMPv6

ASA 컨피그레이션:

```
object service servObj1
 service icmp6 unreachable 0
```

변환 대상:

표 ***23:*** 포트 개체

이름	유형	도메인	값(프로토콜/유형: 코드)	재정의
servObj1	개체	없음	IPV6-ICMP(58)/대상에 연결할 수 없음: 대상에 대한 경로 없음	False

서비스 그룹 변환

마이그레이션 툴은 포트 개체 그룹을 생성하여 관련 액세스 제어 또는 사전 필터 규칙과 연결하는 방식으로 ASA 서비스 그룹을 변환합니다.

마이그레이션 툴은 다음 서비스 그룹 유형을 변환할 수 있습니다.

- 프로토콜
- TCP/UDP
- ICMP/ICMPv6

마이그레이션 툴은 ASA 서비스 개체의 필드를 다음과 같이 Firepower 포트 개체의 필드로 변환합니다.

표 ***24: ASA*** 서비스 그룹 필드 및 이 필드가 매핑되는 ***Firepower*** 포트 개체 필드

ASA 서비스 그룹 필드	포트 개체 그룹 필드
이름	시스템 생성(변환된 컨피그레이션의 명명 규칙, 18 페이지 참조)
설명	설명
그룹 구성원	선택한 포트

중첩된 서비스 그룹 변환

ASA는 중첩된 서비스 그룹, 즉 다른 서비스 그룹을 포함하는 서비스 그룹을 지원합니다. Firepower System은 중첩된 포트 개체 그룹을 지원하지 않습니다. 하지만 단일 액세스 제어 또는 사전 필터 규칙을 여러 그룹에 연결하면 동등한 기능을 얻을 수 있습니다. 마이그레이션 툴은 중첩된 서비스 그룹을 변환할 때 그룹 구조를 "평면화"하여 가장 안쪽 서비스 개체 및 그룹을 포트 개체 및 포트 개체 그룹으로 변환하고 변환된 그룹을 액세스 제어 또는 사전 필터 규칙과 연결합니다.

최대 50개의 포트 개체를 단일 액세스 제어 또는 사전 필터 규칙과 연결할 수 있습니다. 새 포트 개체 수가 50개를 초과하면 툴은 모든 새 포트 개체가 규칙과 연결될 때까지 중복 액세스 제어 또는 사전 필터 규칙을 생성합니다.

소스 및 대상 서비스 둘 다로 사용되는 중첩된 서비스 개체를 포함하는 Firepower System 규칙은 지원되지 않습니다.

예

```
object-group service http-8081 tcp
 port-object eq 80
 port-object eq 81

object-group service http-proxy tcp
```

```
 port-object eq 8080

object-group service all-http tcp
 group-object http-8081
 group-object http-proxy

access-list FMC_inside extended permit tcp host 33.33.33.33 object-group all-http host
33.33.33.33 object-group all-http
```

위의 예에서 서비스 개체 *http 8081* 및 *http-proxy*는 *all-http* 서비스 그룹 내에 중첩됩니다.

이러한 시나리오에서 포트 개체와 관련된 규칙은 무시됩니다. 시스템은 개체를 가져오되 관련 액세스 제어 또는 사전 필터 규칙을 비활성화하며 규칙에 **Nested service groups at both Source and Destination are not supported(**소스 및 대상 둘 다에서 중첩된 서비스 그룹은 지원되지 않습니다**.)**라는 코멘트를 추가합니다.

변환된 서비스 개체, 서비스 그룹 및 시스템이 변환 중에 생성할 수 있는 중복 규칙에 대해 툴이 사용하는 명명 규칙에 대한 설명은 다음 항목을 참조하십시오. 변환된 컨피그레이션의 명명 규칙, 18 페이지

예

ASA 컨피그레이션:

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

변환 대상:

표 ***25:*** 포트 개체 그룹

이름	유형	도메인	값(프로토콜/포트)	재정의
legServGroup1_1	개체	없음	TCP(6)/78	False
legServGroup1_2	개체	없음	TCP(6)/79	False
legServGroup2_1	개체	없음	TCP(6)/80	False
legServGroup2_2	개체	없음	TCP(6)/81	False
legServGroup1	그룹	없음	legServGroup1_1 legServGroup1_2	False
legServGroup2	그룹	없음	legServGroup2_1 legServGroup2_2	False

표 ***26:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모든	모든	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	Permit(허용) 동등 항목	True

예: 프로토콜 서비스 그룹 변환

ASA 컨피그레이션:

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
```

변환 대상:

표 ***27:*** 포트 개체 및 그룹

이름	유형	도메인	값(프로토콜/포트)	재정의
TCPUDP_1	개체	없음	TCP(6)	False
TCPUDP_2	개체	없음	UDP(17)	False
TCPUDP	그룹	없음	TCPUDP_1 TCPUDP_2	False

예: TCP/UDP 서비스 그룹 변환

그룹 생성 중에 생성되는 개체

ASA에서는 서비스 그룹 생성 중에 개체를 즉시 생성할 수 있습니다. 이러한 개체는 서비스 개체로 분류되지만, ASA 컨피그레이션 파일의 항목은 `object service`가 아닌 `port-object`를 사용합니다. 이러한 개체는 독립적으로 생성되지 않으므로 마이그레이션 툴은 그룹 생성과 독립적으로 생성되는 개체에 사용하는 것과 약간 다른 명명 규칙을 사용합니다.

ASA 컨피그레이션:

```
object-group service servGrp5 tcp-udp
 port-object eq 50
 port-object eq 55
```

변환 대상:

표 ***28:*** 포트 개체 및 그룹

이름	유형	도메인	값(프로토콜/포트)	재정의
servGrp5_1	개체	없음	TCP(6)/50	False
servGrp5_2	개체	없음	TCP(6)/55	False
servGrp5	그룹	없음	servGrp5_1 servGrp5_2	False

그룹과 독립적으로 생성되는 개체

ASA 컨피그레이션:

```
object service servObj1
 service tcp destination eq ssh
object service servObj2
 service udp destination eq 22
object service servObj3
 service tcp destination eq telnet
object-group service servGrp1
 service-object object servObj1
 service-object object servObj2
 service-object object servObj3
```

변환 대상:

표 ***29:*** 포트 개체 및 그룹

이름	유형	도메인	값(프로토콜/포트)	재정의
servObj1	개체	없음	TCP(6)/22	False
servObj2	개체	없음	UDP(17)/22	False
servObj3	개체	없음	TCP(6)/23	False
servGrp1	그룹	없음	servObj1 servObj2 servObj3	False

예: ICMP/ICMPv6 서비스 그룹 변환

ICMP

ASA 컨피그레이션:

```
object-group icmp-type servGrp4
 icmp-object echo-reply
```

변환 대상:

표 ***30:*** 포트 개체 및 그룹

이름	유형	도메인	값(프로토콜/포트)	재정의
servGrp4_1	개체	없음	ICMP(1)/에코 응답	False
servGrp4	그룹	없음	servGrp4_1	False

ICMPv6

ASA 컨피그레이션:

```
object-group service servObjGrp3
 service-object icmp6 packet-too-big
 service-object icmp6 parameter-problem
```

변환 대상:

표 ***31:*** 포트 개체 및 그룹

이름	유형	도메인	값(프로토콜/포트)	재정의
servObjGrp3_1	개체	없음	IPV6-ICMP(58)/2	False
servObjGrp3_2	개체	없음	IPV6-ICMP(58)/4	False
servObjGrp3	그룹	없음	servObjGrp3_1 servObjGrp3_2	False

access-group 변환

ASA에서 ACL을 적용하려면 CLI에서 `access-group` 명령을 입력하거나 ASDM 액세스 규칙 편집기에서 **Apply(적용)**를 선택합니다. 이 두 작업을 수행하면 ASA 컨피그레이션 파일에 `access-group` 항목이 생성됩니다(아래 예 참조).

`access-group` 명령은 ACL이 적용되는 인터페이스를 지정하며, 해당 인터페이스에서 ACL을 인바운드(인그레스) 트래픽에 적용할지 아니면 아웃바운드(이그레스) 트래픽에 적용할지를 지정합니다.

FirePOWER System에서 동일한 기능을 구성하려면 다음을 수행합니다.

- 보안 영역을 생성하여 인터페이스와 연결한 다음 액세스 제어 규칙에 해당 보안 영역을 Source Zone(소스 영역) 조건(인바운드 트래픽의 경우) 또는 Destination Zone(대상 영역) 조건(아웃바운드 트래픽의 경우)으로 추가합니다.

- 인터페이스 그룹을 생성하여 인터페이스와 연결한 다음 사전 필터 규칙에 해당 인터페이스 그룹을 Source Interface Group(소스 인터페이스 그룹) 조건(인바운드 트래픽의 경우) 또는 Destination Interface Group(대상 인터페이스 그룹) 조건(아웃바운드 트래픽의 경우)으로 추가합니다.

`access-group` 명령을 변환할 때 마이그레이션 툴은 소스 영역이나 인터페이스 그룹을 생성한 다음 관련 액세스 제어 규칙 또는 사전 필터 규칙에 해당 보안 영역 및 인터페이스 그룹을 조건으로 추가하여 인그레스 및 이그레스 정보를 캡처합니다. 단, 마이그레이션 툴은 보안 영역 또는 인터페이스 그룹 이름의 인터페이스 정보를 유지하지만 관련 인터페이스 또는 디바이스 컨피그레이션은 변환하지 않으므로 변환된 정책을 가져온 후 이러한 컨피그레이션을 수동으로 추가해야 합니다. 변환된 정책을 가져온 후 수동으로 정책을 디바이스와 연결하고, 보안 영역 또는 인터페이스 그룹을 인터페이스와 연결해야 합니다.

ACL을 변환할 때 시스템은 글로벌로 적용되는 규칙을 특정 인터페이스에 적용되는 규칙 뒤에 배치합니다.

특수 사례

ASA 컨피그레이션이 단일 ACL을 인그레스 및 이그레스 인터페이스 둘 다에 적용하는 경우 툴은 ACL을 다음 두 가지 액세스 제어 규칙 또는 사전 필터 규칙 집합으로 변환합니다.

- 인그레스 규칙 집합(활성화됨)
- 이그레스 규칙 집합(비활성화됨)

ASA 컨피그레이션이 단일 ACL을 글로벌로 적용하는 동시에 특정 인터페이스에도 적용하는 경우 툴은 ACL을 다음 두 가지 액세스 제어 규칙 또는 사전 필터 규칙 집합으로 변환합니다.

- 특정 인터페이스와 연결된 규칙 집합(활성화됨)
- 소스 및 대상 영역이 `Any(모두)`로 설정된 규칙 집합(활성화됨)

예: 글로벌로 적용되는 **ACL**

ASA 컨피그레이션:

```
access-list global_access extended permit ip any any
access-group global_access global
```

마이그레이션 툴은 이 컨피그레이션을 다음과 같이 변환합니다.

표 ***32:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역/인터페이스그룹	대상 영역/인터페이스그룹	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
global_access#1	모든	모든	모든	모든	모든	모든	Permit(허용) 동등 항목	True

예: 특정 인터페이스에 적용되는 **ACL**

ASA 컨피그레이션:

```
access-list acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

이 예에서 `access-group` 명령은 `acp1`로 명명된 ACL을 `outside`로 명명된 인터페이스의 인바운드 트래픽에 적용합니다.

마이그레이션 툴은 이 컨피그레이션을 다음과 같이 변환합니다.

표 ***33:*** 보안 영역/인터페이스 그룹

이름	인터페이스 유형	도메인	선택한 인터페이스
acp1_outside_in_zone	• 라우팅됨(ASA 디바이스가 라우팅 모드에서 실행 중인 경우) • 스위칭됨(ASA 디바이스가 Transparent 모드에서 실행 중인 경우)	없음	모두

표 ***34:*** 액세스 제어 또는 사전 필터 규칙

이름	소스영역/인터페이스 그룹	대상 영역/인터페이스 그룹	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	acp1_outside_in_zone	모든	모든	209.165.201.3	Any(모두)	TCP(6)/80	Permit(허용) 동등 항목	True

B 부 록

변환 예

이 섹션에서는 ASA 컨피그레이션 및 마이그레이션 툴이 이러한 컨피그레이션을 변환하는 Firepower Threat Defense 규칙과 개체의 예를 제공합니다.

예

개별 네트워크를 지정하는 액세스 규칙

ASA 컨피그레이션:

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
access-group acp1 global
```

변환 대상:

표 ***35:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모든	모든	3.4.5.0/24	5.6.7.0/24	TCP(6)	모두	Permit(허용) 동등 항목	True

네트워크 개체 그룹이 포함된 액세스 규칙

ASA 컨피그레이션:

```
access-list acp1 extended permit ip object-group host1 object-group host2
access-group acp1 global
```

변환 대상:

표 ***36:*** 네트워크 개체 그룹

이름	도메인	값(네트워크)	유형	재정의
host1	없음	obj1 obj2	그룹	False
host2	없음	obj3 obj4	그룹	False

표 ***37:*** 네트워크 개체 그룹을 사용하는 액세스 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모든	모든	host1	host2	모든	모든	Permit(허용) 동등 항목	True

개별 네트워크와 포트를 지정하는 액세스 규칙

ASA 액세스 규칙:

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 5.6.7.0 255.255.255.0 eq
80
access-group acp1 global
```

변환 대상:

표 ***38:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모든	모든	3.4.5.0/32	5.6.7.0/32	TCP(6)/90	TCP(6)/80	Permit(허용) 동등 항목	True

서비스 개체가 포함된 액세스 규칙

ASA 컨피그레이션:

```
object service servObj1
 service tcp destination eq 78
access-list acp1 extended permit object servObj1 any any
access-group acp1 in interface outside
```

변환 대상:

표 ***39:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
servObj1	개체	없음	TCP(6)/78	False

표 ***40:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모든	모든	모든	모든	모든	servObj1	Permit(허용) 동등 항목	True

서비스 개체 그룹이 포함된 액세스 규칙

ASA 컨피그레이션:

```
object-group service legServGroup tcp
 port-object eq 78
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legServGroup
access-group acp1 global
```

변환 대상:

표 ***41:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
legServGroup	개체	없음	TCP(6)/78	False

표 ***42:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화
acp1#1	모든	모든	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup	Permit(허용) 동등 항목	True

중첩된 서비스 개체 그룹이 포함된 액세스 규칙

ASA 컨피그레이션:

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
```

```
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

변환 대상:

표 ***43:*** 포트 개체 및 그룹

이름	유형	도메인	값(프로토콜/포트)	재정의
legServGroup1_1	개체	없음	TCP(6)/78	False
legServGroup1_2	개체	없음	TCP(6)/79	False
legServGroup2_1	개체	없음	TCP(6)/80	False
legServGroup2_2	개체	없음	TCP(6)/81	False
legServGroup1	그룹	없음	legServGroup1_1 legServGroup1_2	False
legServGroup2	그룹	없음	legServGroup2_1 legServGroup2_2	False

중첩된 그룹인 legacyServiceNestedGrp가 평면화되었으므로 변환된 컨피그레이션에는 해당 그룹과 동등한 항목이 포함되지 않습니다.

표 ***44:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모든	모든	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	Permit(허용) 동등 항목	True

중첩된 확장 서비스 개체 그룹이 포함된 액세스 규칙

ASA 컨피그레이션:

```
object service http
 service tcp source range 9000 12000 destination eq www
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
object-group service all-http
 service-object object http
 service-object object http-proxy
object-group service all-httpz
 group-object all-http
```

```
 service-object tcp destination eq 443
access-list acp1 extended permit object-group all-httpz any any
access-group acp1 in interface inside
```

변환 대상:

표 ***45:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
http_src	개체	없음	TCP(6)/9000-12000	False
http_dst	개체	없음	TCP(6)/80	False
http-proxy_src	개체	없음	TCP(6)/9000-12000	False
http-proxy_dst	개체	없음	TCP(6)/8080	False
all-httpz-dst	그룹	없음	TCP(6)/443	False

중첩된 그룹인 all-httpz가 평면화되었으므로 변환된 컨피그레이션에는 해당 그룹과 동등한 항목이 포함되지 않습니다.

표 ***46:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1_1	모든	모든	모든	모든	http_src	http_dst	Permit(허용) 동등 항목	True
acp1#1_2	모든	모든	모든	모든	http-proxy_src	http-proxy_dst	Permit(허용) 동등 항목	True
acp1#1_3	모든	모든	모든	모든	모든	all-httpz-dst	Permit(허용) 동등 항목	True

"gt" 및 **"neq"** 연산자를 사용하는 서비스 개체가 포함된 액세스 규칙

ASA 컨피그레이션:

```
object service testOperator
 service tcp source gt 100 destination neq 200
access-list acp1 extended permit object testOperator any any
```

변환 대상:

표 ***47:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
testOperator_src	개체	없음	TCP(6)/101-65535	False
testOperator_dst_1	개체	없음	TCP(6)/1-199	False
testOperator_dst_2	개체	없음	TCP(6)/201-65535	False
testOperator_dst	그룹	없음	testOperator_dst_1, testOperator_dst_2	False

표 ***48:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모든	모든	모든	모든	testOperator_src	testOperator_dst	Permit(허용) 동등 항목	True

"lt" 및 **"gt"** 연산자를 사용하는 보안 개체가 포함된 액세스 규칙

ASA 컨피그레이션:

```
object service testOperator
 service tcp source gt 100 destination lt 200
access-list acp1 extended permit object testOperator any any
```

변환 대상:

표 ***49:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
testOperator_src	개체	없음	TCP(6)/101-65535	False
testOperator_dst	개체	없음	TCP(6)/1-199	False

표 ***50:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모두	모든	모든	모두	testOperator_src	testOperator_dst	Permit(허용) 동등 항목	True

"eq" 연산자 및 포트 리터럴 값을 사용하는 **TCP** 서비스 개체가 포함된 액세스 규칙

ASA 컨피그레이션:

```
object service svcObj1
 service tcp source eq telnet destination eq ssh
access-list acp1 extended permit object testOperator any any
```

변환 대상:

표 ***51:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
svcObj1_src	개체	없음	TCP(6)/21	False
svcObj1_dst	개체	없음	TCP(6)/22	False

표 ***52:*** 액세스 제어 또는 사전 필터 규칙

이름	소스영역	대상영역	소스네트워크	대상네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모두	모든	모든	모두	svcObj1_src	svcObj1_dst	Permit(허용) 동등 항목	True

ICMP 서비스 개체가 포함된 액세스 규칙

ASA 컨피그레이션:

```
object-group service icmpObj
 service-object icmp echo-reply 8
 access-list acp1 extended permit object icmpObj any any
```

변환 대상:

표 ***53:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
icmpObj	개체	없음	ICMP(1)/에코 응답	False

표 ***54:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모두	모든	모든	모든	모두	icmpObj	Permit(허용) 동등 항목	True

프로토콜 서비스 개체가 포함된 액세스 규칙

ASA 컨피그레이션:

```
object-group protocol testProtocol
 protocol-object tcp
access-list acp1 extended permit object testProtocol any any
```

변환 대상:

표 ***55:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
testProtocol	개체	없음	TCP(6)	False

표 ***56:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모두	모든	모든	모든	모두	testProtocol	Permit(허용) 동등 항목	True

확장 서비스 개체가 포함된 액세스 규칙(소스에만 해당)

ASA 컨피그레이션:

```
object service serviceObj
 service tcp source eq 300
 service tcp source eq 800
access-list acp1 extended permit object serviceObj any any
```

변환 대상:

표 ***57:*** 포트 개체

이름	유형	도메인	값(프로토콜/포트)	재정의
serviceObj_src_1	개체	없음	TCP(6)/300	False
serviceObj_src_2	개체	없음	TCP(6)/800	False
serviceObj	그룹	없음	serviceObj_src_1 serviceObj_src_2	False

표 ***58:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모두	모든	모든	모든	모두	serviceObj	Permit(허용) 동등 항목	True

확장 서비스 개체가 포함된 액세스 규칙**(**소스 및 대상**)**

ASA 컨피그레이션:

```
object service serviceObj
 service tcp source eq 300 destination eq 400
access-list acp1 extended permit tcp object serviceObj any any
```

변환 대상:

표 ***59:*** 포트 개체

이름	유형	도메인	값**(**프로토콜**/**포트**)**	재정의
serviceObj_src	개체	없음	TCP(6)/300	False
serviceObj_dst	개체	없음	TCP(6)/400	False

표 ***60:*** 액세스 제어 또는 사전 필터 규칙

이름	소스영역	대상영역	소스네트워크	대상네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모두	모든	모든	모두	serviceObj_src	serviceObj_dst	Permit(허용) 동등 항목	True

소스 포트에 포트 인수 연산자 **"neq"**가 포함된 액세스 규칙

ASA 컨피그레이션:

```
access-list acp1 extended permit tcp any neq 300
```

변환 대상:

표 ***61:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모두	모든	모든	모두	1~299, 301~65535	모두	Permit(허용) 동등 항목	True

소스 및 목적지 포트에 포트 인수 연산자 **"neq"**가 포함된 액세스 규칙

ASA 컨피그레이션:

```
access-list acp1 extended permit tcp any neq 300 any neq 400
```

변환 대상:

표 ***62:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1_1	모두	모든	모든	모두	1~299	1~399	Permit(허용) 동등 항목	True
acp1#1_2	모두	모든	모든	모두	301~65535	1~399	Permit(허용) 동등 항목	True
acp1#1_3	모두	모든	모든	모두	1~299	401~65535	Permit(허용) 동등 항목	True
acp1#1_4	모두	모든	모든	모두	301~65535	401~65535	Permit(허용) 동등 항목	True

비활성 액세스 규칙

ASA 컨피그레이션:

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0 inactive
access-group acp1 global
```

변환 대상:

표 ***63:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	모두	모두	3.4.5.0/24	5.6.7.0/24	TCP(6)	모두	Permit(허용) 동등 항목	False

인바운드 트래픽에 적용되는 **ACL(Access Control List)**

ASA 컨피그레이션:

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 in inside
```

변환 대상:

표 ***64:*** 보안 영역/인터페이스 그룹

이름	인터페이스 유형	도메인	선택한 인터페이스
acp1_inside_in_zone	• 라우팅됨(ASA 디바이스가 라우팅 모드에서 실행 중인 경우) • 스위칭됨(ASA 디바이스가 Transparent 모드에서 실행 중인 경우)	없음	모두

표 ***65:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	acp1_inside_in_zone	모두	3.4.5.0/24	모두	TCP(6)/90	TCP(6)/80	Permit(허용) 동등 항목	True

아웃바운드 트래픽에 적용되는 **ACL(Access Control List)**

ASA 컨피그레이션:

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 out outside
```

변환 대상:

표 ***66:*** 보안 영역/인터페이스 그룹

이름	인터페이스 유형	도메인	선택한 인터페이스
acp1_outside_out_zone	• 라우팅됨(ASA 디바이스가 라우팅 모드에서 실행 중인 경우) • 스위칭됨(ASA 디바이스가 Transparent 모드에서 실행 중인 경우)	없음	모두

표 ***67:*** 액세스 제어 또는 사전 필터 규칙

이름	소스 영역	대상 영역	소스 네트워크	대상 네트워크	소스 포트	대상 포트	작업	활성화됨
acp1#1	acp1_outside_out_zone	모두	3.4.5.0/24	모두	TCP(6)/90	TCP(6)/80	Permit(허용) 동등 항목	True