Secure Firewall 마이그레이션 툴 시작하기

Secure Firewall 마이그레이션 툴 정보

이 가이드에는 Secure Firewall 마이그레이션 툴을 다운로드하고 마이그레이션을 완료하는 방법에 대한 정보가 포함되어 있습니다. 또한 발생할 수 있는 마이그레이션 문제를 해결하는 데 도움이 되는 문제 해결 팁도 제공합니다.

이 설명서에 포함된 샘플 마이그레이션 절차(샘플 마이그레이션: FDM 매니지드 디바이스-Threat defense 2100)를 참조하면 마이그레이션 프로세스를 쉽게 이해할 수 있습니다.

Secure Firewall 마이그레이션 툴은 지원되는 FDM 매니지드 디바이스 구성을 지원되는 위협 방어 플랫폼으로 변환합니다. Secure Firewall 마이그레이션 툴을 사용하면 지원되는 FDM 매니지드 디바이스 기능 및 정책을 위협 방어로 자동 마이그레이션할 수 있습니다. 지원되지 않는 모든 기능을 수동으로 마이그레이션해야 할 수 있습니다.

Secure Firewall 마이그레이션 툴은 FDM 매니지드 디바이스 정보를 수집하고 구문 분석한 다음 마지막으로 Secure Firewall Management Center에 푸시합니다. 구문 분석 단계에서 Secure Firewall 마이그레이션 툴은 다음을 식별하는 마이그레이션 전 보고서를 생성합니다.

- FDM 매니지드 디바이스 구성 항목 중 완전히 마이그레이션되는 항목, 부분적으로 마이그레이션되는 항목, 마이그레이션이 지원되지 않는 항목, 마이그레이션에서 무시되는 항목

- Secure Firewall 마이그레이션 툴이 인식할 수 없는 FDM 매니지드 디바이스 구성 요소를 나열하는 오류가 있는 FDM 매니지드 디바이스 구성 라인. 이로 인해 마이그레이션이 차단됩니다.

콘솔

Secure Firewall 마이그레이션 툴을 실행하면 콘솔이 열립니다. 이 콘솔에서는 Secure Firewall 마이그레이션 툴의 각 단계 진행 상황에 대한 자세한 정보를 제공합니다. 콘솔의 내용은 Secure Firewall 마이그레이션 툴 로그 파일에도 작성됩니다.

Secure Firewall 마이그레이션 툴이 열려 실행 중인 동안에는 콘솔이 열려 있어야 합니다.

중요 웹 인터페이스가 실행 중인 브라우저를 닫아 Secure Firewall 마이그레이션 툴을 종료하면 콘솔은 백그라운드에서 계속 실행됩니다. Secure Firewall 마이그레이션 툴을 완전히 종료하려면 키보드에서 Command 키 + C를 눌러 콘솔을 종료합니다.

로그

Secure Firewall 마이그레이션 툴은 각 마이그레이션의 로그를 생성합니다. 로그에는 마이그레이션의 각 단계에서 어떤 일이 발생하는지에 대한 세부 정보가 포함되며, 마이그레이션이 실패할 경우 원인을 파악하는 데 도움이 될 수 있습니다.

Secure Firewall 마이그레이션 툴의 로그 파일은 다음 위치에서 찾을 수 있습니다.
`<migration_tool_folder>\logs`

리소스

Secure Firewall 마이그레이션 툴은 마이그레이션 전 보고서, 마이그레이션 후 보고서, FDM 매니지드 디바이스 구성 및 `resources`(리소스) 폴더에 있는 로그의 사본을 저장합니다.

`resources` 폴더는 다음 위치에서 찾을 수 있습니다. `<migration_tool_folder>\resources`

구문 분석되지 않은 파일

구문 분석되지 않은 파일은 다음 위치에서 찾을 수 있습니다.
`<migration_tool_folder>\resources`

Secure Firewall 마이그레이션 툴에서 검색

Optimize, Review and Validate(최적화**,** 검토 및 검증**)** 페이지의 항목과 같이 Secure Firewall 마이그레이션 툴에 표시되는 테이블의 항목을 검색할 수 있습니다.

테이블의 열 또는 행에서 항목을 검색하려면 테이블 위의 검색( )를 클릭하고 필드에 검색어를 입력합니다. Secure Firewall 마이그레이션 툴이 테이블 행을 필터링하고 검색어가 포함된 행만 표시합니다.

단일 열에서 항목을 검색하려면 열 제목에 있는 **Search(**검색**)** 필드에 검색어를 입력합니다. Secure Firewall 마이그레이션 툴이 테이블 행을 필터링하고 검색어와 일치하는 행만 표시합니다.

포트

Secure Firewall 마이그레이션 툴은 포트 8321-8331 및 포트 8888의 12개 포트 중 하나에서 실행할 때 텔레메트리를 지원합니다. 기본적으로 Secure Firewall 마이그레이션 툴은 포트 8888을 사용합니다. 포트를 변경하려면 `app_config` 파일에서 포트 정보를 업데이트합니다. 업데이트 후 포트 변경 사항을 적용하려면 Secure Firewall 마이그레이션 툴을 다시 실행해야 합니다. `app_config` 파일은 다음 위치에서 찾을 수 있습니다. *<migration_tool_folder>*\app_config.txt.

참고 텔레메트리는 이러한 포트에서만 지원되므로 포트 8321-8331 및 포트 8888을 사용하는 것이 좋습니다. Cisco Success Network를 활성화하는 경우 Secure Firewall 마이그레이션 툴에 다른 포트를 사용할 수 없습니다.

Cisco Success Network

Cisco Success Network는 사용자가 활성화하는 클라우드 서비스입니다. Cisco Success Network를 활성화하는 경우, Secure Firewall 마이그레이션 툴과 Cisco 클라우드 사이에 보안 연결이 설정되어 사용 정보와 통계가 스트리밍됩니다. 스트리밍 텔레메트리는 Secure Firewall 마이그레이션 툴에서 관심 있는 데이터를 선택하고 구조화된 형식으로 원격 관리 스테이션에 전송하여 다음과 같은 이점을 얻을 수 있는 메커니즘을 제공합니다.

- 네트워크에서 제품의 효율성을 향상시킬 수있는 활용 가능한 미사용 기능을 알려줍니다.
- 제품에 사용할 수 있는 추가 기술 지원 서비스 및 모니터링에 대해 알려줍니다.
- Cisco가 제품을 개선할 수 있습니다.

Secure Firewall 마이그레이션 툴은 보안 연결을 설정하고 유지하며 Cisco Success Network에 등록할 수 있도록 지원합니다. Cisco Success Network를 비활성화하여 언제든지 이 연결을 끌 수 있으며, 이 경우 디바이스와 Cisco Success Network 클라우드의 연결이 끊어집니다.

Secure Firewall 마이그레이션 툴 최신 기능

버전	지원 기능
4.0.1	Secure Firewall 마이그레이션 툴 4.0.1에는 다음과 같은 새로운 기능 및 개선 사항이 포함되어 있습니다. Secure Firewall 마이그레이션 툴은 이제 이름과 구성을 기반으로 모든 개체 및 개체 그룹을 분석하고 동일한 이름 및 구성을 가진 개체를 재사용합니다. 이전에는 이름 및 구성을 기준으로 네트워크 개체 및 네트워크 개체 그룹만 분석되었습니다. 원격 액세스 VPN의 XML 프로파일은 여전히 이름을 사용해서만 검증됩니다.

버전	지원 기능
4.0	Secure Firewall 마이그레이션 툴 4.0은 다음을 지원합니다. 대상 Management Center 버전이 7.3 이상이고 소스 Device Manager 버전이 7.2 이상인 경우 FDM 매니지드 디바이스를 Management Center로 마이그레이션합니다. Device Manager의 버전은 대상 Management Center의 버전과 같거나 낮은 버전이어야 합니다. 마이그레이션에는 다음 옵션을 사용할 수 있습니다. 1. **Firepower Device Manager** 마이그레이션**(**공유 구성만 해당**)**: 이 옵션을 사용하면 준비된 마이그레이션을 마이그레이션할 수 있습니다. 이 경우 요구 사항에 따라 초기에 모든 공유 구성을 마이그레이션하고 이후 단계에서 디바이스 구성을 마이그레이션할 수 있습니다. 마이그레이션 프로세스 중에는 공유 구성만 대상 Management Center로 마이그레이션됩니다. Device Manager에서 가져온 구성 번들을 업로드하거나, 툴에 대해 Device Manager 자격 증명을 제공하여 구성 세부 정보를 가져올 수 있습니다. 구성 세부 정보를 자동으로 가져오는 것이 기본 방법입니다. 2. **Firepower Device Manager** 마이그레이션**(**디바이스 및 공유 구성 포함**)**: 이 옵션을 사용하면 디바이스 및 공유 구성을 Device Manager에서 대상 Management Center로 마이그레이션할 수 있습니다. 소스 디바이스 및 해당 구성이 대상 Management Center로 마이그레이션되면 FDM 매니지드 디바이스가 대상 Management Center 디바이스가 됩니다. 툴이 구성 세부 정보를 가져오려면 Device Manager 자격 증명을 제공해야 합니다. 이 마이그레이션 옵션에는 구성의 자동화된 가져오기만 허용됩니다. 3. **Firepower Device Manager(**디바이스 및 공유 구성 포함**)**를 **FTD** 디바이스**(**새 하드웨어**)**로 마이그레이션: 이 옵션을 사용하면 디바이스 및 공유 구성을 대상 Management Center에서 관리하는 Threat Defense 디바이스로 마이그레이션할 수 있습니다. 이 경우 마이그레이션 프로세스 중에 소스 디바이스가 마이그레이션되지 않고 디바이스 구성만 새 Threat Defense 디바이스로 마이그레이션됩니다. Device Manager에서 가져온 구성 번들을 업로드하거나, 툴에 대해 Device Manager 자격 증명을 제공하여 구성 세부 정보를 가져올 수 있습니다. 구성 세부 정보를 자동으로 가져오는 것이 기본 방법입니다.

Secure Firewall 마이그레이션 툴의 플랫폼 요구 사항

Secure Firewall 마이그레이션 툴에는 다음과 같은 인프라 및 플랫폼 요구 사항이 있습니다.

- Microsoft Windows 10 64비트 운영체제 또는 macOS 10.13 이상 버전에서 실행
- Google Chrome을 시스템 기본 브라우저로 사용

- (Windows) 대규모 마이그레이션 푸시 중에 시스템이 절전 모드로 전환되지 않도록 Power & Sleep(전원 및 절전)에서 Sleep(절전) 설정을 Never put the PC to Sleep(절전 모드로 전환 안 함)으로 구성
- (macOS) 대규모 마이그레이션 푸시 중에 컴퓨터와 하드 디스크가 절전 모드로 전환되지 않도록 Energy Saver(에너지 절약) 설정 구성

FDM 매니지드 디바이스 구성 파일에 대한 요구 사항 및 사전 요건

FDM 매니지드 디바이스 구성 번들은 수동으로 또는 Secure Firewall 마이그레이션 툴에서 라이브 FDM 매니지드 디바이스에 연결하여 얻을 수 있습니다. 수동 업로드는 다음 옵션에 대해서만 지원됩니다.

- Firepower Device Manager(디바이스 및 공유 구성 포함)를 FTD 디바이스(새 하드웨어)로 마이그레이션
- Firepower Device Manager 마이그레이션(공유 구성만 해당)

참고 **Firepower Device Manager** 마이그레이션**(**디바이스 및 공유 구성 포함**)** 옵션에 대해서는 수동 업로드가 지원되지 않습니다.

Secure Firewall 마이그레이션 툴에 수동으로 가져오는 FDM 매니지드 디바이스 구성 번들은 다음 요구 사항을 충족해야 합니다.

- 유효한 Device Manager CLI 구성만 포함하고 있습니다.
- 버전 번호를 포함하고 있습니다.
- 구성 번들은 .zip 형식이어야 합니다.
- Device Manager에서 내보낸 완전 추출 구성이 있습니다. FDM 매니지드 디바이스 구성 파일 내보내기, 28 페이지를 참고하십시오.
- 구성이 있는 .txt 파일이 하나 이상 있어야 합니다.
- 암호화된 번들에 대한 키를 제공해야 합니다. 암호화되지 않은 번들의 경우 암호화 키를 비워둘 수 있습니다.
- 구문 오류가 없습니다.
- 직접 코딩하거나 수동으로 변경하지 않았습니다.

Threat Defense 디바이스의 요구 사항 및 사전 요건

Management Center로 마이그레이션할 때 대상 Threat Defense 디바이스가 추가되거나 추가되지 않을 수 있습니다. 나중에 Threat Defense 디바이스에 구축하도록 공유 정책을 Management Center로 마이그레이션할 수 있습니다. 디바이스별 정책을 Threat Defense로 마이그레이션하려면 Management Center에 추가해야 합니다. FDM 매니지드 디바이스 구성을 Threat Defense로 마이그레이션하려는 경우 다음 요구 사항 및 사전 요건을 고려하십시오.

- Threat Defense 하드웨어는 FDM 매니지드 디바이스 모델보다 크거나 같아야 합니다. 예를 들어, 소스 FDM 매니지드 디바이스 모델이 2100인 경우 대상 Threat Defense 모델은 2100, 3100, 4100 또는 9300이 될 수 있으며, 2100보다 낮은 모델은 불가능합니다.
- 대상 Threat Defense 디바이스를 Management Center에 등록해야 합니다.
- Threat Defense 디바이스는 독립형 디바이스 또는 컨테이너 인스턴스일 수 있습니다. 클러스터 또는 고가용성 컨피그레이션의 일부가 아니어야 합니다.
  - 대상 네이티브 Threat Defense 디바이스에서 최소한 FDM 매니지드 디바이스와 같은 수의 물리적 데이터 및 포트 채널 인터페이스('관리 전용' 및 하위 인터페이스 제외)를 사용해야 합니다. 그렇지 않은 경우 대상 Threat Defense 디바이스에 필요한 인터페이스 유형을 추가해야 합니다. 하위 인터페이스는 물리적 또는 포트 채널 매핑을 기반으로 Secure Firewall 마이그레이션 툴에서 생성됩니다.
  - 대상 Threat Defense 디바이스가 컨테이너 인스턴스인 경우 최소한 FDM 매니지드 디바이스와 같은 수의 물리적 인터페이스, 물리적 하위 인터페이스, 포트 채널 인터페이스 및 포트 채널 하위 인터페이스('관리 전용' 제외)를 사용해야 합니다. 그렇지 않은 경우 대상 Threat Defense 디바이스에 필요한 인터페이스 유형을 추가해야 합니다.

참고

- 하위 인터페이스는 Secure Firewall 마이그레이션 툴로 생성되지 않으며 인터페이스 매핑만 허용됩니다.
- 서로 다른 인터페이스 유형에 대한 매핑이 허용됩니다. 예를 들어, 물리적 인터페이스를 포트 채널 인터페이스에 매핑할 수 있습니다.

FDM 매니지드 디바이스 구성 지원

지원되는 **FDM** 매니지드 디바이스 구성

Secure Firewall 마이그레이션 툴은 다음 FDM 매니지드 디바이스 구성을 완전히 마이그레이션할 수 있습니다.

- 네트워크 개체 및 그룹

- 서비스 개체(소스 및 대상에 대해 구성된 서비스 개체 제외)

참고 Secure Firewall 마이그레이션 툴은 소스 및 대상에 대해 구성된 확장 서비스 개체를 마이그레이션하지 않지만, 참조된 ACL 및 NAT 규칙은 전체 기능으로 마이그레이션됩니다.

- 서비스 개체 그룹(중첩된 서비스 개체 그룹 제외)

참고 management center에서 중첩이 지원되지 않으므로 Secure Firewall 마이그레이션 툴은 참조된 규칙의 내용을 확장합니다. 단, 규칙은 전체 기능을 통해 마이그레이션됩니다.

- IPv4 및 IPv6 FQDN 개체 및 그룹
- IPv6 변환 지원(인터페이스, 정적 경로, 개체, ACL 및 NAT)
- 액세스 제어 정책
- 자동 NAT 및 수동 NAT
- 정적 경로, ECMP 경로
- 물리적 인터페이스
- FDM 매니지드 디바이스 인터페이스의 보조 VLAN은 Threat Defense에 마이그레이션되지 않습니다.
- 하위 인터페이스(하위 인터페이스 ID는 마이그레이션 시 항상 VLAN ID와 동일한 숫자로 설정됨)
- 포트 채널
- Virtual tunnel interface(VTI)
- 브리지 그룹(투명 모드만)
- IP SLA 모니터링

  Secure Firewall 마이그레이션 툴에서 IP SLA 개체를 생성하고, 개체를 특정 정적 경로와 매핑하고, 개체를 management center로 마이그레이션합니다.

  IP SLA 모니터는 모니터링되는 주소에 대한 연결 정책을 정의하며, IP 주소에 대한 경로의 가용성을 추적합니다. 정적 경로는 ICMP 에코 요청을 전송하고 응답을 기다리며 주기적으로 가용성을 확인합니다. 에코 요청이 시간 초과되면 정적 경로는 라우팅 테이블에서 제거되고 백업 경로로 교체됩니다. SLA 모니터링 작업은 구축 후 즉시 시작되고 SLA 모니터를 디바이스 구성에서 제거하지 않는 이상 계속 실행됩니다. 즉, 만료되지 않습니다. IP SLA 모니터 개체는 IPv4 정적 경로 정책의 경로 추적 필드에 사용됩니다. IPv6 경로에는 경로 추적을 통해 SLA 모니터를 사용하기 위한 옵션이 없습니다.

- 개체 그룹 검색

  개체 그룹 검색을 활성화하면 네트워크 개체를 포함하는 액세스 컨트롤 정책에 대한 메모리 요구 사항이 감소합니다. Threat Defense의 액세스 정책을 통해 최적의 메모리 사용을 촉진하는 개체 그룹 검색을 활성화하는 것이 좋습니다.

참고

- management center 또는 Threat Defense 6.6 이전 버전에서는 개체 그룹 검색을 사용할 수 없습니다.
- 개체 그룹 검색은 공유 구성 플로우에 대해 지원되지 않으므로 비활성화됩니다.
- 시간 기반 개체

- 시간 기반 개체

  Secure Firewall 마이그레이션 툴이 액세스 규칙을 참조하는 시간 기반 개체를 탐지하면 Secure Firewall 마이그레이션 툴은 시간 기반 개체를 마이그레이션하고 개별 액세스 규칙과 매핑합니다. **Review and Validate Configuration(**컨피그레이션 검토 및 검증**)** 페이지의 규칙에 따라 개체를 검증합니다.

  시간 기반 개체는 시간 기간을 기준으로 네트워크 액세스를 허용하는 액세스 목록 유형입니다. 특정 시간 또는 요일을 기준으로 아웃바운드 또는 인바운드 트래픽을 제한해야 하는 경우 유용합니다.

참고 소스 FDM 매니지드 디바이스에서 대상 FTD로 표준 시간대 구성을 수동으로 마이그레이션해야 합니다.

- 사이트 대 사이트 VPN 터널
  - 사이트 대 사이트 VPN - Secure Firewall 마이그레이션 툴이 소스 FDM 매니지드 디바이스에서 암호화 맵 구성을 탐지하면 Secure Firewall 마이그레이션 툴은 암호화 맵을 Point-to-Point 토폴로지로 management center VPN에 마이그레이션합니다.
  - FDM 매니지드 디바이스의 암호화 맵(정적/유동) 기반 VPN
  - 경로 기반(VTI) 기반 FDM VPN
  - FDM 매니지드 디바이스의 인증서 기반 VPN 마이그레이션
  - management center로의 FDM 매니지드 디바이스 트러스트 포인트 또는 인증서 마이그레이션은 수동으로 수행해야 하며, 마이그레이션 전 활동의 일부입니다.

- 유동 경로 개체, BGP 및 EIGRP
  - Policy-List
  - Prefix-List

- 커뮤니티 목록
- AS(Autonomous System)-경로

- 원격 액세스 VPN
  - SSL 및 IKEv2 프로토콜
  - 인증 방법 - AAA 전용, 클라이언트 인증서 전용, SAML, AAA, 클라이언트 인증서
  - AAA - Radius, 로컬, LDAP 및 AD
  - 연결 프로파일, 그룹-정책, Dynamic Access Policy, LDAP 속성 맵, 인증서 맵
  - 표준 및 확장 ACL
  - 마이그레이션 전 활동의 일부로 다음을 수행합니다.
    - FDM 매니지드 디바이스 트러스트 포인트를 management center에 PKI 개체로 수동 마이그레이션합니다.
    - 소스 FDM 매니지드 디바이스에서 AnyConnect 패키지, Hostscan 파일(Dap.xml, Data.xml, Hostscan 패키지), 외부 브라우저 패키지 및 AnyConnect 프로파일을 검색합니다.
    - 모든 AnyConnect 패키지를 management center에 업로드합니다.
    - AnyConnect 프로파일을 management center에 직접 업로드하거나 Secure Firewall 마이그레이션 툴에서 업로드합니다.

부분적으로 지원되는 **FDM** 매니지드 디바이스 구성

Secure Firewall 마이그레이션 툴은 다음 FDM 매니지드 디바이스 구성의 마이그레이션을 부분적으로 지원합니다. 이러한 컨피그레이션 중 일부에는 고급 옵션을 포함하며 고급 옵션 없이 마이그레이션되는 규칙이 있습니다. management center에서 이러한 고급 옵션을 지원하는 경우 마이그레이션이 완료된 후 수동으로 구성할 수 있습니다.

- 심각도 및 시간 간격과 같은 고급 기록 설정으로 구성된 액세스 제어 정책 규칙.
- 추적 옵션으로 구성된 정적 경로.
- 인증서 기반 VPN 마이그레이션.
- 유동 경로 개체, EIGRP 및 BGP.
  - Route-Map

지원되지 않는 **FDM** 매니지드 디바이스 구성

Secure Firewall 마이그레이션 툴은 다음 FDM 매니지드 디바이스 구성의 마이그레이션을 지원하지 않습니다. management center에서 이러한 구성을 지원하는 경우 마이그레이션이 완료된 후 수동으로 구성을 구성할 수 있습니다.

- SGT 기반 액세스 제어 정책 규칙
- SGT 기반 개체
- 사용자 기반 액세스 제어 정책 규칙
- 블록 할당 옵션으로 구성된 NAT 규칙
- 지원되지 않는 ICMP 유형 및 코드가 포함된 개체
- 터널링 프로토콜 기반 액세스 제어 정책 규칙

참고 Secure Firewall 마이그레이션 툴 및 management center 6.5에서 사전 필터를 지원합니다.

- SCTP로 구성된 NAT 규칙
- 호스트 '0.0.0.0'으로 구성된 NAT 규칙
- SLA 추적으로 DHCP 또는 PPPoE를 통해 얻은 기본 경로
- SLA 모니터 스케줄
- 전송 모드 IPsec transform-set
- management center로의 FDM 매니지드 디바이스 트러스트 포인트 마이그레이션
- BGP용 투명 방화벽 모드

FDM 매니지드 디바이스 및 **Threat Defense**의 개체

FDM 매니지드 디바이스 구성 파일에는 Threat Defense로 마이그레이션할 수 있는 다음과 같은 개체가 포함되어 있습니다.

- 네트워크 개체
- 서비스 개체(Threat Defense에서는 포트 개체라고 함)
- IP SLA 개체
- 시간 기반 개체
- VPN 개체(IKEv1/IKEv2 정책, IKEv1/IKEv2 IPsec-Proposal)
- 유동 경로 개체(정책 목록, 접두사 목록, 커뮤니티 목록, AS 경로, 액세스 목록 및 루트 맵)
- 라우팅 모드에서 지원되는 BGP 및 EIGRP
- RA VPN 개체
- 그룹 정책
- AAA 개체(Radius, SAML, 로컬 영역, AD/LDAP/LDAPS 영역)

- 주소 풀(IPv4 및 IPv6)
- 연결 프로파일
- LDAP 속성 맵
- IKEv2 정책
- IKEv2 IPsec-Proposal
- 인증서 맵
- DAP
- 침입 정책
- 침입 규칙

지침 및 제한 사항

FDM 매니지드 디바이스 마이그레이션 지침

다음은 Secure Firewall 마이그레이션 툴을 사용하여 FDM 매니지드 디바이스 구성을 마이그레이션하기 위한 지침입니다.

- 각 FDM 매니지드 디바이스 개체에 고유한 이름과 구성이 있음 - Secure Firewall 마이그레이션 툴은 변경 없이 개체를 마이그레이션합니다.
- FDM 매니지드 디바이스 개체의 이름에 Management Center에서 지원하지 않는 특수 문자가 하나 이상 포함되어 있음 - Secure Firewall 마이그레이션 툴은 개체 이름의 특수 문자 이름을 "_" 문자로 변경하여 Management Center 개체 명명 기준을 충족합니다.
- FDM 매니지드 디바이스 개체의 이름과 구성이 Management Center의 기존 개체와 동일 - Secure Firewall 마이그레이션 툴은 Threat Defense 구성을 위해 Management Center 개체를 재사용하고 FDM 매니지드 디바이스 개체를 마이그레이션하지 않습니다.
- 여러 FDM 매니지드 디바이스 개체가 대소문자가 다르지만 이름이 같음 - Secure Firewall 마이그레이션 툴이 Threat Defense 개체 명명 기준에 맞게 이름을 바꿉니다.

중요 Secure Firewall 마이그레이션 툴은 모든 개체 및 개체 그룹의 이름과 구성을 전부 분석합니다. 그러나 원격 액세스 VPN 구성의 XML 프로파일은 이름만 사용하여 분석됩니다.

FDM 매니지드 디바이스 구성 제한 사항

소스 FDM 매니지드 디바이스 구성을 마이그레이션하는 경우 다음과 같은 제한 사항이 있습니다.

- 지원되지 않는 개체 및 NAT 규칙은 마이그레이션되지 않습니다.

- 지원되지 않는 ACL 규칙은 비활성화된 규칙으로 Management Center에 마이그레이션됩니다.
- 지원되는 모든 FDM 매니지드 디바이스 암호화 맵 VPN은 Management Center Point-to-Point 토폴로지로 마이그레이션됩니다.
- 지원되지 않거나 불완전한 정적 암호화 맵 VPN 토폴로지는 마이그레이션되지 않습니다.
- 일부 FDM 매니지드 디바이스 구성(예: 유동 라우팅을 Threat Defense로 마이그레이션)은 마이그레이션할 수 없습니다. 이러한 컨피그레이션은 수동으로 마이그레이션해야 합니다.
- 중첩된 서비스 개체 그룹 또는 포트 그룹은 Management Center에서 지원되지 않습니다. 변환 과정에서 Secure Firewall 마이그레이션 툴은 참조된 중첩 개체 그룹 또는 포트 그룹의 콘텐츠를 확장합니다.
- Secure Firewall 마이그레이션 툴은 한 라인에 있는 소스 및 대상 포트를 포함한 확장 서비스 개체 또는 그룹을 여러 라인에 걸친 서로 다른 개체로 분할합니다. 이러한 액세스 제어 규칙에 대한 참조는 정확히 동일한 의미의 Management Center 규칙으로 변환됩니다.
- 소스 FDM 매니지드 디바이스 구성에 특정 터널링 프로토콜(예: GRE, IP-in-IP 및 IPv6-in-IP)을 참조하지 않는 액세스 제어 규칙이 있지만 이러한 규칙이 FDM 매니지드 디바이스의 암호화되지 않은 터널 트래픽과 일치하는 경우, Threat Defense로 마이그레이션 시 해당 규칙이 FDM 매니지드 디바이스에서와 동일한 방식으로 동작하지 않습니다. Threat Defense에서 사전 필터 정책에 이에 대한 특정 터널 규칙을 생성하는 것이 좋습니다.
- 지원되는 FDM 매니지드 디바이스 암호화 맵은 Point-to-Point 토폴로지로 마이그레이션됩니다.
- Management Center에 동일한 이름의 AS 경로 개체가 표시되면 다음 오류 메시지와 함께 마이그레이션이 중지됩니다.

  "충돌하는 AS 경로 개체 이름이 management center에서 탐지되었습니다. 계속 진행하려면 management center의 충돌을 해결하십시오."
- 경로 맵 개체가 Secure Firewall 마이그레이션 툴을 사용하여 부분적으로 마이그레이션됩니다. API 제한으로 인해 match 및 set 절은 지원되지 않습니다.
- ID 정책, SSL 정책, 악성코드, 파일 정책, 보안 인텔리전스, SGT, 사용자 기반 규칙 및 플랫폼 설정과 같은 레이어 7 정책은 API 제한으로 인해 마이그레이션되지 않습니다.

RA VPN 마이그레이션에 대한 제한 사항

원격 액세스 VPN 마이그레이션은 다음과 같은 제한 사항과 함께 지원됩니다.

- 사용자 지정 속성, SSL 설정 및 VPN 로드 밸런싱 마이그레이션은 API 제한으로 인해 지원되지 않습니다.
- LDAP 서버가 암호화 유형이 "none(없음)"인 상태로 마이그레이션됩니다.
- 정책이 전체 management center에 적용되므로 DfltGrpPolicy는 마이그레이션되지 않습니다. management center에서 직접 필요한 변경을 수행할 수 있습니다.
- Radius 서버의 경우 유동 권한 부여가 활성화되면 AAA 서버 연결은 유동 라우팅이 아닌 인터페이스를 통해 이루어져야 합니다. 인터페이스 없이 유동 권한 부여가 활성화된 AAA 서버에서

FDM 매니지드 디바이스 구성이 발견되면 Secure Firewall 마이그레이션 툴은 유동 권한 부여를 무시합니다. Management Center에서 인터페이스를 선택한 후 유동 권한 부여를 수동으로 활성화해야 합니다.

- 우회 액세스 제어 sysopt permit-vpn 옵션은 RA VPN 정책에서 활성화되지 않습니다. 그러나 필요한 경우 Management Center에서 활성화할 수 있습니다.
- 프로파일이 Secure Firewall 마이그레이션 툴에서 Management Center로 업로드된 경우에만 AnyConnect 클라이언트 모듈 및 프로파일 값을 그룹 정책에 따라 업데이트할 수 있습니다.
- Management Center에서 직접 인증서를 매핑해야 합니다.
- IKEv2 매개변수는 기본적으로 마이그레이션되지 않습니다. Management Center를 통해 추가해야 합니다.

마이그레이션에 지원되는 플랫폼

다음 FDM 매니지드 디바이스 및 위협 방어 플랫폼은 Secure Firewall 마이그레이션 툴을 사용한 마이그레이션에 지원됩니다. 지원되는 위협 방어 플랫폼에 대한 자세한 내용은 Cisco Secure Firewall 호환성 가이드에서 참고하십시오.

지원되는 소스 **FDM** 매니지드 디바이스 플랫폼

Firewall 마이그레이션 툴을 사용하여 다음과 같은 FDM 매니지드 디바이스 플랫폼에서 구성을 마이그레이션할 수 있습니다.

- Firepower 1000 Series
- Firepower 2100 시리즈
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Firepower 9300 시리즈
- VMware, AWS, Azure, KVM의 FDM 가상

지원되는 대상 **Threat Defense** 플랫폼

Secure Firewall 마이그레이션 툴을 사용하여 소스 구성을 위협 방어 플랫폼의 다음과 같은 독립형 또는 컨테이너 인스턴스로 마이그레이션할 수 있습니다.

- Firepower 1000 Series
- Firepower 2100 시리즈
- Secure Firewall 3100 Series
- Firepower 4100 Series

- 다음을 포함하는 Firepower 9300 시리즈:
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- VMware ESXi, VMware vSphere Web Client 또는 vSphere 독립형 클라이언트를 사용하여 구축된 VMware 기반 Threat Defense
- Microsoft Azure Cloud 또는 AWS 클라우드 기반 Threat Defense Virtual

참고

- Azure의 threat defense virtual사전 요건 및 사전 스테이징에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense Virtual 시작하기 및 Azure를 참고하십시오.
- AWS 클라우드의 threat defense virtual 사전 요구 사항 및 사전 스테이징에 대한 자세한 내용은 Threat Defense Virtual 사전 요건을 참고하십시오.

이러한 각 환경에서 요건에 따라 사전 스테이징된 후 Secure Firewall 마이그레이션 툴에는 Microsoft Azure 또는 AWS 클라우드에서 management center에 연결하고 클라우드의 management center로 구성을 마이그레이션하기 위한 네트워크 연결이 필요합니다.

참고 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션을 성공적으로 수행하려면 먼저 management center 또는 Threat Defense Virtual을 사전 스테이징하는 사전 요건을 충족해야 합니다.

마이그레이션에 지원되는 대상 Management Center

Secure Firewall 마이그레이션 툴은 Management Center 및 클라우드 사용 Firewall Management Center에서 관리하는 Threat Defense 디바이스로의 마이그레이션을 지원합니다.

Management Center

Management Center는 자체 서버 하드웨어에서 실행되거나 하이퍼바이저에서 가상 디바이스로 실행되는 강력한 웹 기반 다중 디바이스 관리자입니다. 온프레미스 및 가상 Management Center를 모두 마이그레이션을 위한 대상 Management Center로 사용할 수 있습니다.

Management Center는 마이그레이션에 대한 다음 지침을 충족해야 합니다.

- 마이그레이션에 지원되는 소프트웨어 버전, 16 페이지에 설명된 대로 마이그레이션에 지원되는 Management Center 소프트웨어 버전.
- 다음에 설명된 대로 인터페이스에서 마이그레이션하려는 모든 기능을 포함하는 위협 방어용 스마트 라이선스를 얻고 설치해야 합니다.
  - Cisco.com에 있는 Cisco 스마트 어카운트의 Getting Started(시작하기) 섹션
  - Cisco Smart Software Manager에 Firewall Management Center를 등록합니다.
  - Firewall 시스템 라이선싱

클라우드 사용 Firewall Management Center

클라우드 사용 Firewall Management Center는 Threat Defense 디바이스를 위한 관리 플랫폼이며, Cisco Defense Orchestrator를 통해 제공됩니다. 클라우드 사용 Firewall Management Center는 Management Center와 동일한 여러 기능을 제공합니다.

CDO에서 클라우드 사용 방화벽 Management Center에 액세스할 수 있습니다. CDO는 SDC(Secure Device Connector)를 통해 클라우드 사용 Firewall Management Center에 연결합니다. 클라우드 사용 Firewall Management Center에 대한 자세한 내용은 클라우드 사용 Firewall Management Center를 사용하여 Cisco Secure Firewall Threat Defense 디바이스 관리를 참고하십시오.

Secure Firewall 마이그레이션 툴은 클라우드 사용 Firewall Management Center를 마이그레이션 대상 Management Center로 지원합니다. 마이그레이션 대상 Management Center로 클라우드 사용 Firewall Management Center를 선택하려면 CDO 지역을 추가하고 CDO 포털에서 API 토큰을 생성해야 합니다.

CDO 지역

CDO는 3개의 서로 다른 지역에서 사용할 수 있으며, 지역은 URL 확장명으로 식별할 수 있습니다.

표 *1: CDO* 지역 및 *URL*

지역	**CDO URL**
유럽 지역	https://defenseorchestrator.eu/
미국 지역	https://defenseorchestrator.com/
APJC 지역	https://www.apj.cdo.cisco.com/

마이그레이션에 지원되는 소프트웨어 버전

다음은 지원되는 Secure Firewall 마이그레이션 툴, FDM 매니지드 디바이스 및 마이그레이션용 위협 방어 버전입니다.

지원되는 **Secure Firewall** 마이그레이션 버전

software.cisco.com에 게시된 버전은 Cisco 엔지니어링 및 지원 조직에서 공식적으로 지원하는 버전입니다. software.cisco.com에서 최신 버전의 Secure Firewall 마이그레이션 툴을 다운로드하는 것이 좋습니다. 현재 지원되는 버전은 다음과 같습니다.

- Secure Firewall 마이그레이션 툴 v 3.0.1
- Secure Firewall 마이그레이션 툴 v 3.0.2

Secure Firewall 마이그레이션 툴 버전 3.0.1은 현재 지원이 종료되어 software.cisco.com에서 제거될 예정입니다.

지원되는 **FDM** 매니지드 디바이스 버전

Secure Firewall 마이그레이션 툴은 Threat Defense 소프트웨어 버전 7.2 이상을 실행하는 FDM 매니지드 디바이스에서 마이그레이션을 지원합니다.

소스 **FDM** 매니지드 디바이스 구성에 지원되는 **Management Center** 버전

FDM 매니지드 디바이스의 경우 Secure Firewall 마이그레이션 툴은 버전 7.2 이상을 실행하는 Management Center에서 관리하는 Threat Defense 디바이스로의 마이그레이션을 지원합니다.

참고

- 일부 기능은 최신 버전의 Management Center 및 Threat Defense에서만 지원됩니다.
- 마이그레이션 시간을 최적화하기 위해 Management Center를 software.cisco.com/downloads에서 언급된 권장 릴리스 버전으로 업그레이드하는 것이 좋습니다.

지원되는 **Threat Defense** 버전

FDM 매니지드 디바이스의 경우 Secure Firewall 마이그레이션 툴은 Threat Defense 버전 7.2 이상을 실행하는 디바이스로의 마이그레이션을 지원합니다.

위협 방어의 운영체제 및 호스팅 환경 요구 사항을 포함한 Cisco Firewall 소프트웨어 및 하드웨어 호환성에 대한 자세한 내용은 Cisco Firewall 호환성 가이드를 참고하십시오.