

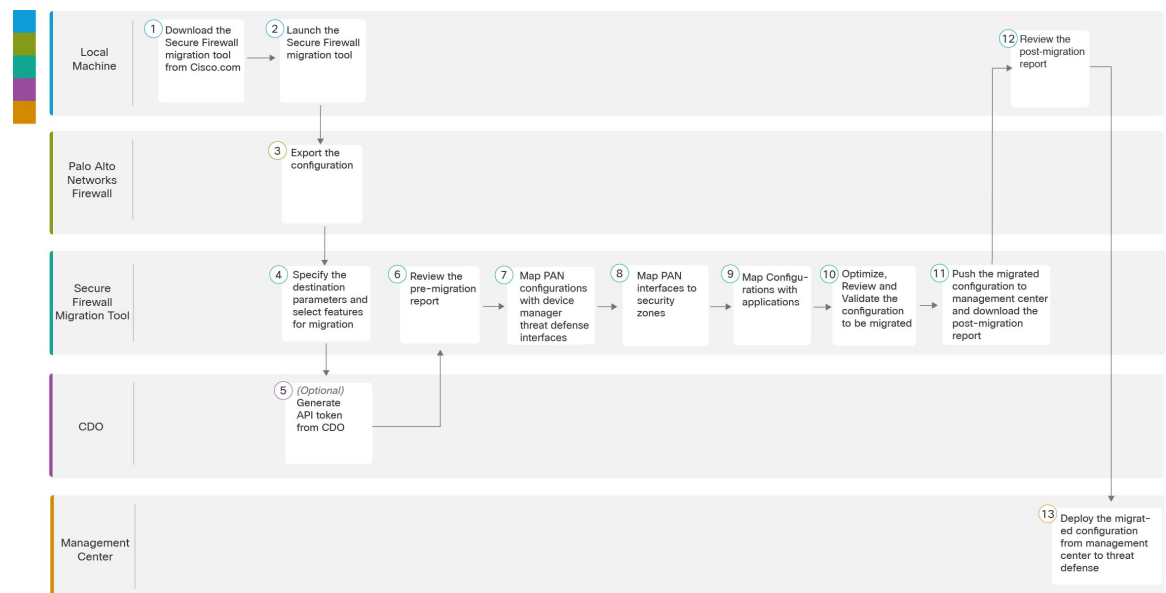


Palo Alto Networks 방화벽을 Threat Defense로 마이그레이션하는 워크플로우

- 엔드 투 엔드 절차, 1 페이지
- 마이그레이션 사전 요건, 3 페이지
- 마이그레이션 실행, 4 페이지
- Secure Firewall 마이그레이션 툴 제거, 32 페이지
- 샘플 마이그레이션: PAN를 Threat Defense 2100으로 , 33 페이지

엔드 투 엔드 절차

다음 순서도는 Secure Firewall 마이그레이션 툴을 사용하여 Palo Alto Networks 방화벽을 Threat Defense로 마이그레이션하는 워크플로우를 보여줍니다.



	업무 환경	단계
①	로컬 컴퓨터	Cisco.com에서 Secure Firewall 마이그레이션 툴의 최신 버전을 다운로드합니다. 자세한 단계는 Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드를 참고하십시오.
②	로컬 컴퓨터	로컬 컴퓨터에서 Secure Firewall 마이그레이션 툴을 실행합니다(Secure Firewall 마이그레이션 툴 실행 참조).
③	Palo Alto Networks 방화벽	구성 파일 내보내기: Palo Alto Networks 방화벽에서 구성을 내보내려면 Palo Alto Networks에서 구성 내보내기를 참조하십시오.
④	Secure Firewall 마이그레이션 툴	이 단계에서 마이그레이션의 대상 매개변수를 지정할 수 있습니다. 자세한 단계는 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정을 참고하십시오.
⑤	Security Cloud Control	(선택 사항) 이 단계는 선택 사항이며, 클라우드 제공 Firewall Management Center를 대상 Management Center로 선택한 경우에만 필요합니다. 자세한 단계는 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 1단계를 참조하십시오.
⑥	Secure Firewall 마이그레이션 툴	마이그레이션 전 보고서를 다운로드한 위치로 이동하여 보고서를 검토합니다. 자세한 단계는 마이그레이션 전 보고서 검토를 참고하십시오.
⑦	Secure Firewall 마이그레이션 툴	PAN 구성이 올바르게 마이그레이션되도록 하려면 PAN 인터페이스를 적절한 위협 방어 인터페이스 개체, 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 단계는 Secure Firewall Device Manager Threat Defense 인터페이스를 사용하여 PAN 방화벽 구성 매핑을 참조하십시오.
⑧	Secure Firewall 마이그레이션 툴	PAN 인터페이스를 적절한 보안 영역에 매핑합니다. 자세한 단계는 보안 영역에 PAN 인터페이스 매핑을 참조하십시오.
⑨	Secure Firewall 마이그레이션 툴	PAN 구성을 해당 대상 애플리케이션에 매핑할 수 있습니다. 자세한 단계는 애플리케이션으로 구성 매핑을 참조하십시오.
⑩	Secure Firewall 마이그레이션 툴	구성을 최적화하고 신중하게 검토하여 구성이 올바른지 확인하고 Threat Defense 디바이스를 구성하는 방법과 일치하는지 확인합니다. 자세한 단계는 마이그레이션할 구성 최적화, 검토 및 검증을 참고하십시오.
⑪	Secure Firewall 마이그레이션 툴	마이그레이션 프로세스의 이 단계에서는 마이그레이션된 구성을 Management Center로 전송하며, 마이그레이션 후 보고서를 다운로드할 수 있습니다. 자세한 단계는 마이그레이션된 구성을 Management Center에 푸시를 참고하십시오.
⑫	로컬 컴퓨터	마이그레이션 후 보고서를 다운로드한 위치로 이동하여 보고서를 검토합니다. 자세한 단계는 마이그레이션 후 보고서 검토 및 마이그레이션 완료를 참고하십시오.

	업무 환경	단계
13	Management Center	Management Center에서 Threat Defense로 마이그레이션된 구성을 구축합니다. 자세한 단계는 마이그레이션 후 보고서 검토 및 마이그레이션 완료 를 참고하십시오.

마이그레이션 사전 요건

PAN 구성을 마이그레이션하기 전에 다음 활동을 수행합니다.

Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드

시작하기 전에

Cisco.com에 인터넷으로 연결되는 Windows 10 64비트 또는 macOS 10.13 이상 버전 시스템이 있어야 합니다.

Security Cloud Control에서 호스팅되는 Secure Firewall 마이그레이션 툴의 클라우드 버전을 사용하려는 경우 4단계로 건너뛸 수 있습니다.

프로시저

단계 1 컴퓨터에서 Secure Firewall 마이그레이션 툴용 폴더를 생성합니다.

이 폴더에는 다른 파일을 저장하지 않는 것이 좋습니다. Secure Firewall 마이그레이션 툴을 실행하면 로그, 리소스 및 기타 모든 파일이 이 폴더에 저장됩니다.



참고 Secure Firewall 마이그레이션 툴의 최신 버전을 다운로드할 때마다 새 폴더를 생성하고 기존 폴더를 사용하지 않아야 합니다.

단계 2 <https://software.cisco.com/download/home/286306503/type>으로 이동하여 **Firewall** 마이그레이션 툴을 클릭합니다.

위 링크를 클릭하면 Firewall NGFW Virtual 아래의 Secure Firewall 마이그레이션 툴로 이동합니다. Firewall Threat Defense 디바이스 다운로드 영역에서 Secure Firewall 마이그레이션 툴을 다운로드할 수도 있습니다.

단계 3 생성한 폴더에 최신 버전의 Secure Firewall 마이그레이션 툴을 다운로드합니다.

Windows 또는 macOS 시스템용 Secure Firewall 마이그레이션 툴의 해당 실행 파일을 다운로드해야 합니다.

단계 4 Security Cloud Control 사용자이고 여기에서 호스팅되는 마이그레이션 툴을 사용하려는 경우, Security Cloud Control 테넌트에 로그인한 후 왼쪽 창에서 **Administration(관리) > Migration(마이그레이션) > Firewall Migration** 툴로 이동하여 마이그레이션 인스턴스를 만듭니다.

마이그레이션 실행

Secure Firewall 마이그레이션 툴 실행

이 작업은 Secure Firewall 마이그레이션 툴의 데스크톱 버전을 사용하는 경우에만 적용됩니다. Security Cloud Control에서 호스팅되는 마이그레이션 툴의 클라우드 버전을 사용하는 경우, [Palo Alto Networks 방화벽에서 구성 내보내기](#)로 건너뛰니다.



참고 Secure Firewall 마이그레이션 툴의 데스크톱 버전을 실행하면 별도의 창에 콘솔이 열립니다. 마이그레이션을 진행하는 동안 Secure Firewall 마이그레이션 툴의 현재 단계 진행률이 콘솔에 표시됩니다. 화면에 콘솔이 표시되지 않으면 Secure Firewall 마이그레이션 툴의 뒤에 있을 가능성이 높습니다.

시작하기 전에

- [Cisco.com](#)에서 [Secure Firewall 마이그레이션 툴 다운로드](#)
- [마이그레이션에 지원되는 대상 Management Center](#) 섹션의 요구 사항을 검토하고 확인합니다.
- Secure Firewall 마이그레이션 툴을 실행하려면 컴퓨터에 최신 버전의 Google Chrome 브라우저가 있어야 합니다. Google Chrome을 기본 브라우저로 설정하는 방법에 대한 자세한 내용은 [Chrome을 기본 웹 브라우저로 설정](#)을 참고하십시오.
- 대규모 컨피그레이션 파일을 마이그레이션하려는 경우 마이그레이션 푸시 중에 시스템이 절전 모드로 전환되지 않도록 절전 설정을 구성합니다.

프로시저

단계 1 컴퓨터에서 Secure Firewall 마이그레이션 툴을 다운로드한 폴더로 이동합니다.

단계 2 다음 중 하나를 수행합니다.

- Windows 시스템에서 Secure Firewall 마이그레이션 툴 실행 파일을 더블 클릭하여 Google Chrome 브라우저에서 실행합니다.

프롬프트가 표시되면 **Yes(예)**를 클릭하여 Secure Firewall 마이그레이션 툴에서 시스템을 변경할 수 있도록 허용합니다.



참고 브라우저의 팝업 차단 기능을 반드시 비활성화해 주십시오. 팝업 차단 기능이 활성화되어 있으면 로그인 팝업이 표시되지 않을 수 있습니다.

Secure Firewall 마이그레이션 툴은 Log(로그) 및 Resources(리소스) 폴더를 포함하여 해당 파일이 있는 폴더에 모든 관련 파일을 생성하고 저장합니다.

- Mac에서 Secure Firewall 마이그레이션 툴*.command 파일을 원하는 폴더로 이동하고, 터미널 애플리케이션을 실행하고, Secure Firewall 마이그레이션 툴이 설치된 폴더로 이동한 후 다음 명령을 실행합니다.

```
# chmod 750 Firewall_Migration_Tool-version_number.command
# ./Firewall_Migration_Tool-version_number.command
```

Secure Firewall 마이그레이션 툴은 Log(로그) 및 Resources(리소스) 폴더를 포함하여 해당 파일이 있는 폴더에 모든 관련 파일을 생성하고 저장합니다.



팁 Secure Firewall 마이그레이션 툴을 열려고 하면 확인된 개발자가 Secure Firewall 마이그레이션 툴을 Apple에 등록하지 않았으므로 경고 대화 상자가 표시됩니다. 확인되지 않은 개발자로부터 애플리케이션을 여는 방법에 대한 자세한 내용은 [확인되지 않은 개발자의 앱 열기](#)를 참고하십시오.



참고 MAC 터미널 압축 방법을 사용합니다.

- 단계 3** Cisco와 텔레메트리 정보를 공유하려는 경우 **End User License Agreement(엔드 유저 라이선스 계약)** 페이지에서 **I agree to share data with Cisco Success Network(Cisco Success Network와 데이터 공유 동의)**를 클릭하고, 그렇지 않은 경우 **I'll do later(나중에)**를 클릭합니다.

Cisco Success Network로 통계를 전송하는 데 동의하면 Cisco.com 계정을 사용하여 로그인하라는 메시지가 표시됩니다. Cisco Success Network로 통계를 보내지 않도록 선택하는 경우 로컬 자격 증명을 사용하여 Secure Firewall 마이그레이션 툴에 로그인합니다.

- 단계 4** Secure Firewall 마이그레이션 툴의 로그인 페이지에서 다음 중 하나를 수행합니다.

- Cisco Success Network와 통계를 공유하려면 **Login with CCO(CCO로 로그인)** 링크를 클릭하여 SSO(Single Sign-On, 단일 인증) 자격 증명으로 Cisco.com 계정에 로그인합니다. Cisco.com 계정이 없는 경우 Cisco.com 로그인 페이지에서 생성합니다.

Cisco.com 계정을 사용하여 로그인한 경우 **8단계**로 진행합니다.

- 인터넷 액세스가 불가능한 에어 갭(air-gapped) 네트워크에 방화벽을 구축한 경우 Cisco TAC에 문의하여 관리자 자격 증명을 사용하는 빌드를 받으십시오. 이 빌드는 시스코에 사용량 통계를 보내지 않으며, TAC가 자격 증명을 제공할 수 있습니다.

- 단계 5** **Reset Password(비밀번호 재설정)** 페이지에서 이전 비밀번호와 새 비밀번호를 입력하고 확인을 위해 새 비밀번호를 다시 입력합니다.

새 비밀번호는 8자 이상이어야 하며 대문자, 소문자, 숫자 및 특수 문자를 포함해야 합니다.

- 단계 6** **Reset(재설정)**을 클릭합니다.

- 단계 7** 새 비밀번호로 로그인합니다.



참고 비밀번호를 잊어버린 경우 <migration_tool_folder>에서 기존의 모든 데이터를 삭제하고 Secure Firewall 마이그레이션 툴을 다시 설치합니다.

단계 8 마이그레이션 전 체크리스트를 검토하고 나열된 모든 항목을 완료했는지 확인합니다.

체크리스트에서 하나 이상의 항목을 완료하지 않은 경우, 완료할 때까지 계속하지 마십시오.

단계 9 **New Migration**(새 마이그레이션)을 클릭합니다.

단계 10 Secure Firewall 마이그레이션 툴의 최신 버전을 실행하고 있는지 확실하지 않은 경우 **Software Update Check**(소프트웨어 업데이트 확인) 화면에서 Cisco.com을 통해 버전을 확인합니다.

단계 11 **Proceed**(진행)를 클릭합니다.

다음에 수행할 작업

다음 단계로 진행할 수 있습니다.

- Secure Firewall 마이그레이션 툴을 사용하여 PAN 방화벽에서 정보를 추출해야 하는 경우 [Palo Alto Networks 방화벽에서 구성 내보내기](#)로 진행합니다.

Secure Firewall 마이그레이션 툴에서 데모 모드 사용

Secure Firewall 마이그레이션 툴을 실행하고 **Select Source Configuration**(소스 구성 선택) 페이지에 있는 경우, **Start Migration**(마이그레이션 시작)을 사용하여 마이그레이션 수행을 시작하거나 **Demo Mode**(데모 모드)를 입력할 수 있습니다.

데모 모드에서는 더미 디바이스를 사용하여 데모 마이그레이션을 수행하고 실제 마이그레이션 플로우가 어떤지 시각화할 수 있습니다. 마이그레이션 툴은 **Source Firewall Vendor**(소스 방화벽 벤더) 드롭다운에서 선택한 항목에 따라 데모 모드를 트리거합니다. 구성 파일을 업로드하거나 라이브 디바이스에 연결하고 마이그레이션을 계속할 수 있습니다. 데모 FMC, 데모 FTD 디바이스와 같은 또는 와 같은 Multicloud Defense 데모 소스 및 대상 디바이스를 선택하여 데모 마이그레이션을 진행할 수 있습니다.



주의 데모 모드를 선택하면 기존 마이그레이션 워크플로우가 있는 경우 지워집니다. **Resume Migration**(마이그레이션 재개)에서 액티브 마이그레이션이 진행 중인 상태에서 데모 모드를 사용하면, 액티브 마이그레이션이 손실되며 데모 모드를 사용한 이후에 처음부터 다시 시작해야 합니다.

또한 실제 마이그레이션 워크플로우에서와 마찬가지로 마이그레이션 전 보고서를 다운로드하여 확인하고, 인터페이스를 매핑하고, 보안 영역을 매핑하고, 인터페이스 그룹을 매핑하는 등 모든 작업을 수행할 수 있습니다. 그러나 구성 검증까지만 데모 마이그레이션을 수행할 수 있습니다. 선택한 데모 대상 디바이스는 데모 모드이므로 구성을 푸시할 수 없습니다. 검증 상태 및 요약을 확인하고 **Exit**

Demo Mode(데모 모드 종료)를 클릭하여 **Select Source Configuration**(소스 구성 선택) 페이지로 다시 이동하여 실제 마이그레이션을 시작할 수 있습니다.



참고 데모 모드에서는 구성 푸시를 제외하고 Secure Firewall 마이그레이션 툴의 전체 기능 집합을 활용하고, 실제 마이그레이션을 수행하기 전에 End-to-End 마이그레이션 절차를 평가판으로 실행할 수 있습니다.

Palo Alto Networks 방화벽에서 컨피그레이션 내보내기

다음과 같은 방법으로 구성 파일을 내보낼 수 있습니다.



참고 구성 추출 방법 [Palo Alto 방화벽의 구성 파일\(Panorama에서 관리하지 않음\)](#), 7 페이지을(를) 사용하는 것이 좋습니다.

Palo Alto 방화벽의 구성 파일(Panorama에서 관리하지 않음)

게이트웨이에서 컨피그레이션을 추출하려면 다음 단계를 수행합니다.

프로시저

- 단계 1 **Device**(디바이스) > **Setup**(설정) > **Operations**(운영)로 이동하고 **Save Named Configuration**(명명된 컨피그레이션 저장) <file_name.xml>을 선택합니다.
- 단계 2 **Ok**(확인)를 클릭합니다.
- 단계 3 **Device**(디바이스) > **Setup**(설정) > **Operations**(운영)로 이동하고 **Export Named Configuration**(명명된 컨피그레이션 내보내기)을 클릭합니다.
- 단계 4 <file_name.xml> 파일을 선택합니다.
- 단계 5 **Ok**(확인)를 클릭합니다.
- 단계 6 실행 중인 컨피그레이션이 포함된 XML 파일 <file_name.xml>을 클릭하고 **OK**(확인)를 클릭하여 컨피그레이션 파일을 내보냅니다.
- 단계 7 내보낸 파일을 방화벽 외부의 위치에 저장합니다. 이 백업을 통해 Secure Firewall 마이그레이션 툴에 업로드하여 구성을 마이그레이션할 수 있습니다.
- 단계 8 (선택 사항) 대상 NAT의 소스와 대상 영역이 동일한 NAT 정책이 있는 경우 다음 단계를 수행합니다.
 - a) 방화벽에 대해 CLI에서 **show routing route** 명령을 실행합니다.
 - b) 라우팅 테이블을 .txt 파일에 복사합니다.
 - c) .txt 파일과 .xml 파일을 panconfig.xml과 함께 압축할 폴더에 .txt 파일을 추가합니다.

이러한 단계는 마이그레이션에 필수가 아닙니다. 이러한 단계를 수행하지 않으면 대상 영역이 Secure Firewall 마이그레이션 툴 마이그레이션 중에 매핑되지 않으며 마이그레이션 보고서에 포함됩니다.



참고 **show routing route** 명령을 사용하여 라우팅 테이블 세부 정보를 추출합니다. 추출된 출력을 메모장에 붙여 넣습니다.

Palo Alto 방화벽의 구성 파일(Panorama에서 관리)

파노라마에서 디바이스를 관리하는 경우 게이트웨이에서 컨피그레이션을 추출해야 합니다. 게이트웨이와 파노라마 컨피그레이션을 병합하고 컨피그레이션을 추출합니다.

Secure Firewall 마이그레이션 툴 사용자 인터페이스에서 다음을 수행합니다.

시작하기 전에

슈퍼 사용자 계정을 사용하여 Palo Alto 방화벽 웹 UI에 로그인합니다.

프로시저

단계 1 **Device**(디바이스) > **Support**(지원) > **Tech Support File**(기술 지원 파일)로 이동합니다.

단계 2 **Generate Tech Support File**(기술 지원 파일 생성)을 클릭합니다.

단계 3 생성된 파일을 사용할 수 있게 되면 **Download Tech Support File**(기술 지원 파일 다운로드)을 클릭합니다.

단계 4 파일의 압축을 풀고 `\opt\pancfg\mgmt\saved-configs\` 경로로 이동하여 `Mered-running-config.xml` 파일을 검색합니다.

Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정

시작하기 전에

Security Cloud Control에서 호스팅되는 마이그레이션 툴의 클라우드 버전을 사용하는 경우 3단계로 건너뛵니다.

- 온프레미스 Firewall Management Center용 Firewall Management Center의 IP 주소를 가져옵니다.
- Secure Firewall 마이그레이션 툴 3.0부터는 온프레미스 Firewall Management Center 또는 클라우드 제공 Firewall Management Center 중에서 선택할 수 있습니다.
- 클라우드 제공 Firewall Management Center의 경우 지역 및 API 토큰을 제공해야 합니다. 자세한 내용은 [마이그레이션에 지원되는 대상 Management Center](#)를 참조하십시오.
- (선택 사항) 인터페이스 및 경로와 같은 디바이스별 구성을 마이그레이션하려면 대상을 추가합니다. Firewall Threat Defense 인 경우 Management Center에 대상 Threat Defense 디바이스를 추가합니다. [Firewall Management Center에 디바이스 추가](#) 참고

- **Review and Validate**(검토 및 검증) 페이지에서 ACL에 IPS 또는 파일 정책을 적용해야 하는 경우 마이그레이션 전에 Firewall Management Center에서 정책을 생성하는 것이 매우 권장됩니다. Secure Firewall 마이그레이션 툴이 연결된 Firewall Management Center에서 정책을 가져오므로 동일한 정책을 사용합니다. 새 정책을 생성하고 여러 액세스 제어 목록에 할당하면 성능이 저하될 수 있으며 푸시가 실패할 수도 있습니다.

프로시저

단계 1 Select Target(대상 선택) 화면의 **Firewall Management(방화벽 관리)** 섹션에서 다음을 수행합니다. 온프레미스 Firewall Management Center 또는 클라우드 제공 Firewall Management Center로 마이그레이션하도록 선택할 수 있습니다.

- 온프레미스 Firewall Management Center로 마이그레이션하려면 다음을 수행합니다.

- a) **On-Prem FMC**(온프레미스 FMC) 라디오 버튼을 클릭합니다.
- b) Management Center의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.
- c) **Domain**(도메인) 드롭다운 목록에서 마이그레이션할 도메인을 선택합니다.

Firewall Threat Defense 디바이스로 마이그레이션하려는 경우 선택한 도메인에서 사용 가능한 Firewall Threat Defense 디바이스로만 마이그레이션할 수 있습니다.

- d) **Connect**(연결)를 클릭하고 2단계로 진행합니다.

- 클라우드 제공 Firewall Management Center로 마이그레이션하려면 다음을 수행합니다.

- a) **Cloud** 사용 **FMC** 라디오 버튼을 클릭합니다.
- b) 지역을 선택하고 Security Cloud Control API 토큰을 붙여넣습니다. API 토큰을 생성합니다. Security Cloud Control에서 다음 단계를 수행합니다.
 1. Security Cloud Control에 로그인합니다.
 2. 오른쪽 상단에서 **Preferences**(환경 설정) > **General Preferences**(일반 환경설정)로 이동하여 **My Tokens**(내 토큰) 섹션의 API 토큰을 복사합니다.
- c) **Connect**(연결)를 클릭하고 2단계로 진행합니다.

단계 2 Firewall Management Center Login(Firewall Management Center 로그인) 대화 상자에서 Secure Firewall 마이그레이션 툴 전용 계정의 사용자 이름과 비밀번호를 입력하고 **Login**(로그인)을 클릭합니다.

Secure Firewall 마이그레이션 툴이 Firewall Management Center에 로그인하여 해당 Firewall Management Center에서 관리되는 Firewall Threat Defense 디바이스 목록을 검색합니다. 콘솔에서 이 단계의 진행 상황을 볼 수 있습니다.

단계 3 Proceed(진행)를 클릭합니다.

단계 4 Choose FTD(FTD 선택) 섹션에서 다음 중 하나를 수행합니다.

- **Select FTD Device(FTD 디바이스 선택)** 드롭다운 목록을 클릭하고 구성을 마이그레이션할 디바이스를 선택합니다.

선택한 Firewall Management Center 도메인의 디바이스가 **IP Address**(IP 주소), **Name**(이름), **Device Model**(디바이스 모델) 및 **Mode**(모드)(라우팅 또는 투명)별로 나열됩니다.



참고 최소한, 선택하는 Firewall Threat Defense 네이티브 디바이스가 마이그레이션하는 컨피그레이션과 동일한 수의 물리적 인터페이스 또는 포트 채널 인터페이스를 가져야 합니다. 최소한, Firewall Threat Defense 디바이스의 컨테이너 인스턴스가 동일한 수의 물리적 인터페이스 또는 포트 채널 인터페이스 및 하위 인터페이스를 가져야 합니다. 컨피그레이션과 동일한 방화벽 모드로 디바이스를 구성해야 합니다. 그러나 이러한 인터페이스가 두 디바이스에서 동일한 이름을 가질 필요는 없습니다.



참고 지원되는 대상 Threat Defense 플랫폼이 Management Center 버전 6.5 이상을 사용하는 Firewall 1010인 경우에만 FDM 5505 마이그레이션 지원은 공유 정책에 적용되며 디바이스별 정책에는 적용되지 않습니다. Threat Defense 없이 진행하면 Secure Firewall 마이그레이션 툴이 Threat Defense에 구성 또는 정책을 푸시하지 않습니다. 따라서 Threat Defense 디바이스별 구성인 인터페이스 및 경로, 사이트 간 VPN은 마이그레이션되지 않습니다. 그러나 NAT, ACL 및 포트 개체와 같은 지원되는 다른 모든 컨피그레이션(공유 정책 및 개체)은 마이그레이션됩니다. 원격 액세스 VPN은 공유 정책이며 Threat Defense 없이도 마이그레이션할 수 있습니다.

원격 구축이 활성화된 상태에서 Firewall Management Center 또는 Firewall Threat Defense 6.7 이상으로의 Palo Alto Networks 방화벽 마이그레이션은 Secure Firewall 마이그레이션 툴에서 지원됩니다. 인터페이스 및 경로의 마이그레이션은 수동으로 진행해야 합니다.

- 컨피그레이션을 Firewall Management Center로 마이그레이션하려면 **Proceed without FTD**(FTD 없이 진행)를 클릭합니다.

Firewall Threat Defense 없이 진행하면 Secure Firewall 마이그레이션 툴이 Firewall Threat Defense에 구성 또는 정책을 푸시하지 않습니다. 따라서 Firewall Threat Defense 디바이스별 구성인 인터페이스 및 라우트, 사이트 간 VPN은 마이그레이션되지 않으며, Firewall Management Center에서 수동으로 구성해야 합니다. 그러나 NAT, ACL 및 포트 개체와 같은 지원되는 다른 모든 컨피그레이션(공유 정책 및 개체)은 마이그레이션됩니다. 원격 액세스 VPN은 공유 정책이며 Threat Defense 없이도 마이그레이션할 수 있습니다.

단계 5 **Proceed**(진행)를 클릭합니다.

마이그레이션하는 대상에 따라 Secure Firewall 마이그레이션 툴에서 마이그레이션할 기능을 선택할 수 있습니다.

단계 6 **Select Features**(기능 선택) 섹션을 클릭하여 대상으로 마이그레이션할 기능을 검토하고 선택합니다.

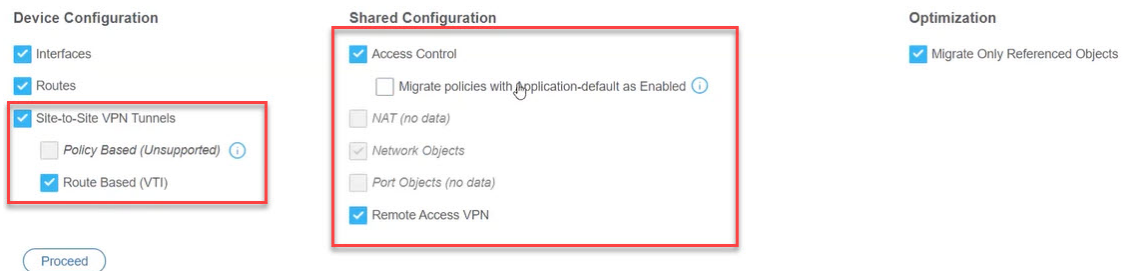
- 대상 Firewall Threat Defense 디바이스로 마이그레이션하는 경우 Secure Firewall 마이그레이션 툴이 **Device Configuration**(디바이스 구성) 및 **Shared Configuration**(공유 구성) 섹션의 구성에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.
- Firewall Management Center로 마이그레이션하는 경우 Secure Firewall 마이그레이션 툴이 **Device Configuration**(디바이스 구성) 및 **Shared Configuration**(공유 구성) 및 **Optimization**(최적화) 섹션에서 구성에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.

- PAN의 경우 **Shared Configuration**(공유 컨피그레이션)에서 관련 **Access Control**(액세스 제어) 옵션을 선택합니다.

Migrate policies with Application-Default as Enabled(애플리케이션 기본값이 활성화된 정책 마이그레이션) - 이 옵션을 선택하면 PAN 애플리케이션이 마이그레이션됩니다. **Migrate policies with Application-Default as Enabled**(애플리케이션 기본값이 활성화된 정책 마이그레이션) 옵션은 이 체크 박스를 선택하는 경우에만 볼 수 있습니다.



참고 **Application Mapping**(애플리케이션 매핑)은 정책을 마이그레이션하도록 선택한 경우에만 활성화됩니다.



VPN으로 구성된 Palo Alto 네트워크 방화벽에서 구성을 마이그레이션하는 경우, **Device Configuration**(디바이스 구성) 창 아래의 사이트 간 VPN 터널 및 **Shared Configuration**(공유 구성) 창 아래의 **Remote Access VPN**(원격 액세스 VPN)을 선택하거나 선택 취소할 수 있습니다. 정책 기반 사이트 간 VPN 구성은 Palo Alto Networks 방화벽에서 지원하지 않으므로 지원되지 않습니다.

"**application-default**"(애플리케이션 기본값)로 지정된 서비스를 포함하는 정책

"**application-default**"(애플리케이션 기본값)로 구성된 서비스와 참조되는 멤버 또는 그룹이 있는 애플리케이션을 포함하는 정책은 **Feature Selection**(기능 선택) 페이지에서 선택한 사항에 따라 마이그레이션됩니다. Firewall Management Center에는 **application-default**(애플리케이션 기본값)에 해당하는 항목이 없으므로 이러한 정책은 "any(모두)" 서비스로 푸시됩니다. **application-default**(애플리케이션 기본값)와 유사한 기능을 복제하는 경우 Palo Alto Networks 방화벽에서 애플리케이션이 사용하는 포트를 찾아 Firewall Management Center에서 Policy(정책)의 Port(포트) 섹션에서 포트를 구성합니다.

예를 들어 "**web-browsing**(웹 브라우징)"과 "**application-default**(애플리케이션 기본값)"로 구성된 서비스를 갖는 정책은 애플리케이션 HTTP(web-browsing(웹 브라우징)과 동일)로 마이그레이션되고 포트는 "**any**(모두)"로 마이그레이션됩니다. "**application-default**(애플리케이션 기본값)"와 동일한 기능을 복제하려면 포트를 TCP/80 및 TCP/8080으로 구성합니다. web-browsing(웹 브라우징)에서는 포트 TCP 80 및 TCP 8080을 사용합니다. 정책에 여러 애플리케이션이 있는 경우 각 애플리케이션에서 사용하는 포트를 구성합니다.

정책에 여러 애플리케이션이 있는 경우 다른 애플리케이션에 대한 추가 액세스를 허용할 수 있으므로 포트를 구성하기 전에 정책을 분할하는 것이 좋습니다.

애플리케이션이 "**any**(모두)"로 구성되고 서비스가 "**application-default**(애플리케이션 기본값)"로 구성된 정책은 **Feature Selection**(기능 선택) 페이지에서 사용 가능한 선택 사항("**any**(모두)"로 구성된 애플리케이션 및 "**any**(모두)"로 구성된 서비스)에 관계없이 비활성화된 상태로 마이그레이션됩니다. 허용되는 동작인 경우

애플리케이션을 활성화하고 변경 사항을 커밋합니다. 그렇지 않은 경우 필요한 애플리케이션 또는 서비스를 선택하고 정책을 활성화합니다.

규칙에 따라 애플리케이션을 사용하여 액세스 제어 목록 분할

구성된 하나의 규칙을 포함하는 액세스 제어 목록을 여러 애플리케이션으로 마이그레이션할 때 ACL을 분할하도록 선택할 수 있습니다. 그러면 ACL이 여러 규칙으로 분할되고 규칙당 하나의 애플리케이션이 사용됩니다. 이렇게 하려면 **Split ACLs with Applications per rule**(규칙에 따라 애플리케이션으로 ACL 분할) 확인란을 선택합니다. 그러나 마이그레이션하려는 구성에 액세스 규칙당 구성된 여러 애플리케이션이 포함되어 있지 않은 경우, 확인란이 나타나지 않습니다.

각 규칙은 규칙당 하나의 애플리케이션을 사용하는 여러 규칙으로 변환되며, 이러한 규칙은 **Optimize, Review, and Validate Configuration**(구성 최적화, 검토 및 검증) 페이지에서 검토할 수 있습니다.

- Secure Firewall 마이그레이션 툴은 대상 Management Center가 7.2 이상인 경우 원격 액세스 VPN의 마이그레이션을 지원합니다. 원격 액세스 VPN은 Threat Defense 없이도 마이그레이션할 수 있는 공유 정책입니다. Threat Defense를 사용하여 마이그레이션을 선택한 경우 Threat Defense 버전은 7.0 이상이어야 합니다.
- (선택 사항) **Optimization(최적화)** 섹션에서 **Migrate only referenced objects**(참조된 개체만 마이그레이션)를 선택하여 액세스 제어 정책 및 NAT 정책에서 참조되는 개체만 마이그레이션합니다.



참고 이 옵션을 선택하면 구성에서 참조되지 않는 개체는 마이그레이션되지 않습니다. 이렇게 하면 마이그레이션 시간이 최적화되고 컨피그레이션에서 사용되지 않는 개체가 제거됩니다.

단계 7 **Proceed(진행)**를 클릭합니다.

단계 8 **Rule Conversion/ Process Config**(규칙 변환/프로세스 컨피그레이션) 섹션에서 **Start Conversion**(변환 시작)을 클릭하여 변환을 시작합니다.

단계 9 Secure Firewall 마이그레이션 툴에서 변환한 요소의 요약 검토합니다.

컨피그레이션 파일이 성공적으로 업로드되고 구문 분석되었는지 확인하려면 마이그레이션을 계속하기 전에 **Pre-Migration Report**(마이그레이션 전 보고서)를 다운로드하여 확인하십시오.

단계 10 **Download Report**(보고서 다운로드)를 클릭하고 **Pre-Migration Report**(마이그레이션 전 보고서)를 저장합니다.

Pre-Migration Report(마이그레이션 전 보고서)의 사본도 Secure Firewall 마이그레이션 툴과 동일한 위치의 **Resources**(리소스) 폴더에 저장됩니다.

마이그레이션 전 보고서 검토

마이그레이션 중에 마이그레이션 전 보고서를 다운로드하지 못한 경우 다음 링크를 사용하여 다운로드하십시오.

마이그레이션 전 보고서 다운로드 엔드포인트 - http://localhost:8888/api/downloads/pre_migration_summary_html_format



참고 Secure Firewall 마이그레이션 툴이 실행 중일 때만 보고서를 다운로드할 수 있습니다.

프로시저

단계 1 **Pre-Migration Report**(마이그레이션 전 보고서)를 다운로드한 위치로 이동합니다.



참고 **Pre-Migration Report**(마이그레이션 전 보고서)의 사본도 Secure Firewall 마이그레이션 툴과 동일한 위치의 Resources (리소스) 폴더에 저장됩니다.

단계 2 **Pre-Migration Report**(마이그레이션 전 보고서)를 열고 내용을 신중하게 검토하여 마이그레이션의 실패를 일으킬 수 있는 문제를 파악합니다.

Pre-Migration Report(마이그레이션 전 보고서)에는 다음 정보가 포함됩니다.

- Firewall Threat Defense 또는 Multicloud Defense로 성공적으로 마이그레이션할 수 있는 지원되는 구성 요소 및 마이그레이션을 위해 선택한 특정 기능의 요약입니다.
- **Configuration Lines with Errors**(오류가 있는 구성 라인) - Secure Firewall 마이그레이션 툴이 구문 분석할 수 없으므로, 마이그레이션할 수 없는 구성 요소에 대한 세부 정보입니다. 계속 진행하기 전에 구성에서 이러한 오류를 해결하고 새 구성 파일을 내보낸 다음 Secure Firewall 마이그레이션 툴에 새 구성 파일을 업로드합니다.
- **Ignored Configuration**(무시된 구성) - Firewall Management Center 또는 Secure Firewall 마이그레이션 툴에서 지원되지 않기 때문에 무시되는 구성 요소의 세부 정보입니다. Secure Firewall 마이그레이션 툴은 이러한 라인을 구문 분석하지 않습니다. 이러한 라인을 검토하고 Firewall Management Center에서 각 기능이 지원되는지 확인한 다음, 지원되지 않는 경우 해당 기능을 수동으로 구성하도록 계획합니다.

Firewall Management Center 및 Firewall Threat Defense에서 지원되는 기능에 대한 자세한 내용은 [Cisco Secure Firewall Management Center 디바이스 컨피그레이션 가이드](#)를 참조하십시오.

단계 3 (선택 사항) **Pre-Migration Report**(마이그레이션 전 보고서)에서 시정 조치를 권장하는 경우, 계속하기 전에 인터페이스에서 해당 시정 조치를 완료하고 구성 파일을 다시 내보낸 후 업데이트된 구성 파일을 업로드하십시오.

단계 4 구성 파일이 성공적으로 업로드되고 구문 분석된 후 Secure Firewall 마이그레이션 툴로 돌아가 **Next**(다음)를 클릭하여 마이그레이션을 계속합니다.

다음에 수행할 작업

[Firepower Threat Defense 인터페이스와 PAN 인터페이스 매핑](#)

PAN Firewall 구성과 Firewall Threat Defense 인터페이스 매핑

Firewall Threat Defense 디바이스에는 구성에 사용되는 것과 같거나 더 많은 수의 물리적 및 포트 채널 인터페이스가 있어야 합니다. 이러한 인터페이스가 두 디바이스에서 동일한 이름을 가질 필요는 없습니다. 인터페이스 매핑 방법을 선택할 수 있습니다.

Firewall Threat Defense 인터페이스에 대한 인터페이스 매핑은 Firewall Threat Defense 디바이스 유형에 따라 달라집니다.

- 대상 Firewall Threat Defense가 네이티브 유형인 경우:
 - Firewall Threat Defense에서 사용되는 PAN 인터페이스 또는 PC(포트 채널) 데이터 인터페이스나 하위 인터페이스(PAN 구성에서는 관리 전용 제외)가 동일하거나 더 많아야 합니다. 이 수가 더 적은 경우 대상 Firewall Threat Defense에 필요한 인터페이스 유형을 추가합니다.
 - 하위 인터페이스는 물리적 인터페이스 또는 포트 채널 매핑을 기반으로 Secure Firewall 마이그레이션 툴에서 생성됩니다.
- 대상 Firewall Threat Defense가 컨테이너 유형인 경우:
 - Firewall Threat Defense에서 같거나 더 많은 수의 PAN 인터페이스, 물리적 하위 인터페이스, 포트 채널 또는 포트 채널 하위 인터페이스(구성의 관리 전용 인터페이스 제외)를 사용해야 합니다. 이 수가 더 적은 경우 대상 Firewall Threat Defense에 필요한 인터페이스 유형을 추가합니다. 예를 들어, 대상 Firewall Threat Defense의 물리적 인터페이스 및 물리적 하위 인터페이스 수가 PAN 보다 100개 적을 경우 대상 Firewall Threat Defense에서 추가 물리적 인터페이스 또는 물리적 하위 인터페이스를 생성할 수 있습니다.

시작하기 전에

Firewall Management Center에 연결하고 대상을 Firewall Threat Defense로 선택했는지 확인합니다. 자세한 내용은 [Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 8 페이지](#)를 참고하십시오.



참고 이 단계는 Firewall Threat Defense 디바이스 없이 Firewall Management Center로 마이그레이션하는 경우 적용되지 않습니다.

프로시저

단계 1 인터페이스 매핑을 변경하려면 **FTD Interface Name**(FTD 인터페이스 이름)의 드롭다운 목록을 클릭하고 해당 인터페이스에 매핑할 인터페이스를 선택합니다.

관리 인터페이스의 매핑은 변경할 수 없습니다. Firewall Threat Defense 인터페이스가 인터페이스에 이미 할당된 경우 드롭다운 목록에서 해당 인터페이스를 선택할 수 없습니다. 할당된 모든 인터페이스는 회색으로 표시되며 사용할 수 없습니다.

하위 인터페이스는 매핑할 필요가 없습니다. Secure Firewall 마이그레이션 툴은 구성의 모든 하위 인터페이스에 대해 Firewall Threat Defense 디바이스의 하위 인터페이스를 매핑합니다.



참고 소스 방화벽의 인터페이스 수가 대상 방화벽보다 많은 경우 대상 방화벽에서 하위 인터페이스를 생성하고 마이그레이션을 다시 시도합니다.

단계 2 각 인터페이스를 Firewall Threat Defense 인터페이스에 매핑했으면 **Next(다음)**를 클릭합니다.

다음에 수행할 작업

PAN 인터페이스를 적절한 Firewall Threat Defense 인터페이스 개체 및 보안 영역에 매핑합니다. 자세한 내용은 [보안 영역에 PAN 인터페이스 매핑](#)을 참고하십시오.

PAN 인터페이스를 보안 영역 및 에 매핑

구성이 올바르게 마이그레이션되도록 하려면 인터페이스를 적절한 Firewall Threat Defense 인터페이스 개체, 보안 영역에 매핑합니다. 구성에서 액세스 제어 정책 및 NAT 정책은 인터페이스 이름(nameif)을 사용합니다. Firewall Management Center에서 이러한 정책은 인터페이스 개체를 사용합니다. 또한 Firewall Management Center 정책은 인터페이스 개체를 다음과 같이 그룹화합니다.

- 보안 영역 — 하나의 인터페이스가 하나의 보안 영역에만 속할 수 있습니다.

Secure Firewall 마이그레이션 툴을 사용하면 보안 영역과 인라인 보안 영역이 있는 인터페이스를 일대일로 매핑할 수 있습니다. 보안 영역 또는 인라인 보안 영역이 인터페이스에 매핑된 경우 Firewall Management Center에서 허용하더라도 다른 인터페이스에 매핑될 수 없습니다. Firewall Management Center의 보안 영역에 대한 자세한 내용은 *Cisco Secure Firewall Management Center* 디바이스 구성 설명서에서 [보안 영역 및 인터페이스 그룹](#)을 참조하십시오.

프로시저

- 단계 1 **Map Security Zones(보안 영역 매핑)** 화면에서 사용 가능한 인터페이스, 보안 영역 및 인라인 보안 영역을 검토합니다.
- 단계 2 Firewall Management Center에 존재하는, 즉 구성 파일에서 보안 영역 유형 개체로 사용 가능하고 드롭다운 목록에서 사용 가능한 보안 영역 및 인터페이스 그룹에 인터페이스를 매핑하려면 다음과 같이 합니다.
 - a) **Security Zones(보안 영역)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.
 - b) **Interface Groups(인터페이스 그룹)** 열에서 해당 인터페이스의 인터페이스 그룹을 선택합니다.
- 단계 3 Firewall Management Center에 존재하는 보안 영역에 인터페이스를 매핑하려면 **Security Zones(보안 영역)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.
- 단계 4 Firewall Management Center에 존재하는 인라인 보안 영역에 인터페이스를 매핑하려면 **Inline Security Zones(인라인 보안 영역)** 열에서 해당 인터페이스의 인라인 보안 영역을 선택합니다.

단계 5 보안 영역을 수동으로 매핑하거나 자동으로 생성할 수 있습니다.

보안 영역을 수동으로 매핑하려면 다음과 같이 합니다.

- Add SZ & IG(SZ 및 IG 추가)**를 클릭합니다.
- Add SZ & IG(SZ 및 IG 추가)** 대화 상자에서 **Add(추가)**를 클릭하여 새 보안 영역을 추가합니다.
- Security Zone(보안 영역)** 열에 보안 영역 이름을 입력합니다. 허용되는 최대 문자 수는 48자입니다.
- Close(닫기)**를 클릭합니다.

자동 생성을 통해 보안 영역을 매핑하려면 다음과 같이 합니다.

- Auto-Create(자동 생성)**를 클릭합니다.
- Auto-Create(자동 생성)** 대화 상자에서 **Zone Mapping(영역 매핑)**을 선택합니다.
- Auto-Create(자동 생성)**를 클릭합니다.

Auto-Create(자동 생성)를 클릭하면 소스 방화벽 영역이 자동으로 매핑됩니다. 동일한 이름 영역이 Firewall Management Center에 이미 있는 경우 해당 영역이 재사용됩니다. 매핑 페이지에 재사용 영역에 대한 "(A)"가 표시됩니다. 예를 들어 **inside(내부)** "(A)"가 표시될 수 있습니다.

단계 6 모든 인터페이스를 적절한 보안 영역에 매핑했으면 **Next(다음)**를 클릭합니다.

애플리케이션으로 구성 매핑

애플리케이션을 해당 대상 애플리케이션에 매핑할 수 있습니다. 애플리케이션을 기반으로 하는 규칙을 마이그레이션할 수 있습니다.

Firewall Management Center의 미리 정의된 애플리케이션 목록과 함께 구성 파일의 일부 애플리케이션이 이 탭에 나열됩니다. Firewall Management Center에 있는 미리 정의된 매핑 중 일부가 매핑됩니다.



참고 미리 정의된 매핑은 편집할 수 없습니다.

Application Mapping(애플리케이션 매핑) 페이지에는 다음 탭이 표시됩니다.

- **Invalid Mappings(잘못된 매핑)** - 해당 마이그레이션에 대한 잘못된 매핑 목록을 봅니다.

다음과 같은 시나리오에서는 매핑은 유효하지 않은 것으로 간주됩니다.

- **Mapping Mode(매핑 모드)**가 **Application(애플리케이션)** 또는 **Port(포트)** 중 하나로 선택되었지만 **Target(대상)**이 비어 있는 경우.
- **Mapping Mode(매핑 모드)**가 **Port(포트)**이고 포트의 구문이 잘못된 경우. 마이그레이션을 계속하려면 **Invalid Mapping(유효하지 않은 매핑)**이 0이어야 합니다.



참고 올바른 검증이 있을 때까지 **Next(다음)** 버튼은 비활성화됩니다.

Cisco Firewall Migration Tool (Version 4.0.3)

Application Mapping

Source: Palo Alto Networks (S)
Target FTD: No FTD

Valid Mappings (16/18) Blank Mappings (2/18) Invalid Mappings (0/18)

Valid Source Applications	Mapping Mode	Target Application/Ports
cloudapp-uploading	application	CloudApp
asana-base	application	Asana
bacnet-create-object	application	BACnet
bacnet-delete-object	application	BACnet
adobe-meeting-file-transfer	application	Adobe Connect
adobe-meeting-remote-control	application	Adobe Connect
adobe-meeting-uploading	application	Adobe Connect
amazon-cloud-drive-base	application	Amazon Cloud Drive
cloudapp	application	CloudApp
cloudapp-base	application	CloudApp

10 per page 1 to 10 of 16 Page 1 of 2

Validate

Back

소스에서 사전 정의된 매핑 목록을 가져오는 경우 자동으로 매핑되는 사전 정의된 애플리케이션이 있습니다. 매핑되지 않은 애플리케이션이 있는 경우, 포트 또는 애플리케이션에 수동으로 매핑해야 합니다.

- **Blank Mappings(빈 매핑)** - 매핑되지 않은 애플리케이션을 표시하며 사용자의 조치가 필요합니다. 애플리케이션은 **Application(애플리케이션)** 또는 **Port(포트)**에 매핑되어야 합니다.



참고 모든 애플리케이션 항목을 매핑하는 것이 좋지만 필수는 아닙니다.

매핑 모드를 선택하고 대상 애플리케이션에 유효한 데이터가 있으면 유효한 매핑입니다.



참고 기본적으로 모든 사전 정의된 매핑을 **Valid Mappings(유효한 매핑)** 탭에서 사용할 수 있습니다.

- **Valid Mappings(유효한 매핑)** - 올바른 매핑을 표시합니다. Secure Firewall 마이그레이션 툴에는 일반적으로 사용되는 애플리케이션을 위해 PAN 및 Firewall Threat Defense 애플리케이션과의 사전 정의된 매핑의 자체 데이터베이스가 있습니다. PAN 애플리케이션이 사전 정의된 매핑 DB와 일치하는 경우 해당 애플리케이션은 자동으로 매핑되며 유효한 매핑 아래에 표시됩니다.

Application(애플리케이션)이 **Blank Mapping(빈 매핑)**에서 **Application(애플리케이션)** 또는 **Port(포트)**에 매핑되면 검증 후에 **Valid Mapping(유효한 매핑)**으로 이동됩니다.



참고 사전 정의된 매핑은 편집할 수 없습니다.

마이그레이션에 따라 유효하지 않은 매핑, 유효한 매핑, 빈 매핑의 개수는 계속 변동됩니다.

다음 표에는 애플리케이션 매핑 속성이 나와 있습니다.

표 1: 애플리케이션 매핑 표 속성

필드	설명
Source Application(소스 애플리케이션)	Palo Alto Networks 방화벽에서 사용되는 애플리케이션 목록을 표시합니다.
Mapping Mode(매핑 모드)	매핑 모드를 Application(애플리케이션) 또는 Port(포트)로 선택합니다. - Application(애플리케이션) - 매핑에 사용할 수 있는 대상 애플리케이션 목록에서 선택합니다. 하나의 애플리케이션만 매핑할 수 있습니다. - Port(s)(포트) - 매핑에 사용할 수 있는 포트 목록에서 선택합니다. Ports(포트)를 선택한 경우 관련 포트 정보를 지정된 형식으로 입력합니다. 예를 들면 tcp/80 및 udp/80입니다. 참고 문자 사이에 공백은 허용되지 않습니다.
대상 애플리케이션	매핑 모드를 기반으로 하는 대상 애플리케이션 또는 포트의 목록을 표시합니다.

ICMP 및 Ping 애플리케이션은 ICMP 및 Ping 서비스로 마이그레이션됩니다. 이 작업은 Secure Firewall 마이그레이션 툴에 의해 자동으로 수행되므로 **Application Mapping**(애플리케이션 매핑) 페이지에 표시되지 않습니다.

프로시저

단계 1 Valid Mappings(유효한 매핑) 탭을 클릭하여 해당 마이그레이션의 유효한 매핑 수를 확인합니다. **Valid Source Application**(유효한 소스 애플리케이션)을 유효한 **Mapping Mode**(유효한 매핑 모드) 및 **Target Application**(대상 애플리케이션)에 매핑합니다.

매핑이 유효하게 되면 유효한 매핑 수가 증가하는 것을 확인할 수 있습니다.

단계 2 **Blank Mappings**(빈 매핑)을 클릭하여 해당 마이그레이션에 대한 빈 매핑 목록을 확인합니다. **Blank Source Application**(빈 소스 애플리케이션)을 유효한 **Mapping Mode**(매핑 모드) 및 **Target Application**(대상 애플리케이션)에 매핑합니다.

예를 들어 매핑 모드를 선택하고 대상을 입력하지 않고 저장하면 빈 매핑의 수가 증가합니다. 탭을 검토하고 올바르게 매핑한 다음 마이그레이션을 진행합니다.



참고 빈 매핑이 있더라도 마이그레이션을 계속할 수 있습니다.

단계 3 **Invalid Mappings**(유효하지 않은 매핑) 탭을 클릭하여 유효하지 않은 매핑 목록을 확인합니다. 다음을 수행하십시오.

- a) **Invalid Application**(유효하지 않은 애플리케이션) - 마이그레이션 중에 잘못된 매핑을 표시합니다.
- b) **Mapping Mode**(매핑 모드) - **Application**(애플리케이션) 또는 **Port**(포트) 중에서 매핑 모드를 선택합니다.
- c) **Target Application**(대상 애플리케이션) - 애플리케이션 매핑의 대상 애플리케이션을 선택합니다.

예를 들어 매핑 모드를 선택했지만 다른 대상에 매핑한 경우, 다른 탭으로 진행할 수 없습니다. **Invalid Mappings**(유효하지 않은 매핑) 탭을 검토하고 올바른 대상 애플리케이션을 입력한 다음 애플리케이션 매핑을 수행합니다.

단계 4 각 탭에서 **Validate**(검증)를 클릭하여 해당 마이그레이션에 대해 유효하지 않거나 비어 있거나 유효한 매핑을 검증합니다.

단계 5 **Next**(다음)를 클릭하여 계속 진행합니다.

단계 6 **Clear Mapped Data**(매핑된 데이터 지우기)를 클릭하여 수동으로 수행한 매핑을 검증 전에 지웁니다. 수행 중인 매핑에 대해 완전히 확신할 수 있는 경우에만 **Validate**(검증)를 클릭하는 것이 좋습니다. 검증을 클릭한 후에는 매핑을 취소할 수 없고 매핑이 유효하게 되기 때문입니다.

다음에 수행할 작업

마이그레이션할 컨피그레이션 검토 및 검증

최적화, 구성 검토 및 검증

마이그레이션된 구성을 Firewall Management Center로 푸시하기 전에 구성을 최적화하고 신중하게 검토하여 해당 구성이 올바르며 Firewall Threat Defense 디바이스 구성 방법과 일치하는지 확인하십시오. 깜박이는 탭은 다음 작업 과정을 수행해야 함을 나타냅니다.



참고 **Optimize, Review and Validate Configuration**(구성 최적화, 검토 및 검증) 화면에서 Secure Firewall 마이그레이션 톨을 닫으면 진행 상황이 저장되고 나중에 마이그레이션을 재개할 수 있습니다. 이 화면 전에 Secure Firewall 마이그레이션 톨을 닫으면 진행 상황이 저장되지 않습니다. 구문 분석 후 오류가 발생한 경우 Secure Firewall 마이그레이션 톨을 다시 실행하면 **Interface Mapping**(인터페이스 매핑) 화면에서 재개됩니다.

여기서 Secure Firewall 마이그레이션 툴은 Firewall Management Center에 이미 있는 IPS(Intrusion Prevention System, 침입 방지 시스템) 정책 및 파일 정책을 가져와 마이그레이션 중인 액세스 제어 규칙에 연결할 수 있도록 합니다.

파일 정책은 네트워크에 대한 지능형 악성코드 차단 및 파일 제어를 수행하기 위해 시스템에서 전체 액세스 제어 구성의 일부로 사용하는 구성 집합입니다. 이 연결은 시스템이 액세스 제어 규칙의 조건에 일치하는 트래픽에 파일을 통과시키기 전에 먼저 파일을 검사하도록 합니다.

마찬가지로 트래픽이 대상으로 들어가기 전 시스템의 최후의 방어선으로 IPS 정책을 사용할 수 있습니다. 침입 정책은 보안 위반 확인을 위해 시스템이 인라인 배포에서 트래픽을 검사하는 방식을 제어하며, 악성 트래픽을 차단하거나 변경할 수 있습니다. 시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 연결된 변수 집합을 사용합니다. 집합 내 대부분의 변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 규칙 삭제, 동적 규칙 상태의 IP 주소를 나타내려면 침입 정책 내 변수를 사용할 수도 있습니다.

탭에서 특정 컨피그레이션 항목을 검색하려면 열 맨 위의 필드에 항목 이름을 입력합니다. 검색어와 일치하는 항목만 표시하도록 테이블 행이 필터링됩니다.



참고 기본적으로 인라인 그룹화 옵션은 활성화되어 있습니다.

Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증) 화면에서 Secure Firewall 마이그레이션 툴을 닫으면 진행 상황이 저장되고 나중에 마이그레이션을 재개할 수 있습니다. 이 화면 전에 닫으면 진행 상황이 저장되지 않습니다. 구문 분석 후 오류가 발생한 경우 Secure Firewall 마이그레이션 툴을 다시 실행하면 **Interface Mapping**(인터페이스 매핑) 화면에서 재개됩니다.

Secure Firewall 마이그레이션 툴 ACL 최적화 개요

Secure Firewall 마이그레이션 툴은 네트워크 기능에 영향을 주지 않고 방화벽 규칙 베이스에서 최적화(비활성화 또는 삭제)할 수 있는 ACL을 식별하고 분리하기 위한 지원을 제공합니다.

ACL 최적화는 다음 ACL 유형을 지원합니다.

- **중복 ACL** - 두 ACL에 동일한 컨피그레이션 및 규칙 집합이 있는 경우 기본이 아닌 ACL을 제거해도 네트워크에 영향을 주지 않습니다. 예를 들어, 액세스 거부에 대해 정의된 규칙 없이 동일한 네트워크에서 FTP 및 IP 트래픽을 허용하는 두 규칙이 있는 경우 첫 번째 규칙을 삭제할 수 있습니다.
- **새도우 ACL** - 첫 번째 ACL은 두 번째 ACL의 컨피그레이션을 완전히 새도우합니다. 두 규칙에 유사한 트래픽이 있는 경우, 두 번째 규칙은 액세스 목록의 뒷부분에 나타나므로 어떤 트래픽에도 적용되지 않습니다. 두 규칙이 트래픽에 대해 서로 다른 작업을 지정하는 경우, 새도우된 규칙을 이동하거나 규칙 중 하나를 편집하여 필요한 정책을 구현할 수 있습니다. 예를 들어 기본 규칙은 IP 트래픽을 거부할 수 있으며, 새도우된 규칙은 지정된 소스 또는 대상에 대한 FTP 트래픽을 허용할 수 있습니다.
- **ACL 비활성화**—방화벽 구성에서 명시적으로 비활성화된 ACL입니다. 규칙은 구성 파일에 존재하지만, Secure Firewall 마이그레이션 툴은 트래픽을 처리할 때 해당 규칙을 무시합니다.

Secure Firewall 마이그레이션 툴은 ACL 최적화를 위한 규칙을 비교하는 동안 다음 매개변수를 사용합니다.



참고 최적화는 ACP 규칙에 대해서만 PAN에 사용할 수 있습니다.

- 소스 ACL은 해당 ACE(인라인 값)로 확장된 후 다음 매개변수에 대해 비교됩니다.
 - 소스 및 대상 영역
 - 소스 및 대상 네트워크
 - 소스 및 대상 포트

Download Report(보고서 다운로드)를 클릭하여 Excel 파일로 정리된 ACL 이름과 이에 해당하는 중복, 새도, 비활성화된 ACL을 검토합니다. 자세한 ACL 정보를 보려면 세부 **ACL** 정보 시트를 사용합니다.

동적 IP/포트 대체 인터페이스

Palo Alto Networks에서 Threat Defense로 마이그레이션에 대한 **Optimize, Review and Validate Configuration**(구성 최적화, 검토 및 검증) 페이지에서 NAT 구성을 검토할 때, NAT 규칙에 동적 IP/포트-대체 구성 설정이 있는지와 규칙이 마이그레이션 또는 삭제되었는지를 확인할 수 있습니다.

Secure Firewall 마이그레이션 툴은 구성된 동적 IP 또는 포트 대체 인터페이스 주소가 대상 영역 주소와 동일한 경우 NAT 규칙을 마이그레이션합니다. 이 값이 다르면 규칙이 마이그레이션되지 않고 지원되지 않는 것으로 나열됩니다. Secure Firewall Management Center는 대상 주소만 동적 IP 또는 포트 대체 인터페이스로 가질 수 있기 때문입니다. NAT 규칙에 대체 구성이 없는 경우, 마이그레이션이 검증 없이 발생하며 **Dynamic IP/Port-Fallback**(동적 IP/포트-대체) 열에서 **Not Available**(해당 없음)로 나열됩니다.

프로시저

단계 1 Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증) 화면에서 **Access Control Rules**(액세스 제어 규칙)를 클릭하고 다음과 같이 합니다.

- a) 테이블의 각 항목에 대해 매핑을 검토하고 올바른지 확인합니다.
- b) 하나 이상의 액세스 제어 목록 정책을 마이그레이션하지 않으려면 해당 행의 확인란을 선택하고 **Actions**(작업) **Do not migrate**(마이그레이션 하지 않음)을 선택한 다음 **Save**(저장)를 클릭합니다.

마이그레이션하지 않도록 선택하는 모든 규칙은 테이블에서 회색으로 표시됩니다.

- c) 액세스 제어 목록 정책을 편집하려면 해당 정책 옆의 체크 박스를 선택하고 **Actions**(작업) > **Edit**(편집)를 선택합니다.
- d) **Edit Rule**(규칙 편집) 대화 상자에서 기존 데이터를 업데이트하거나 새 데이터를 추가합니다.

소스 또는 대상에 개체를 추가하려면:

1. 왼쪽 창에서 해당 개체 옆에 있는 체크 박스를 선택합니다.

2. **Selected Sources**(선택된 소스) 또는 **Selected Destination and Applications**(선택된 대상 및 애플리케이션) 열 아래에 있는 **Add Source**(소스 추가) 또는 **Add Destination**(대상 추가) 버튼을 클릭하여 개체를 해당 위치로 이동합니다.

또한 삭제 아이콘을 클릭하여 소스 또는 대상에서 기존 개체를 삭제할 수도 있습니다.



참고 적용되지 않는 규칙은 표에서 회색으로 표시됩니다.

- e) 하나 이상의 액세스 제어 정책에 Firewall Management Center 파일 정책을 적용하려면 해당 행의 체크 박스를 선택하고 **Actions**(작업) > **File Policy**(파일 정책)를 선택합니다.

File Policy(파일 정책) 대화 상자에서 적절한 파일 정책을 선택하고 선택한 액세스 제어 정책에 적용한 후 **Save**(저장)를 클릭합니다.

- f) 하나 이상의 액세스 제어 정책에 Firewall Management Center IPS 정책을 적용하려면 해당 행의 체크 박스를 선택하고 **Actions**(작업) > **IPS Policy**(IPS 정책)를 선택합니다.

IPS Policy(IPS 정책) 대화 상자에서 적절한 IPS 정책과 해당 변수 집합을 선택하고 선택한 액세스 제어 정책에 적용한 후 **Save**(저장)를 클릭합니다.

- g) 기록이 활성화된 액세스 제어 규칙의 기록 옵션을 변경하려면 해당 행의 체크 박스를 선택하고 **Actions**(작업) > **Log**(로그)를 선택합니다.

Log(로그) 대화 상자에서 연결 시작 또는 종료 시 또는 두 경우에 모두 이벤트 기록을 활성화할 수 있습니다. 기록을 활성화한 경우 **Event Viewer**(이벤트 뷰어) 또는 **Syslog**(시스템 로그) 또는 둘 다에 연결 이벤트를 보내도록 선택해야 합니다. 시스템 로그 서버에 연결 이벤트를 전송하도록 선택하는 경우 **Syslog**(시스템 로그) 드롭다운 메뉴에서 Firewall Management Center에 이미 구성된 시스템 로그 정책을 선택할 수 있습니다.

- h) 액세스 제어 테이블에서 마이그레이션된 액세스 제어 규칙에 대한 작업을 변경하려면 해당 행의 체크 박스를 선택하고 **Actions**(작업) > **Rule Action**(규칙 작업)을 선택합니다.



팁 액세스 제어 규칙에 연결된 IPS 및 파일 정책은 **Allow**(허용) 옵션을 제외한 모든 규칙 작업 시 자동으로 제거됩니다.

오름차순, 내림차순, 같음, 보다 큼, 보다 작음 필터링 순서 시퀀스로 ACE 수를 필터링할 수 있습니다.

기존 필터 기준을 지우고 새 검색을 로드하려면 **Clear Filter**(필터 지우기)를 클릭합니다.



참고 ACE를 기준으로 ACL을 정렬하는 순서는 보기 전용입니다. ACL은 발생한 연대순으로 표시됩니다.

단계 2 다음 탭을 클릭하고 컨피그레이션 항목을 검토합니다.

- 액세스 제어

- 개체(네트워크 개체, 포트 개체, URL 개체, VLAN 태그)
- NAT
- 인터페이스
- 경로
- 사이트 간 VPN 터널
- 원격 액세스 VPN



참고 사이트 간 및 원격 액세스 VPN 구성의 경우 이와 관련된 VPN 필터 구성 및 확장 액세스 목록 개체가 마이그레이션되며 각 탭에서 검토할 수 있습니다.

하나 이상의 NAT 규칙 또는 라우팅 인터페이스를 마이그레이션하지 않으려면 해당 행의 체크 박스를 선택하고 **Actions(작업) > Do not migrate(마이그레이션하지 않음)**를 선택한 다음 **Save(저장)**를 클릭합니다.

마이그레이션하지 않도록 선택하는 모든 규칙은 테이블에서 회색으로 표시됩니다.

단계 3 (선택 사항) 구성을 검토하는 동안 **Network Objects(네트워크 개체)** 또는 **Port Objects(포트 개체)** 탭에서 **Actions(작업) > Rename(이름 변경)**를 선택하여 하나 이상의 네트워크 또는 포트 개체의 이름을 변경할 수 있습니다.

이름이 변경된 개체를 참조하는 액세스 규칙 및 NAT 정책도 새 개체 이름으로 업데이트됩니다.

단계 4 **Routes(경로)** 영역에서 경로를 보고 항목을 선택하고 **Actions(작업) > Do not Migration(마이그레이션 안 함)**을 선택하여 마이그레이션하지 않을 경로를 선택할 수 있습니다.

단계 5 **Site-to-Site VPN Tunnels(사이트 간 VPN 터널)** 섹션에는 소스 방화벽 구성의 VPN 터널이 나열됩니다. 각 행의 소스 인터페이스, VPN 유형, IKEv1 및 IKEv2 구성과 같은 VPN 터널 데이터를 검토하고 모든 행에 사전 공유 키 값을 제공하는지 확인합니다.

단계 6 여러 사이트 간 VPN 터널 구성이 포함된 구성의 경우 여러 항목에 대한 사전 공유 키를 한 번에 업데이트하려면 아래 단계를 수행합니다.

- 사전 공유 키를 업데이트 할 사이트 간 VPN 구성 항목을 선택합니다.

- 테이블을 편집 가능한 Excel 시트로 내보내려면 다운로드()를 클릭합니다.

- 각 VPN 설정에 대한 각 열에 사전 공유 키를 입력하고 파일을 저장합니다. IKE의 IKEv1 및 IKEv2 버전을 모두 포함하는 VPN 설정의 경우에는 두 값을 쉼표로 구분하여 열에 입력합니다.

- 업로드()를 클릭합니다. 마이그레이션 툴이 Excel의 항목을 읽고 VPN 구성의 해당 사전 공유 키 열에 자동으로 추가합니다.



참고 누락된 사전 공유 키를 일괄 업데이트의 일환으로 업데이트하려면 항목을 선택하고 **Actions(작업) > Update Pre-Shared Key(사전 공유 키 업데이트)**를 선택하는 기본 방법을 사용하거나 Excel을 내보내고 키를 업데이트한 다음 키를 가져옵니다.

대상 위협 방어 디바이스가 이미 사이트 간 VPN 토폴로지를 구성하고 있는 경우, 마이그레이션 툴은 이를 탐지하고 이를 삭제할지 여부를 선택하라는 메시지를 표시합니다. 삭제를 선택하면 마이그레이션 툴이 자동으로 삭제하므로 관리 센터에 로그인하여 수동으로 삭제하지 않아도 됩니다. **No(아니요)**를 선택하는 경우, 마이그레이션을 계속하려면 대상 위협 방어 디바이스에서 기존 VPN 구성을 수동으로 삭제해야 합니다.

단계 7 Remote Access VPN(원격 액세스 VPN) 섹션에서는 원격 액세스 VPN에 해당하는 모든 개체가 Palo Alto Networks Firewall에서 Management Center로 마이그레이션되며 다음과 같이 표시됩니다.

- **Policy Assignment(정책 할당)**: 연결 프로파일, VPN 프로토콜, 대상 디바이스 및 VPN 인터페이스의 이름을 검토하고 검증합니다. 연결 프로파일의 이름을 변경하려면 해당 항목을 선택하고 **Actions(작업) > Rename(이름 변경)**을 선택합니다.
- **IKEV2**: IKEv2 프로토콜 구성 및 해당 구성으로 매핑된 소스 인터페이스(있는 경우)를 검토하고 검증합니다.
- **Anyconnect Packages(AnyConnect 패키지)**: AnyConnect 패키지, 를 검색하고 AnyConnect 프로파일은 마이그레이션을 위해 소스 디바이스에서 검색되어야 합니다.

마이그레이션 전 작업의 일부로 모든 AnyConnect 패키지를 Management Center에 업로드합니다. AnyConnect 프로파일을 Management Center에 직접 업로드하거나 Secure Firewall 마이그레이션 툴에서 업로드할 수 있습니다.

Management Center에서 가져온 기존 AnyConnect, Hostscan 또는 외부 브라우저 패키지를 선택합니다. AnyConnect 패키지를 하나 이상 선택해야 합니다. 소스 구성에서 사용 가능한 경우 Hostscan, dap.xml, data.xml 또는 외부 브라우저를 선택해야 합니다. AnyConnect 프로파일은 선택 사항입니다.

소스 방화벽에서 올바른 Dap.xml 파일이 검색되는지 확인합니다. 구성 파일에 있는 dap.xml에 대해 검증이 수행됩니다. 검증에 필요한 모든 파일을 선택하고 업로드해야 합니다. 업데이트에 실패하면 완료되지 않은 것으로 표시되고 Secure Firewall 마이그레이션 툴이 검증을 진행하지 않습니다.

- **Address Pool(주소 풀)** - 여기에 표시된 모든 Ipv4 및 Ipv6 풀을 검토합니다.
- **Group-Policy(그룹 정책)** - 이 영역에서 사용자 프로파일, 관리 프로파일, 클라이언트 모듈 프로파일을 선택하거나 제거합니다. 이 영역에는 클라이언트 프로파일이 있는 그룹 정책, 관리 프로파일, 관리 모듈이 표시되며, 프로파일이 없는 그룹 정책이 표시됩니다. 프로파일이 AnyConnect file(AnyConnect 파일) 섹션에 추가된 경우 사전 선택된 것으로 표시됩니다. 사용자 프로파일, 관리 프로파일 및 클라이언트 모듈 프로파일을 선택하거나 제거할 수 있습니다.
- **Connection Profile(연결 프로파일)** - 여기에 표시된 모든 연결 프로파일/터널 그룹을 검토합니다.
- **Trustpoints(트러스트 포인트)** - PAN Firewall에서 Management Center로의 트러스트 포인트 또는 PKI 개체 마이그레이션은 사전 마이그레이션 활동의 일부이며 원격 액세스 VPN을 성공적으로 마이그레이션하는 데 필요합니다. **Remote Access Interface(원격 액세스 인터페이스)** 섹션에서 전역 SSL, IKEv2 및 인터페이스에 대한 트러스트 포인트를 매핑하여 다음 마이그레이션 단계를 진행합니다.

SAML(Security Assertion Markup Language, 보안 어설션 마크업 언어) 개체가 존재하는 경우 SAML 섹션에서 SAML IDP 및 SP에 대한 트러스트 포인트를 매핑할 수 있습니다. SP 인증서 업로드는 선택 사항입니다. 특정 터널 그룹에 대해 트러스트 포인트를 재정의할 수도 있습니다. 재정의된 SAML 트러스트 포인트 구성을 소스에서 사용할 수 있는 경우 **Override SAML(SAML 재정의)** 옵션에서 선택할 수 있습니다.

단계 8 (선택 사항) 그리드의 각 구성 항목에 대한 세부 정보를 다운로드하려면 **Download(다운로드)**를 클릭합니다.

단계 9 검토를 완료한 후 **Validate(검증)**를 클릭합니다. 확인이 필요한 필수 필드는 값을 입력할 때까지 계속 깜박입니다. 모든 필수 필드를 입력한 후에만 유효성 검사 버튼이 활성화됩니다.

검증 과정에서 Secure Firewall 마이그레이션 툴은 Firewall Management Center에 연결하여 기존 개체를 검토하고 마이그레이션할 개체 목록과 비교합니다. 개체가 이미 Firewall Management Center에 있는 경우 Secure Firewall 마이그레이션 툴은 다음과 같이 합니다.

- 개체의 이름과 구성이 동일한 경우 Secure Firewall 마이그레이션 툴은 기존 개체를 재사용하고 Firewall Management Center에 새 개체를 생성하지 않습니다.
- 개체의 이름은 같지만 구성이 다른 경우 Secure Firewall 마이그레이션 툴이 개체 충돌을 보고합니다.

콘솔에서 검증 진행 상황을 볼 수 있습니다.

단계 10 검증이 완료된 후 **Validation Status(검증 상태)** 대화 상자에 하나 이상의 개체 충돌이 표시되면 다음과 같이 합니다.

a) **Resolve Conflicts(충돌 해결)**를 클릭합니다.

Secure Firewall 마이그레이션 툴은 개체 충돌이 보고된 위치에 따라 **Network Objects(네트워크 개체)** 또는 **Port Objects(포트 개체)** 탭 중 하나 또는 둘 다에 경고 아이콘을 표시합니다.

b) 탭을 클릭하고 개체를 검토합니다.

c) 충돌이 있는 각 개체의 항목을 확인하고 **Actions(작업) > Resolve Conflicts(충돌 해결)**를 선택합니다.

d) **Resolve Conflicts(충돌 해결)** 창에서 권장 작업을 완료합니다.

예를 들어, 기존 Firewall Management Center 개체와의 충돌을 방지하기 위해 개체 이름에 접미사를 추가하라는 메시지가 표시될 수 있습니다. 기본 접미사를 수락하거나 자체 접미사로 대체할 수 있습니다.

e) **Resolve(해결)**를 클릭합니다.

f) 탭에서 모든 개체 충돌을 해결했으면 **Save(저장)**를 클릭합니다.

g) **Validate(검증)**를 클릭하여 컨피그레이션을 재검증하고 모든 개체 충돌이 해결되었는지 확인합니다.

단계 11 **Optimize Your Configuration(구성 최적화)** 대화 상자에는 최적화된 각 속성 옆에 체크 표시가 나타나며, 최적화가 필요한 속성을 표시합니다. **Proceed(진행)**를 클릭하여 최적화를 시작합니다. 최적화 단계를 건너뛸 수는 있지만, 마이그레이션을 진행하기 전에 속성을 최적화하는 것이 좋습니다.

단계 12 검증이 완료되고 **Validation Status(검증 상태)** 대화 상자에 **Successfully Validated(검증 성공)** 메시지가 표시되면 마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시, 26 페이지로 진행합니다.

마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시

구성을 성공적으로 검증하고 모든 개체 충돌을 해결하지 않은 경우 마이그레이션된 구성을 Firewall Management Center에 푸시할 수 없습니다.

마이그레이션 프로세스의 이 단계에서는 마이그레이션된 컨피그레이션을 Firewall Management Center에 보냅니다. Firewall Threat Defense 디바이스에 컨피그레이션이 구축되지 않습니다. 하지만 Firewall Threat Defense의 모든 기존 컨피그레이션이 이 단계에서 지워집니다.



참고 Secure Firewall 마이그레이션 툴이 마이그레이션된 구성을 Firewall Management Center에 보내는 동안에는 구성을 변경하거나 디바이스에 구축하지 마십시오.

프로시저

단계 1 Validation Status(검증 상태) 대화 상자에서 검증 요약を 검토합니다.

단계 2 Push Configuration(구성 푸시)을 클릭하여 마이그레이션된 구성을 Firewall Management Center에 보냅니다.



참고 Secure Firewall 마이그레이션 툴이 중복 개체 속성을 감지하면 대화 상자가 나타나 중복된 값을 수정하라는 메시지가 표시됩니다. 중복 속성의 이름을 변경한 후에야 마이그레이션을 진행할 수 있습니다.

Secure Firewall 마이그레이션 툴에 마이그레이션 진행 상황의 요약이 표시됩니다. 콘솔에서 Firewall Management Center에 푸시되는 구성 요소의 세부적인 라인별 진행 상황을 볼 수 있습니다.



참고 대량 구성 푸시가 수행될 때 오류가 있는 구성이 있는 경우, 마이그레이션 툴에서 마이그레이션을 중단하여 오류를 수동으로 수정하거나 잘못된 구성 없이 마이그레이션을 계속하라는 메시지를 표시하는 경고가 표시됩니다. 오류가 있는 구성을 표시하도록 선택한 다음 **Continue with migration(마이그레이션 계속 진행)** 또는 **Abort(중단)**를 선택할 수 있습니다. 마이그레이션을 중단하는 경우 문제 해결 번들을 다운로드하고 분석을 위해 Cisco TAC와 공유할 수 있습니다.

마이그레이션을 계속하면 마이그레이션 툴이 마이그레이션을 부분 성공 마이그레이션으로 처리합니다. 마이그레이션 후 보고서를 다운로드하여 푸시 오류로 인해 마이그레이션되지 않은 구성 목록을 볼 수 있습니다.

단계 3 마이그레이션이 완료되면 **Download Report(보고서 다운로드)**를 클릭하여 마이그레이션 후 보고서를 다운로드하고 저장합니다.

Post-Migration Report(마이그레이션 후 보고서)의 사본도 Secure Firewall 마이그레이션 툴과 동일한 위치의 Resources 폴더에 저장됩니다.

단계 4 마이그레이션이 실패한 경우 마이그레이션 후 보고서, 로그 파일, 구문 분석되지 않은 파일을 신중하게 검토하여 실패의 원인을 파악합니다.

문제 해결을 위해 지원 팀에 문의할 수도 있습니다.

마이그레이션 실패 지원

마이그레이션이 실패할 경우 지원 팀에 문의합니다.

1. **Complete Migration**(마이그레이션 완료) 화면에서 **Support**(지원) 버튼을 클릭합니다.

도움말 지원 페이지가 나타납니다.

2. **Support Bundle**(지원 번들) 체크 박스를 선택한 다음 다운로드할 컨피그레이션 파일을 선택합니다.



참고 로그 및 dB 파일은 기본적으로 다운로드하도록 선택됩니다.

3. **Download**(다운로드)를 클릭합니다.

지원 번들 파일은 로컬 경로에 .zip으로 다운로드됩니다. 압축 폴더의 압축을 풀고 로그 파일, DB 및 컨피그레이션 파일을 봅니다.

4. **Email us**(이메일 문의)를 클릭하여 기술 팀에 실패 세부 정보를 이메일로 보냅니다.

다운로드한 지원 파일을 이메일에 첨부할 수도 있습니다.

5. **Visit TAC page**(TAC 페이지 방문)를 클릭하여 Cisco 지원 페이지에서 TAC 케이스를 생성합니다.



참고 마이그레이션하는 동안 언제든지 지원 페이지에서 TAC 케이스를 열 수 있습니다.

마이그레이션 후 보고서 검토 및 마이그레이션 완료

마이그레이션 후 보고서는 다양한 범주의 ACL 수, ACL 최적화 및 컨피그레이션 파일에서 수행된 최적화의 전체 보기에 대한 세부 정보를 제공합니다. 자세한 내용은 [최적화, 구성 검토 및 검증, 19 페이지](#)를 참조해 주십시오.

개체를 검토하고 확인합니다.

- 카테고리
 - 총 ACL 규칙(소스 컨피그레이션)
 - 최적화를 위해 고려된 총 ACL 규칙. 예를 들어, 중복, 새도우 등이 있습니다.
 - 최적화할 ACL 수는 최적화 전후에 계산한 총 ACL 규칙 수를 제공합니다.

마이그레이션 중에 마이그레이션 후 보고서를 다운로드하지 못한 경우 다음 링크를 사용하여 다운로드하십시오.

마이그레이션 후 보고서 다운로드 엔드포인트 - http://localhost:8888/api/downloads/post_migration_summary_html_format



참고 Secure Firewall 마이그레이션 툴이 실행 중일 때만 보고서를 다운로드할 수 있습니다.

프로시저

단계 1 **Post-Migration Report**(마이그레이션 후 보고서)를 다운로드한 위치로 이동합니다.

단계 2 마이그레이션 후 보고서를 열고 내용을 신중하게 검토하여 구성이 어떻게 마이그레이션되었는지 파악합니다.

- **Migration Summary**(마이그레이션 요약) - 에서 Firewall Threat Defense로 성공적으로 마이그레이션된 구성의 요약으로, 인터페이스, Firewall Management Center 호스트 이름 및 도메인, 대상 Firewall Threat Defense 디바이스(적용 가능한 경우) 및 성공적으로 마이그레이션된 구성 요소에 대한 정보가 포함됩니다.

또한 마이그레이션 전과 마이그레이션 후의 상태 수 차이를 보여주는 비교 차트를 확인할 수 있습니다.

- **Selective Policy Migration**(선택적 정책 마이그레이션) - 마이그레이션하도록 선택한 특정 기능에 대한 세부 정보를 Device Configuration Features(디바이스 구성 기능), Shared Configuration Features(공유 구성 기능), Optimization(최적화)의 세 범주에서 확인할 수 있습니다.
- **Interface to Threat Defense Interface Mapping**(ASA FPS 포함 ASA FDM 매니지드 디바이스 인터페이스-Threat Defense 인터페이스 매핑) - 성공적으로 마이그레이션된 인터페이스와 구성의 인터페이스를 Firewall Threat Defense 디바이스의 인터페이스에 매핑한 방법에 대한 세부 정보입니다. 이러한 매핑이 예상과 일치하는지 확인합니다.



참고 이 섹션은 마이그레이션에 대상 Firewall Threat Defense 디바이스가 없는 경우 또는 인터페이스를 마이그레이션하도록 선택하지 않은 경우에는 적용되지 않습니다.

- **Source Interface Names to Threat Defense Security Zones**(소스 인터페이스 이름 - Threat Defense 보안 영역) - 성공적으로 마이그레이션된 PAN 논리적 인터페이스 및 이름과 Firewall Threat Defense에서 이를 보안 영역에 매핑한 방법에 대한 세부 정보입니다. 이러한 매핑이 예상과 일치하는지 확인합니다.



참고 **Access Control Lists**(액세스 제어 목록) 및 **NAT**가 마이그레이션하도록 선택되지 않은 경우 이 섹션은 적용되지 않습니다.

- **Object Conflict Handling(개체 충돌 처리)** - Firewall Management Center의 기존 개체와 충돌하는 것으로 확인된 개체에 대한 세부 정보입니다. 개체의 이름과 구성이 동일한 경우 Secure Firewall 마이그레이션 툴에서 Firewall Management Center 개체를 재사용했습니다. 개체의 이름은 같지만 컨피그레이션이 다른 경우 해당 개체의 이름을 변경했습니다. 이러한 개체를 신중하게 검토하고 충돌이 적절하게 해결되었는지 확인합니다.
- **Access Control Rules, NAT, and Routes You Chose Not to Migrate(마이그레이션하지 않도록 선택한 액세스 제어 규칙, NAT 및 경로)** - Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션하지 않도록 선택한 규칙에 대한 세부 정보입니다. Secure Firewall 마이그레이션 툴에서 비활성화되고 마이그레이션되지 않은 이러한 규칙을 검토합니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
- **Partially Migrated Configuration(부분적으로 마이그레이션된 구성)** - 고급 옵션이 포함되어 있지만 고급 옵션 없이 마이그레이션될 수 있는 규칙을 비롯하여 부분적으로만 마이그레이션된 규칙에 대한 세부 정보입니다. 이러한 라인을 검토하고 Firewall Management Center에서 고급 옵션이 지원되는지 확인한 다음 지원되는 경우 해당 옵션을 수동으로 구성합니다.
- **Unsupported Configuration(지원되지 않는 구성)** - Secure Firewall 마이그레이션 툴이 해당 기능의 마이그레이션을 지원하지 않으므로 마이그레이션할 수 없는 구성 요소에 대한 세부 정보입니다. 이러한 라인을 검토하여 각 기능이 Firewall Threat Defense에서 지원되는지 확인합니다. 지원되는 경우 Firewall Management Center에서 해당 기능을 수동으로 구성합니다.
- **Expanded Access Control Policy Rules(확장 액세스 제어 정책 규칙)** - 마이그레이션 중에 단일 포인트 규칙에서 여러 Firewall Threat Defense 규칙으로 확장된 액세스 제어 정책 규칙에 대한 세부 정보입니다.
- **Actions Taken on Access Control Rules(액세스 제어 규칙에 대해 수행된 작업)**
 - **Access Rules You Chose Not to Migrate(마이그레이션하지 않도록 선택한 액세스 규칙)** - Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션하지 않도록 선택한 액세스 제어 규칙에 대한 세부 정보입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
 - **Access Rules with Rule Action Change(규칙 작업이 변경된 액세스 규칙)** - Secure Firewall 마이그레이션 툴을 사용하여 '규칙 작업'이 변경된 모든 액세스 제어 정책 규칙에 대한 세부 정보입니다. 규칙 작업 값은 Allow(허용), Trust(신뢰), Monitor(모니터링), Block(차단), Block with reset(차단 후 재설정)입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
 - **Access Control Rules that have IPS Policy and Variable Set Applied(IPS 정책 및 변수 집합이 적용된 액세스 제어 규칙)** - IPS 정책이 적용된 모든 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 Firewall Threat Defense에서 해당 기능이 지원되는지 확인합니다.
 - **Access Control Rules that have File Policy Applied(파일 정책이 적용된 액세스 제어 규칙)** - 파일 정책이 적용된 모든 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 Firewall Threat Defense에서 해당 기능이 지원되는지 확인합니다.
 - **Access Control Rules that have Rule 'Log' Setting Change(규칙 '로그' 설정이 변경된 액세스 제어 규칙)** - Secure Firewall 마이그레이션 툴을 사용하여 '로그 설정'이 변경된 액세스 제어 규칙에 대한 세부 정보입니다. 로그 설정 값은 False(거짓), Event Viewer(이벤트 뷰어), Syslog(시스템 로그)입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.

- **Errors/Failure on Migrated Configuration(마이그레이션된 구성의 오류/실패)** — 마이그레이션된 구성 요소를 적용하는 과정에서 마이그레이션 실패를 유발한 오류에 대한 세부 정보입니다. 아래에 보고된 오류는 잘못 마이그레이션된 구성 때문일 수도 있고, 기존 구성이나 지원되지 않는 기능으로 인해 관리 센터에서 충돌이 발생한 것일 수도 있습니다. 대상 관리 센터로 구성을 전송하거나 재개하기 전에 이러한 오류를 검토하고 확인하십시오.



참고 마이그레이션되지 않은 지원되지 않는 규칙은 원치 않는 트래픽이 방화벽을 통과하는 문제를 일으킵니다. 이 트래픽이 Firewall Threat Defense에서 차단되도록 Firewall Management Center에서 규칙을 구성하는 것이 좋습니다.



참고 **Review and Validate(검토 및 검증)** 페이지에서 ACL에 IPS 또는 파일 정책을 적용해야 하는 경우 마이그레이션 전에 Management Center에서 정책을 생성하는 것이 좋습니다. Secure Firewall 마이그레이션 툴이 연결된 Management Center에서 정책을 가져오므로 동일한 정책을 사용합니다. 새 정책을 생성하고 여러 정책에 할당하면 성능이 저하될 수 있으며 푸시가 실패할 수도 있습니다.

Firewall Management Center 및 Firewall Threat Defense에서 지원되는 기능에 대한 자세한 내용은 [Management Center 컨피그레이션 가이드, 버전 6.2.3](#)을 참고하십시오.

단계 3 **Pre-Migration Report(마이그레이션 전 보고서)**를 열고 Firewall Threat Defense 디바이스에서 수동으로 마이그레이션해야 하는 구성 항목을 기록해 둡니다.

단계 4 Firewall Management Center에서 다음과 같이 합니다.

- Firewall Threat Defense 디바이스에 대해 마이그레이션된 컨피그레이션을 검토하여 다음을 비롯한 모든 예상 규칙 및 기타 컨피그레이션 항목이 마이그레이션되었는지 확인합니다.
 - ACL(액세스 제어 목록)
 - NAT(Network Address Translation) 규칙
 - 포트 및 네트워크 개체
 - 경로
 - 인터페이스
 - 유동 경로 개체
- 마이그레이션되지 않은 부분적으로 지원되는 항목 및 규칙, 지원되지 않는 항목 및 규칙, 무시된 항목 및 규칙, 비활성화된 항목 및 규칙을 모두 구성합니다.

이러한 항목 및 규칙에 대한 정보는 [Management Center 컨피그레이션 가이드](#)를 참고하십시오. 다음은 수동 구성이 필요한 컨피그레이션 항목의 예입니다.

- **Threat Defense의 플랫폼 설정**에 설명된 SSH 및 HTTPS 액세스를 포함한 플랫폼 설정
- **시스템 로그 구성**에 설명된 시스템 로그 설정

- Threat Defense 라우팅 개요에 설명된 동적 라우팅
- FlexConfig 정책에 설명된 서비스 정책
- Threat Defense VPN에 설명된 VPN 컨피그레이션
- 연결 기록에 설명된 연결 로그 설정

단계 5 검토를 완료한 후 마이그레이션된 컨피그레이션을 Firewall Management Center에서 Firewall Threat Defense 디바이스로 구축합니다.

지원되지 않는 규칙과 부분적으로 지원되는 규칙에 대한 데이터가 **Post-Migration Report**(마이그레이션 후 보고서)에 올바르게 반영되어 있는지 확인합니다.

Secure Firewall 마이그레이션 툴이 Firewall Threat Defense 디바이스에 정책을 할당합니다. 변경 사항이 실행 중인 컨피그레이션에 반영되어 있는지 확인합니다. 마이그레이션되는 정책을 쉽게 식별할 수 있도록 해당 정책의 설명에 구성의 호스트 이름이 포함되어 있습니다.

구문 분석 요약

구문 분석 요약에는 개체, 인터페이스, NAT, 정책 및 애플리케이션의 수가 표시됩니다. 요약은 사전 구문 분석 요약, 구문 분석 요약 및 사전 푸시 요약의 세 가지 구성 요소로 이루어집니다.

- 사전 구문 분석 요약- 사전 구문 분석 요약은 구성이 업로드된 후 표시됩니다. 이 단계에서 Secure Firewall 마이그레이션 툴은 다양한 구성 요소의 개수를 표시합니다. 사용자 정의 애플리케이션 또는 그룹에서 사용된 애플리케이션만 표시됩니다. 구성이 다중 가상 시스템인 경우 전체 vsys에 대한 인터페이스 수가 표시됩니다. 사전 구문 분석 요약에는 모든 애플리케이션이 표시되지 않습니다. 정책에서 직접 호출되는 애플리케이션은 계산에 포함되지 않기 때문입니다. 따라서 애플리케이션 수는 구문 분석 요약과 다릅니다. 유사한 동작이 NAT에 적용됩니다. 사전 구문 분석 요약의 일부 구성 요소가 개수 0을 표시할 수 있지만 이것이 해당 구성에 0 구성이 있다는 의미는 아닙니다.
- 구문 분석 요약- Start Conversion(변환 시작)을 클릭하면 구문 분석 요약이 표시됩니다. 이 단계에서 Secure Firewall 마이그레이션 툴이 구성에 대한 작업을 수행하며 지원되지 않는 모든 구성이 요약 수에서 제거됩니다. 지원되지 않는 정책도 개수에 포함됩니다. 지원되지 않는 정책은 비활성화된 상태로 Firewall Management Center로 마이그레이션되기 때문입니다. 구성의 모든 구성 요소가 구문 분석됩니다. 구문 분석 요약에 표시되는 개수는 마이그레이션될 정확한 구성 개수입니다.
- 사전 푸시 요약—사전 푸시 요약은 구성을 Firewall Management Center에 푸시하라는 프롬프트가 표시되기 전에 표시됩니다. 사전 구문 분석 요약 수는 Secure Firewall 마이그레이션 툴이 수행하는 작업에 따라 구문 분석 요약과 다를 수 있습니다. NAT에서 직접 참조된 IP는 개체로 푸시됩니다. 애플리케이션이 포트에 매핑된 경우, 서비스 수가 증가하고 애플리케이션이 중단됩니다. 애플리케이션 매핑을 비워 두면 애플리케이션 수가 줄어듭니다. 정적 경로 중복 항목이 있는 경우 해당 항목이 제거되고 수가 감소합니다.

마이그레이션 실패

다음은 마이그레이션 중 파싱 실패입니다.

- 파싱 실패 - Secure Firewall 마이그레이션 툴에 구성이 업로드된 후 파싱 실패가 발생했습니다. 인터페이스의 잘못된 구성으로 인한 것입니다. 여러 IP가 구성되거나 /32 또는 /128 IP가 인터페이스에 할당된 경우 파싱이 실패합니다.

인터페이스에 여러 IP가 할당되거나 터널링되거나, 루프백 또는 VLAN 인터페이스가 라우팅의 일부인 경우 푸시가 실패합니다.

해결 방법—사전 마이그레이션 보고서를 다운로드하고 마이그레이션 보고서의 오류가 있는 구성 라인 섹션을 참조합니다. 이 섹션에는 문제를 일으키는 구성의 세부 사항이 표시됩니다. 문제를 해결하고 구성을 Secure Firewall 마이그레이션 툴에 다시 업로드해야 합니다.

경로의 터널, 루프백 또는 VLAN 인터페이스로 인해 푸시 실패가 발생한 경우, 이러한 인터페이스는 Firewall Management Center에서 지원되지 않으므로 해당 경로를 삭제하고 마이그레이션을 다시 시도해야 합니다.

- 푸시 실패 - Secure Firewall 마이그레이션 툴이 구성을 마이그레이션하고 Firewall Management Center로 푸시하는 과정에서 푸시 실패가 발생합니다. 푸시 실패는 마이그레이션 후 보고서에 캡처됩니다.

해결 방법- 마이그레이션 후 보고서를 다운로드하고 마이그레이션 보고서의 오류 보고 섹션을 참조합니다. 이 섹션에는 문제를 일으키는 구성의 세부 정보가 표시됩니다. 실패가 표시되는 섹션에 대해 **do not migrate**(마이그레이션 안 함) 옵션을 선택하여 **Review and Validation**(검토 및 검증) 페이지에서 문제를 해결해야 합니다. 또는 소스 구성에서 문제를 수정하고 구성을 Secure Firewall 마이그레이션 툴에 다시 업로드할 수 있습니다.

Secure Firewall 마이그레이션 툴 제거

모든 구성 요소는 Secure Firewall 마이그레이션 툴과 같은 폴더에 저장됩니다.

시작하기 전에

이 절차는 Secure Firewall 마이그레이션 툴의 데스크톱 버전을 사용하는 경우에만 적용됩니다.

프로시저

단계 1 Secure Firewall 마이그레이션 툴을 배치한 폴더로 이동합니다.

단계 2 로그를 저장하려면 log 폴더를 잘라내거나 복사하여 다른 위치에 붙여 넣습니다.

단계 3 마이그레이션 전 보고서와 마이그레이션 후 보고서를 저장하려면 resources 폴더를 잘라내거나 복사하여 다른 위치에 붙여 넣습니다.

단계 4 Secure Firewall 마이그레이션 툴을 배치한 폴더를 삭제합니다.



팁 로그 파일은 콘솔 창과 연결되어 있습니다. Secure Firewall 마이그레이션 툴의 콘솔 창이 열려 있으면 로그 파일과 폴더를 삭제할 수 없습니다.

샘플 마이그레이션: PAN를 Threat Defense 2100으로



참고 마이그레이션을 완료한 후 대상 디바이스에서 실행할 수 있는 테스트 계획을 생성합니다.

- 유지 보수 기간 작업별
- 유지 보수 기간 작업, 34 페이지

유지 보수 기간 작업별

시작하기 전에

Firewall Management Center를 설치하고 구축했는지 확인합니다. 자세한 내용은 해당 [Firepower Management Center 하드웨어 설치 가이드](#) 및 해당 [Firepower Management Center 시작 가이드](#)를 참고하십시오.

프로시저

- 단계 1 네트워크에 Firepower 2100 Series 디바이스를 구축하고 인터페이스를 연결한 다음 어플라이언스의 전원을 켭니다.
자세한 내용은 [Management Center를 사용하는 2100 Series용 Cisco Threat Defense 빠른 시작 가이드](#)를 참고하십시오.
- 단계 2 Firewall Management Center에서 관리할 Firepower 2100 Series 디바이스를 등록합니다.
자세한 내용은 [Management Center에 디바이스 추가](#)를 참고하십시오.
- 단계 3 <https://software.cisco.com/download/home/286306503/type>에서 Secure Firewall 마이그레이션 툴의 최신 버전을 다운로드하여 실행합니다.
자세한 내용은 [Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드, 3 페이지](#)을 참고하십시오.
- 단계 4 Secure Firewall 마이그레이션 툴을 실행하고 대상 매개변수를 지정할 때 Firewall Management Center에 등록한 Firepower 2100 Series 디바이스를 선택하십시오.
자세한 내용은 [Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 8 페이지](#)을 참고하십시오.
- 단계 5 인터페이스와 Firewall Threat Defense 인터페이스를 매핑합니다.



참고 Secure Firewall 마이그레이션 툴을 사용하면 인터페이스 유형을 Firewall Threat Defense 인터페이스 유형에 매핑할 수 있습니다.

자세한 내용은 [Threat Defense 인터페이스와 인터페이스 매핑](#)을 참고하십시오.

단계 6 논리적 인터페이스를 보안 영역에 매핑하는 동안 **Auto-Create**(자동 생성)를 클릭하여 Secure Firewall 마이그레이션 툴이 새 보안 영역을 생성하도록 허용합니다. 기존 보안 영역을 사용하려면 논리적 인터페이스를 보안 영역에 수동으로 매핑합니다.

자세한 내용은 [보안 영역 및 인터페이스 그룹에 논리적 인터페이스 매핑](#)을 참고하십시오.

단계 7 이 가이드의 지침에 따라 마이그레이션할 컨피그레이션을 순차적으로 검토 및 검증한 다음 컨피그레이션을 Firewall Management Center로 푸시합니다.

단계 8 마이그레이션 후 보고서를 검토하고 Firewall Threat Defense에 다른 컨피그레이션을 수동으로 설정하고 구축한 다음 마이그레이션을 완료합니다.

자세한 내용은 [툴](#)을 참고하십시오.

단계 9 마이그레이션을 계획하는 동안 생성한 테스트 계획을 사용하여 Firepower 2100 Series 디바이스를 테스트합니다.

유지 보수 기간 작업

시작하기 전에

유지 보수 기간 전에 수행해야 하는 모든 작업을 완료했는지 확인합니다. [유지 보수 기간 작업별, 33 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 주변 스위칭 인프라에서 ARP(Address Resolution Protocol) 캐시를 지웁니다.

단계 2 주변 스위칭 인프라에서 Firepower 2100 Series 디바이스 인터페이스 IP 주소에 대한 기본 ping 테스트를 수행하여 액세스 가능한지 확인합니다.

단계 3 레이어 3 라우팅이 필요한 디바이스에서 Firepower 2100 Series 디바이스 인터페이스 IP 주소에 대한 기본 ping 테스트를 수행합니다.

단계 4 Firepower 2100 Series 디바이스에 새 IP 주소를 할당하고 예 할당된 IP 주소를 재사용하지 않는 경우 다음 단계를 수행합니다.

1. 이제 Firepower 2100 Series 디바이스 IP 주소를 가리키도록 IP 주소를 참조하는 모든 정적 경로를 업데이트합니다.
2. 라우팅 프로토콜을 사용하는 경우 인접한 라우터(neighbor router)에서 Firepower 2100 Series 디바이스 IP 주소가 예상 대상의 다음 홉으로 표시되는지 확인합니다.

단계 5 Firepower 2100 디바이스에 대해 관리 Firewall Management Center 내에서 포괄적인 테스트 계획을 실행하고 로그를 모니터링합니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.