# 마이그레이션 실행



# Cisco.com에서 Firewall 마이그레이션 툴 다운로드

시작하기 전에

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

단계 **1** 컴퓨터에서 Firewall 마이그레이션 툴용 폴더를 생성합니다.

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

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

단계 **2** https://software.cisco.com/download/home/286306503/type으로 이동하여 **Firewall** 마이그레이션 툴을 클릭합니다.

위 링크를 클릭하면 Firewall NGFW Virtual 아래의 Firewall 마이그레이션 툴로 이동합니다. 위협 방어 디바이스 다운로드 영역에서 Firewall 마이그레이션 툴을 다운로드할 수도 있습니다.

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

Windows 또는 macOS 시스템용 Firewall 마이그레이션 툴의 해당 실행 파일을 다운로드합니다.

# Firewall 마이그레이션 툴 실행

참고 Firewall 마이그레이션 툴을 실행하면 별도의 창에 콘솔이 열립니다. 마이그레이션을 진행하는 동안 Firewall 마이그레이션 툴에 현재 단계의 진행률이 콘솔에 표시됩니다. 화면에 콘솔이 표시되지 않으면 Firewall 마이그레이션 툴의 뒤에 있을 가능성이 높습니다.

시작하기 전에

- Cisco.com에서 Firewall 마이그레이션 툴 다운로드
- Firewall 마이그레이션 툴에 대한 지침 및 제한 사항 섹션의 요구 사항을 검토하고 확인합니다.
- 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 설정을 참고하십시오.
- 대규모 컨피그레이션 파일을 마이그레이션하려는 경우 마이그레이션 푸시 중에 시스템이 절전 모드로 전환되지 않도록 절전 설정을 구성합니다.

단계 **1** 컴퓨터에서 Firewall 마이그레이션 툴을 다운로드한 폴더로 이동합니다.

단계 **2** 다음 중 하나를 수행합니다.

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

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

  Firewall 마이그레이션 툴은 log 및 resources 폴더를 포함하여 해당 파일이 있는 폴더에 모든 관련 파일을 생성하고 저장합니다.

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

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

Firewall 마이그레이션 툴은 log 및 resources 폴더를 포함하여 해당 파일이 있는 폴더에 모든 관련 파일을 생성하고 저장합니다.

팁 Firewall 마이그레이션 툴을 열려고 하면 확인된 개발자가 Firewall 마이그레이션 툴을 Apple에 등록하지 않았으므로 경고 대화 상자가 표시됩니다. 확인되지 않은 개발자로부터 애플리케이션을 여는 방법에 대한 자세한 내용은 확인되지 않은 개발자의 앱 열기를 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 Network**와 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 Firewall 마이그레이션 툴에 로그인합니다.

단계 **4** Firewall 마이그레이션 툴의 로그인 페이지에서 다음을 수행합니다.

- Cisco Success Network와 통계를 공유하려면 **Login with CCO(CCO**로 로그인**)** 링크를 클릭하여 단일 로그인 자격 증명을 사용해 Cisco.com 계정에 로그인합니다.

  참고 Cisco.com 계정이 없는 경우 Cisco.com 로그인 페이지에서 생성합니다.

- 다음 기본 자격 증명을 사용하여 로그인합니다.
  - **Username(**사용자 이름**)**—admin
  - **Password(**비밀번호**)**—Admin123

Cisco.com 계정을 사용하여 로그인한 경우 8단계로 진행합니다.

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 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** **Software Update Check(**소프트웨어 업데이트 확인**)** 화면에서, Firewall 마이그레이션 툴의 최신 버전을 실행하고 있는지 확실하지 않은 경우 Cisco.com에서 버전을 확인하는 링크를 클릭합니다.

단계 **11** **Proceed(**진행**)**를 클릭합니다.

다음에 수행할 작업

다음 단계로 진행할 수 있습니다.

- Firewall 마이그레이션 툴을 사용하여 Fortinet 방화벽에서 정보를 추출해야 하는 경우 Fortinet 방화벽에서 컨피그레이션 내보내기로 진행합니다.

# Fortinet 방화벽에서 컨피그레이션 내보내기

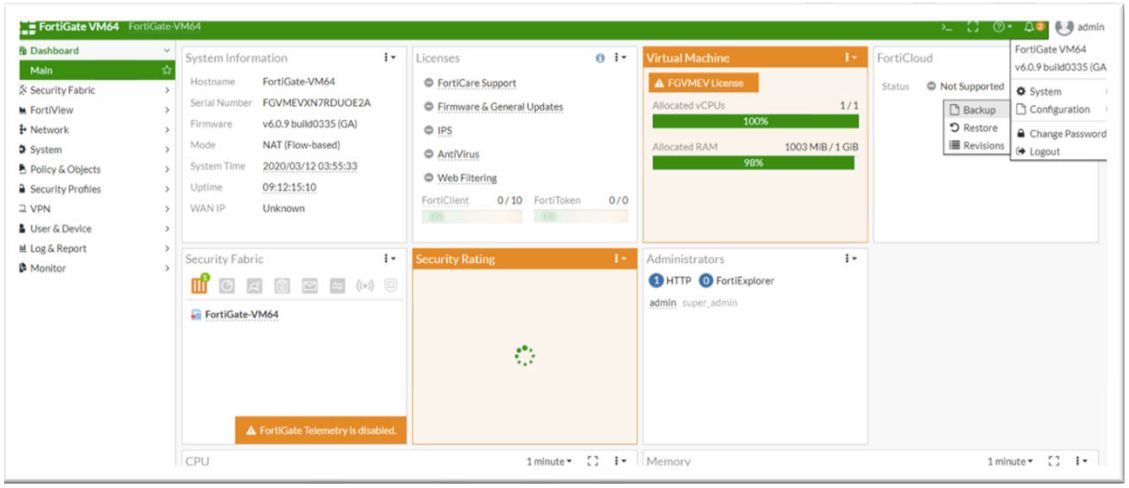
다음과 같은 방법으로 Fortinet 방화벽 컨피그레이션을 내보낼 수 있습니다.

- Fortinet 방화벽 GUI에서 Fortinet 방화벽 컨피그레이션 내보내기
- FortiManager에서 Fortinet 방화벽 컨피그레이션 내보내기

## Fortinet 방화벽 GUI에서 Fortinet 방화벽 컨피그레이션 내보내기

Fortinet 방화벽 GUI에서 컨피그레이션을 추출하려면 다음 단계를 수행합니다.

단계 **1** FortiGate VM64 GUI에서 **Admin(**관리**)** > **Configuration(**컨피그레이션**)** > **Backup(**백업**)**을 선택합니다.




단계 **2** 백업을 로컬 PC 또는 USB 디스크로 전송합니다.

참고 VDOM이 활성화된 경우 백업 범위가 전체 FortiGate 컨피그레이션(Global(전역))인지 아니면 특정 VDOM 컨피그레이션(VDOM)인지를 지정합니다.

단계 **3** 백업이 VDOM 컨피그레이션인 경우 **VDOM** 목록에서 VDOM 이름을 선택합니다.

참고 Firewall 마이그레이션 툴에서 백업 프로세스를 진행하려면 암호화되지 않은 파일이 필요합니다.

단계 **4** **OK(**확인**)**를 선택합니다.

컨피그레이션 파일을 저장할 위치를 묻는 메시지가 웹 브라우저에 표시됩니다.

컨피그레이션 파일의 확장명은 **.conf**입니다.

다음에 수행할 작업

Fortinet 컨피그레이션 파일 업로드

# FortiManager에서 Fortinet 방화벽 컨피그레이션 내보내기

FortiManager에서 관련 디바이스 컨피그레이션을 추출할 수 있습니다.

단계 **1** FortiManager에 로그인합니다.

단계 **2** 백업을 실행할 정확한 Fortigate 디바이스를 찾습니다.

단계 **3** **Configuration and Installation Status(**컨피그레이션 및 설치 상태**)**에서 **Total Revision(**총 수정**)** 옆의 아이콘을 선택하여 최신 수정 버전을 가져옵니다.

단계 **4** **Download(**다운로드**)**를 클릭하여 컨피그레이션 파일을 다운로드합니다.

다운로드한 파일은 확장명이 .conf인 파일 형식입니다.

다음에 수행할 작업

Fortinet 컨피그레이션 파일 업로드

# Fortinet 컨피그레이션 파일 업로드

시작하기 전에

소스 Fortinet 디바이스에서 컨피그레이션 파일을 `.conf` 또는 `.txt`로 내보냅니다.

참고 직접 코딩하거나 수동으로 변경한 컨피그레이션 파일을 업로드하지 마십시오. 텍스트 편집기에서 파일에 빈 라인 또는 기타 문제가 추가되어 마이그레이션이 실패할 수 있습니다.

단계 **1** Firewall Migration Tool이 컨피그레이션 파일을 업로드합니다. 대규모 컨피그레이션 파일의 경우 이 단계는 시간이 더 오래 걸립니다. 콘솔에서는 구문 분석 중인 Fortinet 컨피그레이션 라인을 포함하여 진행 상황의 라인별 로그 보기를 제공합니다. 콘솔이 표시되지 않는 경우 Firewall Migration Tool뒤의 별도 창에서 콘솔을 찾을 수 있습니다. **Context Selection(**컨텍스트 선택**)** 섹션에는 업로드된 컨피그레이션이 멀티 컨텍스트 Fortinet에 해당하는지 여부가 나와 있습니다.

단계 2 **Context Selection(**컨텍스트 선택**)** 섹션을 검토하고 마이그레이션할 Fortinet VDOM을 선택합니다.

단계 3 **Parsed Summary(**구문 분석 요약**)** 섹션에 구문 분석 상태가 표시됩니다.

단계 4 업로드된 컨피그레이션 파일에서 Firewall Migration Tool이 감지하고 구문 분석한 요소에 대한 요약을 검토합니다.

단계 5 **Next(**다음**)**를 클릭하여 대상 매개변수를 선택합니다.

---

다음에 수행할 작업

Firewall 마이그레이션 툴의 대상 매개변수 지정, 6 페이지

# Firewall 마이그레이션 툴의 대상 매개변수 지정

시작하기 전에

- 온프레미스 FMC에 대한 management center의 IP 주소를 가져옵니다.
- (선택 사항) 인터페이스 및 경로와 같은 디바이스별 컨피그레이션을 마이그레이션하려는 경우 management center에 대상 위협 방어 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 management center에서 정책을 생성하는 것이 매우 권장됩니다. Firewall 마이그레이션 툴이 연결된 management center에서 정책을 가져오므로 동일한 정책을 사용합니다. 새 정책을 생성하고 여러 액세스 제어 목록에 할당하면 성능이 저하될 수 있으며 푸시가 실패할 수도 있습니다.

---

단계 1 **Domain(**도메인**)** 드롭다운 목록에서 마이그레이션할 도메인을 선택합니다.

위협 방어 디바이스로 마이그레이션하려는 경우 선택한 도메인에서 사용 가능한 위협 방어 디바이스로만 마이그레이션할 수 있습니다.

단계 2 **Connect(**연결**)**를 클릭합니다.

단계 3 **Firewall Management Center Login(Firewall Management Center** 로그인**)** 대화 상자에서 Firepower 마이그레이션 툴 전용 계정의 사용자 이름과 비밀번호를 입력하고 **Login(**로그인**)**을 클릭합니다.

Firewall 마이그레이션 툴이 management center에 로그인하여 해당 management center에서 관리되는 위협 방어 디바이스 목록을 검색합니다. 콘솔에서 이 단계의 진행 상황을 볼 수 있습니다.

단계 4 **Proceed(**진행**)**를 클릭합니다.

단계 5 **Choose Threat Defense(**위협 방어 선택**)** 섹션에서 다음 중 하나를 수행합니다.

- **Select Firewall Threat Defense Device(Firewall Threat Defense** 디바이스 선택**)** 드롭다운 목록을 클릭하고 Fortinet 컨피그레이션을 마이그레이션할 디바이스를 선택합니다.

  선택한 management center 도메인의 디바이스가 **IP Address(IP** 주소**)** 및 **Name(**이름**)**별로 나열됩니다.

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

원격 구축이 활성화된 상태에서 management center 또는 위협 방어 6.7 이상으로의 Fortinet 방화벽 마이그레이션은 Firewall 마이그레이션 툴에서 지원됩니다. 하지만 인터페이스와 경로는 수동으로 마이그레이션해야 합니다.

- 컨피그레이션을 management center로 마이그레이션하려면 **Proceed without Threat Defense(Threat Defense** 없이 진행**)**를 클릭합니다.

  위협 방어 없이 진행하면 Firewall 마이그레이션 툴이 위협 방어에 컨피그레이션 또는 정책을 푸시하지 않습니다. 따라서 위협 방어 디바이스별 컨피그레이션인 인터페이스 및 경로, 사이트 대 사이트 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 위협 방어 없이도 마이그레이션할 수 있습니다.

단계 **6** **Proceed(**진행**)**를 클릭합니다.

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

단계 **7** **Select Features(**기능 선택**)** 섹션을 클릭하여 대상으로 마이그레이션할 기능을 검토하고 선택합니다.

- 대상 위협 방어 디바이스로 마이그레이션하는 경우 Firewall 마이그레이션 툴이 **Device Configuration(**디바이스 컨피그레이션**)** 및 **Shared Configuration(**공유 컨피그레이션**)** 섹션의 Fortinet 컨피그레이션에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.
- management center로 마이그레이션하는 경우 Firewall 마이그레이션 툴이 **Shared Configuration(**공유 컨피그레이션**)** 섹션의 Fortinet 컨피그레이션에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.

  참고 마이그레이션할 대상 위협 방어 디바이스를 선택하지 않은 경우 **Device Configuration(**디바이스 컨피그레이션**)** 섹션을 사용할 수 없습니다.

- Firewall 마이그레이션 툴은 마이그레이션 중에 ACL에 대한 대상 영역의 매핑을 활성화하는 대상 보안 영역을 지원합니다.

  소스 및 대상 네트워크 개체 또는 그룹과 서비스 개체 또는 그룹의 특성에 따라 이 작업으로 인해 Fortinet에서 management center로 마이그레이션할 때 ACL 규칙이 급증할 수 있습니다.

- Firewall 마이그레이션 툴은 대상 관리 센터가 7.2 이상인 경우 원격 액세스 VPN의 마이그레이션을 지원합니다. 원격 액세스 VPN은 위협 방어 없이도 마이그레이션할 수 있는 공유 정책입니다. 위협 방어 플로우를 사용하여 마이그레이션을 선택한 경우 위협 방어 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 Fortinet 컨피그레이션에서 참조되지 않는 개체는 마이그레이션되지 않습니다. 이렇게 하면 마이그레이션 시간이 최적화되고 컨피그레이션에서 사용되지 않는 개체가 제거됩니다.

단계 **8** **Proceed(**진행**)**를 클릭합니다.

단계 **9** **Rule Conversion/ Process Config(**규칙 변환/프로세스 컨피그레이션**)** 섹션에서 **Start Conversion(**변환 시작**)**을 클릭하여 변환을 시작합니다.

단계 **10** Firewall 마이그레이션 툴에서 변환한 요소의 요약을 검토합니다.

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

단계 **11** **Download Report(**보고서 다운로드**)**를 클릭하고 **Pre-Migration Report(**마이그레이션 전 보고서**)**를 저장합니다.

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

---

다음에 수행할 작업

마이그레이션 전 보고서 검토, 8 페이지

# 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 Firewall Migration Tool이 실행 중일 때만 보고서를 다운로드할 수 있습니다.

---

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

**Pre-Migration Report(**마이그레이션 전 보고서**)**의 사본도 Firewall Migration Tool과 동일한 위치의 `Resources` 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.

- 위협 방어로 성공적으로 마이그레이션할 수 있는 지원되는 Fortinet 컨피그레이션 요소 및 마이그레이션을 위해 선택한 특정 Fortinet 기능의 요약입니다.

- **Configuration Lines with Errors(**오류가 있는 컨피그레이션 라인**)** - Firewall Migration Tool이 구문 분석 할 수 없으므로 마이그레이션할 수 없는 Fortinet 컨피그레이션 요소에 대한 세부 정보입니다. 계속 진행하기 전에 Fortinet 컨피그레이션에서 이러한 오류를 해결하고 새 컨피그레이션 파일을 내보낸 다음 Firewall Migration Tool에 새 컨피그레이션 파일을 업로드합니다.
- **Partially Supported Configuration(**부분적으로 지원되는 컨피그레이션**)** - 부분적으로만 마이그레이션할 수 있는 Fortinet 컨피그레이션 요소에 대한 세부 정보입니다. 이러한 컨피그레이션 요소에는 고급 옵션이 있는 규칙 및 개체가 포함되는데, 이 경우 고급 옵션 없이 규칙 또는 개체를 마이그레이션할 수 있습니다. 이러한 라인을 검토하고 management center에서 고급 옵션이 지원되는지 확인한 다음, 지원되는 경우 Firewall Migration Tool을 사용하여 마이그레이션을 완료한 후 해당 옵션을 수동으로 구성하도록 계획합니다.
- **Unsupported Configuration(**지원되지 않는 컨피그레이션**)** - Firewall Migration Tool이 해당 기능의 마이그레이션을 지원하지 않으므로 마이그레이션할 수 없는 Fortinet 컨피그레이션 요소에 대한 세부 정보입니다. 이러한 라인을 검토하고 management center에서 각 기능이 지원되는지 확인한 다음, 지원되는 경우 Firewall Migration Tool을 사용하여 마이그레이션을 완료한 후 해당 기능을 수동으로 구성하도록 계획합니다.
- **Ignored Configuration(**무시된 컨피그레이션**)** - management center 또는 Firewall Migration Tool에서 지원되지 않기 때문에 무시되는 FPS 구성 요소를 사용하는 Fortinet의 세부 정보입니다. Firewall Migration Tool는 이러한 행을 구문 분석하지 않습니다. 이러한 라인을 검토하고 management center에서 각 기능이 지원되는지 확인한 다음, 지원되는 경우 해당 기능을 수동으로 구성하도록 계획합니다.

management center 및 위협 방어에서 지원되는 기능에 대한 자세한 내용은 Management Center 컨피그레이션 가이드를 참고하십시오.

단계 **3** **Pre-Migration Report(**마이그레이션 전 보고서**)**에서 시정 조치를 권장하는 경우, 계속하기 전에 인터페이스 Fortinet에서 해당 시정 조치를 완료하고 Fortinet 컨피그레이션 파일을 다시 내보낸 후 업데이트된 컨피그레이션 파일을 업로드하십시오.

단계 **4** Fortinet 컨피그레이션 파일이 성공적으로 업로드되고 구문 분석된 후 Firewall Migration Tool로 돌아가 **Next(**다음**)**를 클릭하여 마이그레이션을 계속합니다.

---

다음에 수행할 작업

Fortinet 컨피그레이션을 Secure Firewall Device ManagerThreat Defense 인터페이스와 매핑

# Fortinet 컨피그레이션을 Secure Firewall Device ManagerThreat Defense 인터페이스와 매핑

위협 방어 디바이스에는 Fortinet 컨피그레이션에 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.

**Map Threat Defense Interface(Threat Defense** 인터페이스 매핑**)** 화면에서 Firewall 마이그레이션 툴로 위협 방어 디바이스의 인터페이스 목록을 검색합니다. 기본적으로 Firewall 마이그레이션 툴은 인터페이스 ID에 따라 Fortinet의 인터페이스와 위협 방어 디바이스를 매핑합니다.

위협 방어 인터페이스에 대한 Fortinet 인터페이스 매핑은 위협 방어디바이스 유형에 따라 달라집니다.

- 대상 위협 방어가 네이티브 유형인 경우:
  - 위협 방어에서 같거나 더 많은 수의 Fortinet 인터페이스 또는 PC(Port Channel) 데이터 인터페이스( Fortinet 컨피그레이션의 관리 전용 및 하위 인터페이스 제외)를 사용해야 합니다. 이 수가 더 적은 경우 대상 위협 방어에 필요한 인터페이스 유형을 추가합니다.
  - 하위 인터페이스는 물리적 인터페이스 또는 포트 채널 매핑을 기반으로 Firewall 마이그레이션 툴에서 생성됩니다.
- 대상 위협 방어가 컨테이너 유형인 경우:
  - 위협 방어에서 같거나 더 많은 수의 Fortinet인터페이스, 물리적 하위 인터페이스, 포트 채널 또는 포트 채널 하위 인터페이스(Fortinet컨피그레이션의 관리 전용 인터페이스 제외)를 사용해야 합니다. 이 수가 더 적은 경우 대상 위협 방어에 필요한 인터페이스 유형을 추가합니다. 예를 들어, 대상 위협 방어의 물리적 인터페이스 및 물리적 하위 인터페이스 수가 Fortinet보다 100개 적을 경우 대상 위협 방어에서 추가 물리적 인터페이스 또는 물리적 하위 인터페이스를 생성할 수 있습니다.
  - 하위 인터페이스는 Firewall 마이그레이션 툴로 생성되지 않습니다. 물리적 인터페이스, 포트 채널 또는 하위 인터페이스 간의 인터페이스 매핑만 허용됩니다.

시작하기 전에

management center에 연결하고 대상을 위협 방어로 선택했는지 확인합니다. 자세한 내용은 Firewall 마이그레이션 툴의 대상 매개변수 지정, 6 페이지를 참고하십시오.

참고 이 단계는 위협 방어 디바이스 없이 management center로 마이그레이션하는 경우 적용되지 않습니다.

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

관리 인터페이스의 매핑은 변경할 수 없습니다. 위협 방어 인터페이스가 Fortinet 인터페이스에 이미 할당된 경우 드롭다운 목록에서 해당 인터페이스를 선택할 수 없습니다. 할당된 모든 인터페이스는 회색으로 표시되며 사용할 수 없습니다.

하위 인터페이스는 매핑할 필요가 없습니다. Firewall 마이그레이션 툴은 Fortinet 컨피그레이션의 모든 하위 인터페이스에 대해 위협 방어 디바이스의 하위 인터페이스를 매핑합니다.

단계 **2** 각 Fortinet인터페이스를 위협 방어 인터페이스에 매핑했으면 **Next(**다음**)**를 클릭합니다.

다음에 수행할 작업

Fortinet 인터페이스를 적절한 위협 방어 인터페이스 개체, 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 내용은 보안 영역 에 Fortinet 인터페이스 매핑을 참고하십시오.

# 보안 영역 에 **Fortinet** 인터페이스 매핑

Fortinet 컨피그레이션이 올바르게 마이그레이션되도록 하려면 Fortinet 인터페이스를 적절한 위협 방어 인터페이스 개체, 보안 영역 및 인터페이스 그룹에 매핑합니다. Fortinet 컨피그레이션에서 액세스 제어 정책 및 NAT 정책은 인터페이스 이름(nameif)을 사용합니다. management center에서 이러한 정책은 인터페이스 개체를 사용합니다. 또한 management center 정책은 인터페이스 개체를 다음과 같이 그룹화합니다.

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

Firewall Migration Tool을 사용하면 보안 영역이 있는 인터페이스를 일대일로 매핑할 수 있습니다. 보안 영역 이 인터페이스에 매핑된 경우 management center에서 허용하더라도 다른 인터페이스에 매핑될 수 없습니다. management center의 보안 영역에 대한 자세한 내용은 보안 영역을 참고하십시오.

---

단계 **1** management center에 존재하는, 즉 컨피그레이션 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 **2** management center에 존재하는 보안 영역에 인터페이스를 매핑하려면 **Security Zones(**보안 영역**)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.

단계 **3** 보안 영역을 수동으로 매핑하거나 자동으로 생성할 수 있습니다.

보안 영역을 수동으로 매핑하려면 다음과 같이 합니다.

a) **Add SZ(SZ** 추가**)**를 클릭합니다.
b) **Add SZ(SZ** 추가**)** 대화 상자에서 **Add(**추가**)**를 클릭하여 새 보안 영역을 추가합니다.
c) **Security Zone(**보안 영역**)** 열에 보안 영역 이름을 입력합니다. 허용되는 최대 문자 수는 48자입니다.
d) **Close(**닫기**)**를 클릭합니다.

자동 생성을 통해 보안 영역을 매핑하려면 다음과 같이 합니다.

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

**Auto-Create(**자동 생성**)**를 클릭하면 소스 방화벽 영역이 자동으로 매핑됩니다. 동일한 이름 영역이 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 **4** 모든 인터페이스를 적절한 보안 영역에 매핑했으면 **Next(**다음**)**를 클릭합니다.

---

# 최적화,마이그레이션할 컨피그레이션 검토 및 검증

마이그레이션된 Fortinet 컨피그레이션을 management center로 푸시하기 전에 컨피그레이션을 최적화하고 신중하게 검토하여 해당 컨피그레이션이 올바르며 위협 방어 디바이스 구성 방법과 일치하는지 확인하십시오. 깜박이는 탭은 다음 작업 과정을 수행해야 함을 나타냅니다.

여기서 Firewall Migration Tool은 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(**컨피그레이션 최적화**,** 검토 및 검증**)** 화면에서 Firewall Migration Tool을 닫으면 진행 상황이 저장되고 나중에 마이그레이션을 재개할 수 있습니다. 이 화면 전에 Firewall Migration Tool을 닫으면 진행 상황이 저장되지 않습니다. 구문 분석 후 오류가 발생한 경우 Firewall Migration Tool을 다시 실행하면 **Interface Mapping(**인터페이스 매핑**)** 화면에서 재개됩니다.

**Firewall Migration Tool ACL** 최적화 개요

Firewall Migration Tool는 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.
- 섀도우 ACL - 첫 번째 ACL은 두 번째 ACL의 컨피그레이션을 완전히 섀도잉합니다. 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, 섀도잉된 규

칙을 이동하거나 규칙 중 하나를 편집하여 필요한 정책을 구현할 수 있습니다. 예를 들어 기본 규칙은 IP 트래픽을 거부할 수 있으며, 섀도잉된 규칙은 지정된 소스 또는 대상에 대한 FTP 트래픽을 허용할 수 있습니다.

Firewall Migration Tool는 ACL 최적화를 위한 규칙을 비교하는 동안 다음 매개변수를 사용합니다.

참고 최적화는 Fortinet ACP 규칙 작업에만 사용할 수 있습니다.

- 비활성화된 ACL은 최적화 프로세스 중에 고려되지 않습니다.
- 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

개체 최적화

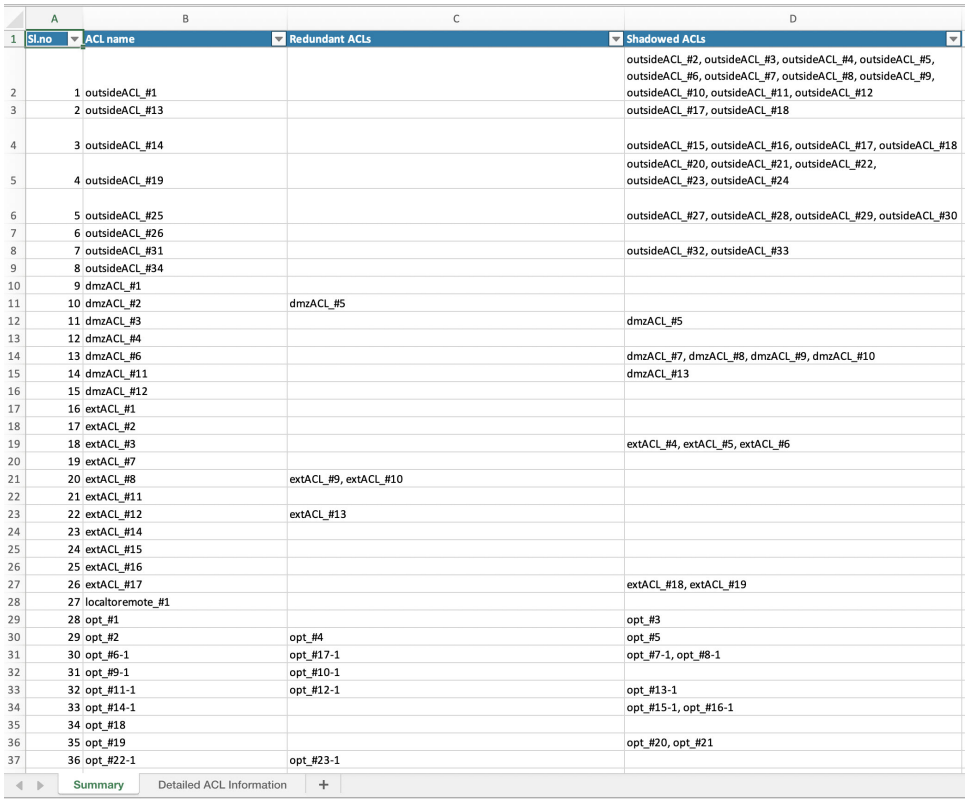
마이그레이션 프로세스 중에 개체 최적화를 위해 다음 개체가 고려됩니다.

- 참조되지 않은 개체 - 마이그레이션을 시작할 때 참조되지 않은 개체를 마이그레이션하지 않도록 선택할 수 있습니다.
- 중복 개체 - 개체가 이미 management center에 있는 경우 중복 개체를 생성하는 대신 정책이 재사용됩니다.
- 일치하지 않는 개체 - 이름은 비슷하지만 콘텐츠가 다른 개체가 있는 경우 마이그레이션 푸시 전에 Firewall Migration Tool에서 개체 이름을 수정합니다.

# ACL 최적화 보고

ACL 최적화 보고서에는 다음 정보가 표시됩니다.

- 요약 시트 - ACL 최적화의 요약을 표시합니다.



| | A | B | C | D |
|---|---|---|---|---|
| 1 | Sl.no | ACL name | Redundant ACLs | Shadowed ACLs |
| 2 | 1 | outsideACL_#1 | | outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12 |
| 3 | 2 | outsideACL_#13 | | outsideACL_#17, outsideACL_#18 |
| 4 | 3 | outsideACL_#14 | | outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18 |
| 5 | 4 | outsideACL_#19 | | outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24 |
| 6 | 5 | outsideACL_#25 | | outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30 |
| 7 | 6 | outsideACL_#26 | | |
| 8 | 7 | outsideACL_#31 | | outsideACL_#32, outsideACL_#33 |
| 9 | 8 | outsideACL_#34 | | |
| 10 | 9 | dmzACL_#1 | | |
| 11 | 10 | dmzACL_#2 | dmzACL_#5 | |
| 12 | 11 | dmzACL_#3 | | dmzACL_#5 |
| 13 | 12 | dmzACL_#4 | | |
| 14 | 13 | dmzACL_#6 | | dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10 |
| 15 | 14 | dmzACL_#11 | | dmzACL_#13 |
| 16 | 15 | dmzACL_#12 | | |
| 17 | 16 | extACL_#1 | | |
| 18 | 17 | extACL_#2 | | |
| 19 | 18 | extACL_#3 | | extACL_#4, extACL_#5, extACL_#6 |
| 20 | 19 | extACL_#7 | | |
| 21 | 20 | extACL_#8 | extACL_#9, extACL_#10 | |
| 22 | 21 | extACL_#11 | | |
| 23 | 22 | extACL_#12 | extACL_#13 | |
| 24 | 23 | extACL_#14 | | |
| 25 | 24 | extACL_#15 | | |
| 26 | 25 | extACL_#16 | | |
| 27 | 26 | extACL_#17 | | extACL_#18, extACL_#19 |
| 28 | 27 | localtoremote_#1 | | |
| 29 | 28 | opt_#1 | | opt_#3 |
| 30 | 29 | opt_#2 | opt_#4 | opt_#5 |
| 31 | 30 | opt_#6-1 | opt_#17-1 | opt_#7-1, opt_#8-1 |
| 32 | 31 | opt_#9-1 | opt_#10-1 | |
| 33 | 32 | opt_#11-1 | opt_#12-1 | opt_#13-1 |
| 34 | 33 | opt_#14-1 | | opt_#15-1, opt_#16-1 |
| 35 | 34 | opt_#18 | | |
| 36 | 35 | opt_#19 | | opt_#20, opt_#21 |
| 37 | 36 | opt_#22-1 | opt_#23-1 | |

Summary | Detailed ACL Information | +

- 상세 ACL 정보 - 기본 ACL의 상세 정보를 표시합니다. 각 ACL에는 비교 및 최적화 카테고리와의 연결 여부를 보여주어 기본 ACL을 식별하기 위한 ACL 유형(섀도우 또는 중복) 태그가 제공됩니다.

| 1 | Sl.no | ACL name | Source zone | Destination zone | Source network | Destination network | Source port | Destination port | Action | ACL type |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | **1** | **outsideACL_#1** | **outside** | **ANY** | **any** | **10.0.0.0/8** | **ANY** | **ANY** | **permit** | |
| 3 | | outsideACL_#2 | outside | ANY | any | 10.0.0.0/24 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 4 | | outsideACL_#3 | outside | ANY | 192.168.0.1 | 10.0.0.0/24 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 5 | | outsideACL_#4 | outside | ANY | 192.168.0.10 | 10.0.0.0/24 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 6 | | outsideACL_#5 | outside | ANY | any | 10.1.1.0/24 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 7 | | outsideACL_#6 | outside | ANY | any | 10.1.1.0/24 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 8 | | outsideACL_#7 | outside | ANY | any | 10.1.1.0/24 | ANY | tcp:80 | permit | Shadowed by outsideACL_#1 |
| 9 | | outsideACL_#8 | outside | ANY | any | 10.10.10.10, 10.10.0.0/16 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 10 | | outsideACL_#9 | outside | ANY | 200.200.200.1 | 10.10.10.10, 10.10.0.0/16 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 11 | | outsideACL_#10 | outside | ANY | 10.10.10.10, 10.10.0.0/16 | 10.10.0.0/19, 10.99.99.99 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 12 | | outsideACL_#11 | outside | ANY | any | 10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 13 | | outsideACL_#12 | outside | ANY | any | 10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/19 | ANY | ANY | permit | Shadowed by outsideACL_#1 |
| 14 | **2** | **outsideACL_#13** | **outside** | **ANY** | **any** | **192.168.0.0/16** | **ANY** | **ANY** | **permit** | |
| 15 | | outsideACL_#17 | outside | ANY | 10.10.1.1 | 192.168.0.0/16 | ANY | tcp:443 | permit | Shadowed by outsideACL_#13 |
| 16 | | outsideACL_#18 | outside | ANY | 10.10.1.1 | 192.168.0.0/16 | ANY | tcp:80 | permit | Shadowed by outsideACL_#13 |

# 마이그레이션된 컨피그레이션을 **Secure Firewall Management Center**에 푸시

컨피그레이션을 성공적으로 검증하고 모든 개체 충돌을 해결하지 않은 경우 마이그레이션된 ASA Fortinet 컨피그레이션을 Secure Firewall Management Center에 푸시할 수 없습니다.

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

참고 Firewall Migration Tool이 마이그레이션된 컨피그레이션을 Secure Firewall Management Center에 보내는 동안에는 컨피그레이션을 변경하거나 디바이스에 구축하지 마십시오.

단계 **1** **Validation Status(**검증 상태**)** 대화 상자에서 검증 요약을 검토합니다.

단계 **2** **Push Configuration(**컨피그레이션 푸시**)**을 클릭하여 마이그레이션된 ASA Fortinet컨피그레이션을 Secure Firewall Management Center에 보냅니다.

Firewall Migration Tool에 마이그레이션 진행 상황의 요약이 표시됩니다. 콘솔에서 Secure Firewall Management Center에 푸시되는 구성 요소의 세부적인 라인별 진행 상황을 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 Firewall Migration Tool과 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 언제라도 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,마이그레이션할 컨피그레이션 검토 및 검증, 12 페이지을 참조해 주십시오.

개체를 검토하고 확인합니다.

- 카테고리
  - 총 ACL 규칙(소스 컨피그레이션)
  - 최적화를 위해 고려된 총 ACL 규칙. 예를 들어, 중복, 섀도우 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 Firewall Migration Tool이 실행 중일 때만 보고서를 다운로드할 수 있습니다.

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

단계 **2** 마이그레이션 후 보고서를 열고 내용을 신중하게 검토하여 Fortinet 컨피그레이션이 어떻게 마이그레이션되었는지 파악합니다.

- **Migration Summary(**마이그레이션 요약**)** - Fortinet 인터페이스, management center 호스트 이름 및 도메인, 대상 threat defense 디바이스(적용 가능한 경우) 및 성공적으로 마이그레이션된 컨피그레이션 요소에 대한 정보를 포함하여 Fortinet에서 threat defense로 성공적으로 마이그레이션된 컨피그레이션의 요약입니다.
- **Selective Policy Migration(**선택적 정책 마이그레이션**)** - 마이그레이션하도록 선택한 특정 Fortinet 기능에 대한 세부 정보를 Device Configuration Features(디바이스 컨피그레이션 기능), Shared Configuration Features(공유 컨피그레이션 기능), Optimization(최적화)의 세 범주에서 확인할 수 있습니다.

- **FortinetInterface to Threat Defense Interface Mapping**(인터페이스 대 Threat Defense인터페이스 매핑) - 성공적으로 마이그레이션된 인터페이스 및 Fortinet 컨피그레이션의 인터페이스를 threat defense 디바이스의 인터페이스에 매핑한 방법에 대한 세부 정보입니다. 이러한 매핑이 예상과 일치하는지 확인합니다.

  참고 이 섹션은 마이그레이션에 대상 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 Fortinet 논리적 인터페이스 및 이름과 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**)** - management center의 기존 개체와 충돌하는 것으로 확인된 Fortinet 개체에 대한 세부 정보입니다. 개체의 이름과 컨피그레이션이 동일한 경우 Firewall Migration Tool에서 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**)** - Firewall Migration Tool을 사용하여 마이그레이션하지 않도록 선택한 규칙에 대한 세부 정보입니다. Firewall Migration Tool에서 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 컨피그레이션**)** - 고급 옵션이 포함되어 있지만 고급 옵션 없이 마이그레이션될 수 있는 규칙을 비롯하여 부분적으로만 마이그레이션된 Fortinet 규칙에 대한 세부 정보입니다. 이러한 라인을 검토하고 management center에서 고급 옵션이 지원되는지 확인한 다음 지원되는 경우 해당 옵션을 수동으로 구성합니다.

- **Unsupported Configuration(**지원되지 않는 컨피그레이션**)** - Firewall Migration Tool이 해당 기능의 마이그레이션을 지원하지 않으므로 마이그레이션할 수 없는 Fortinet 컨피그레이션 요소에 대한 세부 정보입니다. 이러한 라인을 검토하여 각 기능이 threat defense에서 지원되는지 확인합니다. 지원되는 경우 management center에서 해당 기능을 수동으로 구성합니다.

- **Expanded Access Control Policy Rules(**확장 액세스 제어 정책 규칙**)** - 마이그레이션 중에 단일 Fortinet 포인트 규칙에서 여러 threat defense 규칙으로 확장된 Fortinet 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**)**- Firewall Migration Tool을 사용하여 마이그레이션하지 않도록 선택한 Fortinet액세스 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**)** - Firewall Migration Tool을 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 Fortinet 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 threat defense에서 해당 기능이 지원되는지 확인합니다.
- **Access Control Rules that have File Policy Applied(**파일 정책이 적용된 액세스 제어 규칙**)** - 파일 정책이 적용된 모든 Fortinet 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 threat defense에서 해당 기능이 지원되는지 확인합니다.
- **Access Control Rules that have Rule 'Log' Setting Change(**규칙 '로그' 설정이 변경된 액세스 제어 규칙**)** - Firewall Migration Tool을 사용하여 '로그 설정'이 변경된 Fortinet 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.

참고 마이그레이션되지 않은 지원되지 않는 규칙은 원치 않는 트래픽이 방화벽을 통과하는 문제를 일으킵니다. 이 트래픽이 threat defense에서 차단되도록 management center에서 규칙을 구성하는 것이 좋습니다.

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

management center 및 threat defense에서 지원되는 기능에 대한 자세한 내용은 Management Center 컨피그레이션 가이드, 버전 6.2.3을 참고하십시오.

단계 **3** **Pre-Migration Report(**마이그레이션 전 보고서**)**를 열고 threat defense 디바이스에서 수동으로 마이그레이션해야 하는 Fortinet 컨피그레이션 항목을 기록해 둡니다.

단계 **4** management center에서 다음과 같이 합니다.

a) 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
- Interfaces
- 동적 경로 개체

b) 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 가이드를 참고하십시오. 다음은 수동 구성이 필요한 컨피그레이션 항목의 예입니다.

- Threat Defense의 플랫폼 설정에 설명된 SSH 및 HTTPS 액세스를 포함한 플랫폼 설정

- 시스템 로그 구성에 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 management center에서 threat defense 디바이스로 구축합니다.

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

Firewall Migration Tool는 threat defense 디바이스에 정책을 할당합니다. 변경 사항이 실행 중인 컨피그레이션에 반영되어 있는지 확인합니다. 마이그레이션되는 정책을 쉽게 식별할 수 있도록 해당 정책의 설명에 Fortinet 컨피그레이션의 호스트 이름이 포함되어 있습니다.

# Firewall 마이그레이션 툴 제거

모든 구성 요소는 Firewall 마이그레이션 툴과 같은 폴더에 저장됩니다.

단계 **1** 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** Firewall 마이그레이션 툴을 배치한 폴더를 삭제합니다.

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