



Secure Firewall 마이그레이션 툴 시작하기

- [Secure Firewall 마이그레이션 툴 정보, 1 페이지](#)
- [Secure Firewall 마이그레이션 툴 최신 기능, 4 페이지](#)
- [Secure Firewall 마이그레이션 툴 라이선싱, 23 페이지](#)
- [Secure Firewall 마이그레이션 툴의 플랫폼 요구 사항, 23 페이지](#)
- [Threat Defense 디바이스의 요구 사항 및 사전 요건, 24 페이지](#)
- [Check Point 구성 지원, 25 페이지](#)
- [지침 및 제한 사항, 28 페이지](#)
- [마이그레이션에 지원되는 플랫폼, 31 페이지](#)
- [마이그레이션에 지원되는 대상 Management Center, 33 페이지](#)
- [마이그레이션에 지원되는 소프트웨어 버전, 34 페이지](#)

Secure Firewall 마이그레이션 툴 정보

이 설명서에 포함된 샘플 마이그레이션 절차([샘플 마이그레이션: Check Point-Threat defense 2100](#))를 참조하면 마이그레이션 프로세스를 쉽게 이해할 수 있습니다.

Secure Firewall 마이그레이션 툴은 지원되는 Check Point 구성을 지원되는 Secure Firewall Threat Defense 플랫폼으로 전환합니다. Secure Firewall 마이그레이션 툴을 사용하면 지원되는 Check Point 기능 및 정책을 Firewall Threat Defense로 자동 마이그레이션할 수 있습니다.



참고 마이그레이션 전 보고서에서 무시된 구성 항목이 있는지 확인하고, 해당 항목이 있는 경우 마이그레이션 후 수동으로 구성해야 합니다.

Secure Firewall 마이그레이션 툴은 Check Point 정보를 수집하고 구문 분석한 다음 Secure Firewall Management Center에 푸시합니다. 구문 분석 단계에서 Secure Firewall 마이그레이션 툴은 다음을 식별하는 마이그레이션 전 보고서를 생성합니다.

- 오류가 있는 Check Point 컨피그레이션 XML 또는 JSON 라인

- Check Point는 Secure Firewall 마이그레이션 툴이 인식할 수 없는 Check Point XML 또는 JSON 라인을 나열합니다. **Pre-Migration Report**(마이그레이션 전 보고서) 및 콘솔 로그의 오류 섹션 아래 XML 또는 JSON 컨피그레이션 라인을 보고합니다. 이로 인해 마이그레이션이 차단됩니다.

구문 분석 오류가 있는 경우 문제를 해결하고, 새 구성을 다시 업로드하고, 대상 디바이스에 연결하고, Check Point 인터페이스를 Firewall Threat Defense 인터페이스에 매핑하고, 보안 영역 및 인터페이스 그룹을 매핑하고, 구성을 검토하고 검증할 수 있습니다. 그런 다음 컨피그레이션을 대상 디바이스로 마이그레이션할 수 있습니다.

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, Check Point 구성 및 **resources**(리소스) 폴더에 있는 로그의 사본을 저장합니다.

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

구문 분석되지 않은 파일

Secure Firewall 마이그레이션 툴은 구문 분석되지 않은 파일에서 무시한 구성 라인에 대한 정보를 기록합니다. Secure Firewall 마이그레이션 툴은 Check Point 구성 파일을 구문 분석할 때 이 파일을 생성합니다.

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) 창의 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.

알림 센터

성공 메시지, 오류 메시지 및 마이그레이션 중에 표시되는 경고를 비롯한 모든 알림은 알림 센터에서 캡처되며 **Successes**(성공), **Warnings**(경고) 및 **Errors**(오류)로 분류됩니다. 마이그레이션 중에 언제든지



지 오른쪽 상단에서 아이콘을 클릭하면 팝업된 다양한 알림과 툴에서 팝업된 시간을 확인할 수 있습니다.

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 수 있는 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
10.0.2	이 패치 릴리스에는 버그 수정이 포함되어 있습니다.
10.0.1	이제 Secure Firewall 마이그레이션 툴을 사용하여 DHCP 및 DNS 구성을 마이그레이션할 수 있습니다. 지원되는 마이그레이션: Check Point 방화벽에서 Firewall Threat Defense(으)로 이 릴리스에서는 Secure Firewall 6100 시리즈 디바이스에 대한 포괄적인 마이그레이션 지원 기능이 도입되었습니다. 마이그레이션 툴은 이제 개선된 애플리케이션 매핑 화면을 제공합니다. 이 개선 사항을 통해 애플리케이션 구성을 Firewall Threat Defense(으)로 마이그레이션하는 과정이 간소화됩니다. 지원되는 마이그레이션: Check Point 방화벽에서 Firewall Threat Defense(으)로 Check Point 중견·중소 기업(SMB) 디바이스에서 Cisco Secure Firewall Threat Defense(으)로 방화벽 구성을 마이그레이션하는 지원 기능을 추가했습니다. 방화벽 마이그레이션 툴은 사전 구문 분석 단계에서 구문 분석된 요약 페이지에 속성 개수를 표시하지 않습니다. 이번 변경 사항은 내용을 더 명확하게 하고 마이그레이션 절차를 간소화합니다. 지원되는 마이그레이션: 모두 이제 Firewall Threat Defense를 실행 중인 Cisco Adaptive Security Appliance(ASA) 55XX-X 시리즈 디바이스에서 Cisco Firewall 1000, 2000, 3000, 4000, 6000 및 9000 시리즈 디바이스와 같은 Firewall Threat Defense 디바이스로 구성을 마이그레이션할 수 있습니다.

버전	지원 기능
10.0	이 릴리스에서는 CSF200 시리즈 디바이스에 대한 포괄적인 마이그레이션 지원 기능이 도입되었습니다. 지원되는 마이그레이션: 모두
	이 릴리스로의 원활한 전환을 돕기 위해 방화벽 관리 센터 및 Firewall Threat Defense 10.0에 대한 마이그레이션 지원이 제공됩니다. 지원되는 마이그레이션: 모두
	이번 릴리스에서는 텔레메트리 기능이 대폭 개선되어, 분석 및 문제 해결을 위한 데이터 수집이 향상되었습니다. 지원되는 마이그레이션: 모두
	이번 릴리스에서는 구문 분석 성능이 대폭 향상되어 시스템의 응답 속도가 빨라지고 효율성이 높아졌습니다. 지원되는 마이그레이션: Check Point 방화벽에서 Firewall Threat Defense, Palo Alto Networks 방화벽에서 Firewall Threat Defense, ASA 방화벽에서 Firewall Threat Defense.
	사용자 경험을 개선하기 위해 이중 네트워크 주소 변환(NAT) 기능이 강화되었습니다. 참조: Check Point 구성 지원 지원되는 마이그레이션: Check Point 방화벽에서 Firewall Threat Defense(으)로
7.7.10.4	이 패치 릴리스에는 버그 수정이 포함되어 있습니다.

버전	지원 기능
7.7.10.3	이제 Secure Firewall 마이그레이션 툴은 구성을 방화벽 관리 센터에 구축할 때 중복된 개체 이름이나 값으로 인해 발생하는 충돌을 식별할 수 있습니다. 그런 다음 툴은 사용자에게 이러한 충돌을 해결하기 위해 적절한 조치를 취하도록 안내합니다. 참조: 마이그레이션된 구성을 Firewall Management Center에 푸시 지원되는 마이그레이션: 모두
	성능 향상을 위해 ACL 최적화 분석 시간이 단축되었습니다. ACL 최적화를 클릭한 후 진행을 클릭하면, 구성 최적화, 검토 및 검증 창에 ACL 최적화 분석에 소요되는 예상 시간을 표시하는 배너가 나타납니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: 모두
	이제 구성 최적화, 검토 및 검증 > ACL 최적화 창에서 비활성화된 ACL 목록을 확인할 수 있습니다. 이번 개선 사항을 통해 마이그레이션 프로세스의 효율성이 더욱 높아집니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: 모두
	마이그레이션 중 최적화 프로세스를 간소화하기 위해, Secure Firewall 마이그레이션 툴은 모든 속성이 최적화되었는지 확인하는 검사를 수행합니다. 구성 최적화, 검토 및 검증 창에서 검증을 클릭하면 누락된 모든 속성이 구성 최적화 대화 상자에 표시됩니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: 모두
7.7.10.2	이 패치 릴리스에는 버그 수정이 포함되어 있습니다.

버전	지원 기능
7.7.10.1	이 릴리스에는 다음과 같은 새로운 기능이 포함되어 있습니다. - Secure Firewall 마이그레이션 툴에는 이제 투명 모드와 라우팅 모드 방화벽 컨텍스트를 별도로 선택할 수 있는 옵션이 제공되어, 각 컨텍스트를 독립적으로 관리하고 마이그레이션할 수 있게 되었으며, 이를 통해 마이그레이션 과정에서 더 큰 유연성과 제어력을 확보할 수 있습니다. 참조: ASA 보안 컨텍스트 선택 지원되는 마이그레이션: Secure Firewall ASA - Secure Firewall 마이그레이션 툴에서는 이제 구성 최적화, 검토 및 검증 창에서 NAT 규칙의 소스 및 대상 영역을 편집할 수 있는 옵션을 제공합니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: Secure Firewall ASA - Secure Firewall 마이그레이션 툴이 이제 negate 매개변수가 포함된 액세스 제어 항목(ACE)의 마이그레이션을 지원합니다. 참조: Check Point 구성 지원 지원되는 마이그레이션: Check Point 방화벽 - Secure Firewall 마이그레이션 툴이 이제 인라인 보안 영역에 대한 인터페이스 매핑을 지원하여, 세분화된 정책 적용 및 트래픽 제어가 가능해졌습니다. 참조: 보안 영역 및 인터페이스 그룹에 PAN 인터페이스 매핑 지원되는 마이그레이션: Palo Alto Networks 방화벽 - 이제 Secure Firewall 마이그레이션 툴을 사용하여 VLAN 태그 개체 및 기타 지원되는 개체 유형을 위협 방어 디바이스로 마이그레이션할 수 있습니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: Palo Alto Networks 방화벽

버전	지원 기능
7.7.10	이 릴리스에는 다음과 같은 새로운 기능이 포함되어 있습니다. • 이제 Secure Firewall 마이그레이션 툴을 사용하여 Microsoft Azure 네이티브 방화벽의 구성을 Firewall Threat Defense(으)로 마이그레이션할 수 있습니다. 자세한 내용 및 마이그레이션 단계는 마이그레이션 툴을 사용하여 Microsoft Azure 네이티브 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션하기를 참조하십시오. • 이제 Secure Firewall 마이그레이션 툴을 사용하여 Check Point 방화벽의 구성을 Multicloud Defense(으)로 마이그레이션할 수 있습니다. 자세한 내용 및 마이그레이션 단계는 마이그레이션 툴을 사용하여 Check Point 방화벽을 Cisco Multicloud Defense로 마이그레이션하기를 참조하십시오. • 이제 Secure Firewall 마이그레이션 툴을 사용하여 Fortinet 방화벽의 구성을 Multicloud Defense(으)로 마이그레이션할 수 있습니다. 자세한 내용 및 마이그레이션 단계는 마이그레이션 툴을 사용하여 Fortinet 방화벽을 Cisco Multicloud Defense로 마이그레이션하기를 참조하십시오. • Secure Firewall 마이그레이션 툴이 이제 기존 보안 그룹 태그 개체 구성을 감지합니다. 이 감지 기능은 사용자, 디바이스 또는 시스템에 특정 태그를 연결함으로써 보안 정책 관리를 간소화하고, 동적이며 확장 가능한 액세스 제어를 가능하게 합니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: Secure Firewall ASA • 이제 구성 최적화, 검토 및 검증 페이지에서 개체나 개체 그룹을 추가, 삭제 또는 수정하여 액세스 규칙을 편집할 수 있습니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: 모두 • 사용자 경험을 개선하기 위해 마이그레이션 전/후 보고서가 개선되었습니다. 이제 각 섹션별로 CSV 파일을 다운로드하여 상세하게 분석할 수 있습니다. 마이그레이션 후 보고서에는 각 범주별로 마이그레이션 전 보고서와 마이그레이션 후 보고서의 구성 항목 수를 비교하는 비교 차트가 도입되었습니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: 모두

버전	지원 기능
7.7	이 릴리스에는 다음과 같은 새로운 기능이 포함되어 있습니다. • 이제 Secure Firewall 마이그레이션 툴을 사용하여 Secure Firewall ASA의 구성을 Multicloud Defense(으)로 마이그레이션할 수 있습니다. 자세한 내용 및 마이그레이션 단계는 마이그레이션 툴을 사용하여 Cisco Secure Firewall ASA를 Cisco Multicloud Defense로 마이그레이션하기를 참조하십시오. • 이제 Secure Firewall 마이그레이션 툴을 사용하여 Palo Alto Networks 방화벽의 구성을 Multicloud Defense(으)로 마이그레이션할 수 있습니다. 자세한 내용 및 마이그레이션 단계는 마이그레이션 툴을 사용하여 Palo Alto Networks 방화벽을 Cisco Multicloud Defense로 마이그레이션하기를 참조하십시오.

버전	지원 기능
7.0.1	

버전	지원 기능
	이 릴리스에는 다음과 같은 새로운 기능과 개선 사항이 포함되어 있습니다. - 이제 ASA 및 FDM 매니지드 디바이스 및 서드파티 방화벽과 같은 Cisco 방화벽에서 Cisco Secure Firewall 1200 시리즈 디바이스로 구성을 마이그레이션할 수 있습니다. 참조: Cisco Secure Firewall 1200 시리즈 - 이제 둘 이상의 사이트 간 VPN 터널 구성에 대한 사전 공유 키를 한 번에 업데이트할 수 있습니다. 최적화, 검토 및 검증 페이지에 있는 사이트 간 VPN 테이블을 Excel 시트로 내보내고, 각 셀에 사전 공유 키를 지정한 다음 시트를 다시 업로드합니다. 마이그레이션 툴은 Excel에서 사전 공유 키를 읽고 테이블을 업데이트합니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: 모두 - 이제 마이그레이션을 방해하는 잘못된 구성을 무시하면서 마이그레이션의 최종 푸시를 계속할 수 있습니다. 이전에는 오류로 인해 단일 개체의 푸시가 실패한 경우에도 전체 마이그레이션이 실패했습니다. 또한 이제 마이그레이션을 수동으로 중단하여 오류를 수정하고 마이그레이션을 다시 시도할 수도 있습니다. 참조: 마이그레이션된 컨피그레이션을 Management Center에 푸시 지원되는 마이그레이션: 모두 - 이제 Secure Firewall 마이그레이션 툴은 대상 위협 방어 디바이스에서 기존 사이트 간 VPN 구성을 탐지하며, Management Center에 로그인하지 않고도 삭제할지 선택하라는 메시지를 표시합니다. No(아니요)를 선택하고 Management Center에서 수동으로 삭제하면 마이그레이션을 계속 진행할 수 있습니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: 모두 - 대상 관리 센터에서 관리하는 위협 방어 디바이스 중 하나에 기존 허브 및 스포크 토폴로지가 구성된 경우, 관리 센터에서 수동으로 수행할 필요 없이 마이그레이션 툴에서 바로 대상 위협 방어 디바이스를 기존 토폴로지에 스포크 중 하나로 추가하도록 선택할 수 있습니다. 참조: 구성 최적화, 검토 및 검증 지원되는 마이그레이션: Secure Firewall ASA - 서드파티 방화벽을 마이그레이션할 때 이제 고가용성 쌍의 일부인 위협 방어 디바이스를 대상으로 선택할 수 있습니다. 이전에는 독립형 위협 방어 디바이스만 대상 디바이스로 선택할 수 있었습니다. 지원되는 마이그레이션: Palo Alto Networks, Check Point, Fortinet 방화벽

버전	지원 기능
	마이그레이션 이제 Secure Firewall 마이그레이션 툴은 모든 단계에서 마이그레이션 지침과 함께 더욱 개선된 직관적인 데모 모드를 제공합니다. 또한 요구 사항에 따라 대상 위협 방어 디바이스의 버전을 선택하고 테스트할 수도 있습니다. 지원되는 마이그레이션: 모두
7.0	이 릴리스에는 다음과 같은 새로운 기능과 개선 사항이 포함되어 있습니다. Cisco Secure Firewall ASA를 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 대상 관리 센터에서 위협 방어 HA(고가용성) 쌍을 설정하고 Secure Firewall ASA HA 쌍에서 관리 센터로 구성을 마이그레이션할 수 있습니다. Select Target(대상 선택) 페이지에서 Proceed with HA Pair Configuration(HA 쌍 구성 진행)을 선택하고 액티브 디바이스 및 스탠바이 디바이스를 선택합니다. 액티브 위협 방어 디바이스를 선택할 경우, HA 쌍 설정이 성공적으로 수행되려면 동일한 디바이스가 관리 센터에 있어야 합니다. 자세한 내용은 마이그레이션 툴을 사용하여 <i>Cisco Secure Firewall ASA</i>를 <i>Cisco Secure Firewall Threat Defense</i>로 마이그레이션 책에서 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정을 참조하십시오. - 이제 Cisco ASA 디바이스에서 사이트 간 VPN 구성을 마이그레이션할 때 위협 방어 디바이스를 사용하여 사이트 간 허브 앤 스포크 VPN 토폴로지를 구성할 수 있습니다. Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증) 페이지의 Site-to-Site VPN Tunnels(사이트 간 VPN 터널) 아래에서 Add Hub & Spoke Topology(허브 및 스포크 토폴로지 추가)를 클릭합니다. 자세한 내용은 마이그레이션 툴을 사용하여 <i>Cisco Secure Firewall ASA</i>를 <i>Cisco Secure Firewall Threat Defense</i>로 마이그레이션 책에서 구성 최적화, 검토 및 검증을 참조하십시오. Fortinet 방화벽에서 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 SSL VPN과 Central SNAT 구성의 IPv6, 여러 인터페이스와 인터페이스 영역을 Fortinet 방화벽에서 위협 방어 디바이스로 마이그레이션할 수 있습니다. 자세한 내용은 마이그레이션 툴을 사용하여 <i>Fortinet</i> 방화벽을 <i>Cisco Secure Firewall Threat Defense</i>로 마이그레이션하기 책에서 Fortinet 구성 지원을 참조하십시오.

버전	지원 기능
6.0.1	

버전	지원 기능
	이 릴리스에는 다음과 같은 새로운 기능과 개선 사항이 포함되어 있습니다. Cisco Secure Firewall ASA를 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 Secure Firewall ASA에서 Threat Defense로 구성을 마이그레이션할 때 네트워크 및 포트 개체를 최적화할 수 있습니다. Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증) 페이지의 해당 탭에서 이러한 개체를 검토하고 Optimize Objects and Groups(개체 및 그룹 최적화)를 클릭하여 대상 Management Center로 개체를 마이그레이션하기 전에 개체 목록을 최적화합니다. 마이그레이션 툴은 동일한 값을 가진 개체 및 그룹을 식별하고 어떤 개체 및 그룹을 유지할지 선택하라는 메시지를 표시합니다. 자세한 정보는 구성 최적화, 검토 및 검증을 참조하십시오. FDM 매니지드 디바이스를 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 DHCP, DDNS 및 SNMPv3 구성을 FDM 매니지드 디바이스에서 Threat Defense 디바이스로 마이그레이션할 수 있습니다. Select Features(기능 선택) 페이지에서 DHCP 확인란과 Server(서버), Relay(릴레이) 및 DDNS 확인란을 선택합니다. 자세한 정보는 구성 최적화, 검토 및 검증을 참조하십시오. Fortinet 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 다른 개체 유형과 함께 URL 개체도 Fortinet 방화벽에서 Threat Defense 디바이스로 마이그레이션할 수 있습니다. 마이그레이션 중에 Objects(개체) 창의 Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증) 페이지에서 URL Objects(URL 개체) 탭을 검토합니다. 자세한 정보는 구성 최적화, 검토 및 검증을 참조하십시오. Palo Alto Networks 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 다른 개체 유형과 함께 URL 개체도 Palo Alto Networks 방화벽에서 Threat Defense 디바이스로 마이그레이션할 수 있습니다. 마이그레이션 중에 Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증) 페이지의 Objects(개체) 창에서 URL Objects(URL 개체) 탭을 검토합니다. 자세한 정보는 구성 최적화, 검토 및 검증을 참조하십시오. Check Point Firewall에서 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 포트 개체, FQDN 개체 및 개체 그룹을 Check Point 방화벽에서 Threat Defense 디바이스로 마이그레이션할 수 있습니다. 마이그레이션 중에 Objects(개체) 창의 Optimize, Review and Validate Configuration(구성

버전	지원 기능
	최적화, 검토 및 검증) 페이지를 검토합니다. 자세한 정보는 구성 최적화, 검토 및 검증을 참조하십시오.

버전	지원 기능
6.0	

버전	지원 기능
	이 릴리스에는 다음과 같은 새로운 기능과 개선 사항이 포함되어 있습니다. Cisco Secure Firewall ASA를 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 Secure Firewall ASA의 WebVPN 구성을 Threat Defense 디바이스의 Zero Trust Access Policy 구성으로 마이그레이션할 수 있습니다. Select Features(기능 선택) 페이지에서 WebVPN 확인란을 선택하고 Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증) 페이지에서 새 WebVPN 탭을 검토합니다. Threat Defense 디바이스 및 대상 Management Center 는 버전 7.4 이상에서 실행 중이어야 하며 Snort3을 탐지 엔진으로 실행해야 합니다. - 이제 SNMP(Simple Network Management Protocol) 및 DHCP(Dynamic Host Configuration Protocol) 구성을 Threat Defense 디바이스로 마이그레이션할 수 있습니다. Select Features(기능 선택) 페이지에서 SNMP 및 DHCP 확인란을 선택합니다. Secure Firewall ASA에서 DHCP를 구성한 경우, DHCP 서버 또는 릴레이 에이전트 및 DDNS 구성도 마이그레이션하도록 선택할 수 있습니다. - 이제 멀티 컨텍스트 ASA 디바이스를 수행하는 경우 ECMP(Equal-Cost Multipath) 라우팅 구성을 단일 인스턴스 Threat Defense 병합 컨텍스트 마이그레이션으로 마이그레이션할 수 있습니다. 구분 분석된 요약의 Routes(경로) 파일에는 이제 ECMP 영역도 포함되며, 구성 최적화, 검토 및 검증 페이지의 Routes(경로) 탭에서 동일한 영역을 검증할 수 있습니다. - 이제 Secure Firewall ASA의 DVTI(Dynamic Virtual Tunnel Interface) 구성에서 Threat Defense 디바이스로 동적 터널을 마이그레이션할 수 있습니다. 이는 ASA 인터페이스를 보안 영역, 인터페이스 그룹 및 VRF에 매핑 페이지에서 매핑할 수 있습니다. 이 기능을 적용하려면 ASA 버전이 9.19(x) 이상인지 확인합니다. FDM 매니지드 디바이스를 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 SNMP 및 HTTP를 비롯한 레이어 7 보안 정책과 악성코드 및 파일 정책 구성을 FDM 매니지드 디바이스에서 Threat Defense 디바이스로 마이그레이션할 수 있습니다. Select Features(기능 선택) 페이지에서 대상 Management Center 버전이 7.4 이상이고 Platform Settings(플랫폼 설정) 및 File and Malware Policy(파일 및 악성코드 정책) 확인란이 선택되어 있는지 확인합니다. Check Point Firewall에서 Cisco Secure Firewall Threat Defense로 마이그레이션 - 이제 Check Point 방화벽에서 사이트 간 VPN(정책 기반) 구성을 Threat

버전	지원 기능
	Defense 디바이스로 마이그레이션할 수 있습니다. 이 기능은 Check Point R80 이상 버전, Management Center 및 Threat Defense 버전 6.7 이상에 적용됩니다. Select Features(기능 선택) 페이지에서 Site-to-Site VPN Tunnel(사이트 간 VPN 터널) 확인란이 선택되어 있는지 확인합니다. 이는 디바이스별 구성이므로 Proceed Without FTD(FTD 없이 진행)를 선택하는 경우 마이그레이션 툴이 이러한 구성을 표시하지 않는다는 점에 유의합니다. Fortinet 방화벽에서 Cisco Secure Firewall Threat Defense로 마이그레이션 이제 Fortinet 방화벽에서 Threat Defense 디바이스로 구성을 마이그레이션할 때 애플리케이션 ACL(Access Control List)을 최적화할 수 있습니다. Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증) 페이지의 ACL 최적화 버튼을 사용하여 이중 및 새도 ACL 목록을 확인하고, 최적화 보고서를 다운로드하여 자세한 ACL 정보를 확인합니다.
5.0.1	이 릴리스에는 다음과 같은 새로운 기능과 개선 사항이 포함되어 있습니다. - Secure Firewall 마이그레이션 툴은 이제 Secure Firewall ASA 디바이스에서 Threat Defense 디바이스로의 여러 투명 방화벽 모드 보안 컨텍스트 마이그레이션을 지원합니다. Secure Firewall ASA 디바이스에 있는 둘 이상의 투명 방화벽 모드 컨텍스트를 투명 모드 인스턴스로 병합하고 마이그레이션할 수 있습니다. 하나 이상의 컨텍스트에 VPN 구성이 있는 VPN 구성 ASA 구축에서는 VPN 구성을 대상 Threat Defense 디바이스로 마이그레이션하려는 컨텍스트를 하나만 선택할 수 있습니다. 선택하지 않은 컨텍스트에서는 VPN 구성만 무시되고 다른 모든 구성이 마이그레이션됩니다. 자세한 내용은 ASA 보안 컨텍스트 선택을 참조하십시오. - 이제 Secure Firewall 마이그레이션 툴을 사용하여 Fortinet 및 Palo Alto Networks Firewall에서 Threat Defense로 사이트 간 및 원격 액세스 VPN 구성을 마이그레이션할 수 있습니다. Select Features(기능 선택) 창에서 마이그레이션할 VPN 기능을 선택합니다. 마이그레이션 툴을 사용하여 Palo Alto Networks Firewall에서 Secure Firewall Threat Defense로 마이그레이션 및 마이그레이션 툴을 사용하여 Fortinet 방화벽을 Secure Firewall Threat Defense로 마이그레이션 가이드의 Secure Firewall 마이그레이션 툴의 대상 매개변수 지정 섹션을 참조하십시오. - 이제 Secure Firewall ASA 디바이스에서 하나 이상의 라우팅 또는 투명 방화벽 모드 보안 컨텍스트를 선택하고 Secure Firewall 마이그레이션 툴을 사용하여 단일 컨텍스트 또는 멀티 컨텍스트 마이그레이션을 수행할 수 있습니다.

버전	지원 기능
5.0	- Secure Firewall 마이그레이션 툴은 이제 Secure Firewall ASA에서 Threat Defense 디바이스로의 여러 보안 컨텍스트 마이그레이션을 지원합니다. 컨텍스트 중 하나에서 구성을 마이그레이션하거나 모든 라우팅 방화벽 모드 컨텍스트의 구성을 병합하여 마이그레이션할 수 있습니다. 여러 투명 방화벽 모드 상황에서 구성을 병합하는 기능도 곧 제공될 예정입니다. 자세한 내용은 ASA 기본 보안 상황 선택을 참고하십시오. - 마이그레이션 툴은 이제 VRF(virtual routing and forwarding, 가상 라우팅 및 포워딩) 기능을 활용하여 새로 병합된 구성의 일부가 될 멀티 컨텍스트 ASA 환경에서 관찰된 분리된 트래픽 흐름을 복제합니다. Parsed Summary(구문 분석 요약) 페이지의 새 VRF 타일에서, 마이그레이션 툴이 새 Contexts(컨텍스트) 타일에서 탐지한 컨텍스트 수와 구문 분석 후에 확인할 수 있습니다. 또한 마이그레이션 툴은 보안 영역 및 인터페이스 그룹에 인터페이스 매핑 페이지에서 이러한 VRF가 매핑되는 인터페이스를 표시합니다. - 이제 Secure Firewall 마이그레이션 툴에서 새로운 데모 모드를 사용하여 전체 마이그레이션 워크플로우를 시도하고 실제 마이그레이션이 어떻게 이루어지는지 시각화할 수 있습니다. 자세한 내용은 방화벽 마이그레이션 툴의 데모 모드 사용을 참조하십시오. - 새로운 개선 사항과 버그 픽스를 통해, Secure Firewall 마이그레이션 툴은 이제 Palo Alto Networks Firewall을 Threat Defense로 마이그레이션할 때 개선되고 더 빠른 마이그레이션 환경을 제공합니다.
4.0.3	Secure Firewall 마이그레이션 툴 4.0.3에는 버그 수정 및 다음과 같은 개선 사항이 포함되어 있습니다. 이제 마이그레이션 툴에서는 PAN 구성을 Threat Defense로 마이그레이션할 수 있는 향상된 Application Mapping(애플리케이션 매핑) 화면을 제공합니다. 자세한 내용은 마이그레이션 툴을 사용하여 <i>Palo Alto Networks Firewall</i>을 <i>Secure Firewall Threat Defense</i>로 마이그레이션 가이드의 애플리케이션으로 구성 매핑을 참조하십시오.

버전	지원 기능
4.0.2	Secure Firewall 마이그레이션 툴 4.0.2에는 다음과 같은 새로운 기능 및 개선 사항이 포함되어 있습니다. - Secure Firewall 마이그레이션 툴 4.0.2에는 내장 설정 추출기 도구가 도입되었으며, 이는 이제 Extract Config Information(구성 정보 추출) 페이지에 표시됩니다. 따라서 구성 추출이 쉽게 이루어지고 추출기 툴을 다운로드하는 작업이 필요하지 않습니다. FMT-CP-Config-Extractor 툴은 더 이상 다운로드할 수 있는 독립형 애플리케이션으로 제공되지 않습니다. 자세한 내용은 구성 추출기를 사용하여 디바이스 구성 내보내기를 참조하십시오. - 이제 마이그레이션 툴에 상시 연결 텔레메트리가 있습니다. 그러나 이제 제한적 또는 광범위한 텔레메트리 데이터를 보내도록 선택할 수 있습니다. 제한된 텔레메트리 데이터에는 데이터 포인트가 거의 포함되지 않지만 광범위한 텔레메트리 데이터에는 더 자세한 텔레메트리 데이터 목록이 포함됩니다. Settings(설정) > Send Telemetry Data to Cisco?(시스코로 텔레메트리 데이터 전송?)에서 이 설정을 변경할 수 있습니다.
4.0.1	Secure Firewall 마이그레이션 툴 4.0.1에는 다음과 같은 새로운 기능 및 개선 사항이 포함되어 있습니다. - 이제 Check Point R81 구성을 Secure Firewall Threat Defense로 마이그레이션할 수 있습니다. - 이제 멀티 도메인 VSX(Virtual System Extension) 구축에서 구성을 내보내기 위해 Check Point 보안 게이트웨이에 연결할 때 가상 시스템 ID를 추가하도록 선택할 수 있습니다. - 몇 가지 명령을 수동으로 실행하여 Check Point VSX 버전 R77에서 구성을 추출할 수 있습니다. 자세한 내용은 마이그레이션 툴을 사용하여 <i>Check Point Firewall</i>을 <i>Threat Defense</i>로 마이그레이션 가이드의 FMT-CP-Config-Extractor_v4.0-7965 툴을 사용하여 디바이스 구성 내보내기를 참조하십시오.
3.0.1	FirePOWER Services를 포함한 ASA, Check Point, Palo Alto Networks 및 Fortinet의 경우 Secure Firewall 3100 Series는 대상 디바이스로만 지원됩니다.
3.0	Secure Firewall 마이그레이션 툴 3.0은 대상 Management Center가 7.2 이상인 경우 Check Point에서 클라우드 제공 Firewall Management Center로의 마이그레이션을 지원합니다.

버전	지원 기능
2.5.2	Secure Firewall 마이그레이션 툴 2.5.2는 Check Point 방화벽의 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 구성 및 규칙 집합이 있는 경우 기본이 아닌 ACL을 제거해도 네트워크에 영향을 주지 않습니다. - 새도우 ACL - 첫 번째 ACL은 두 번째 ACL의 컨피그레이션을 완전히 새도입합니다. 참고 최적화는 Check Point ACP 규칙 작업에만 사용할 수 있습니다. Secure Firewall 마이그레이션 툴 2.5.2는 대상 Firewall Management Center가 7.1 이상인 경우 BGP(Border Gateway Protocol) 및 유동 경로 개체 마이그레이션을 지원합니다.

버전	지원 기능
2.2	• r80 Check Point OS 버전 지원 • Check Point(r80) 디바이스에서 컨피그레이션을 추출하도록 Live Connect를 지원합니다. • 다음과 같은 지원되는 Check Point 컨피그레이션 요소를 r80용 Firewall Threat Defense로 마이그레이션할 수 있습니다. • 인터페이스 • 고정 경로 • 개체 • 네트워크 주소 변환 • 액세스 제어 정책 • Global Policy(전역 정책) - 이 옵션을 선택하면 경로 조회가 없으므로 ACL 정책의 소스 및 대상 영역이 Any(모두)로 마이그레이션됩니다. • Zone-Based Policy(영역 기반 정책) - 이 옵션을 선택하면 소스 및 대상 네트워크 개체 또는 그룹에 대한 라우팅 메커니즘을 통해 예측 경로 조회를 기반으로 소스 및 대상 영역이 도출됩니다. 참고 경로 조회는 정적 경로 및 동적 경로(PBR 및 NAT 제외)로만 제한되며, 소스 및 대상 네트워크 개체 그룹의 특성에 따라 이 작업으로 인해 규칙이 급증할 수 있습니다. 참고 영역 기반 정책에 대한 IPv6 경로 조회는 지원되지 않습니다.

버전	지원 기능
2.0	- Secure Firewall 마이그레이션 툴의 새로운 최적화 기능을 통해 검색 필터를 사용하여 마이그레이션 결과를 빠르게 가져올 수 있습니다. - Secure Firewall 마이그레이션 툴을 사용하여 다음과 같은 지원되는 Check Point 구성 요소를 Firewall Threat Defense로 마이그레이션할 수 있습니다. - 인터페이스 - 고정 경로 - 개체 - 액세스 제어 정책 - Global Policy(전역 정책) - 이 옵션을 선택하면 ACL 정책의 소스 및 대상 영역이 Any(모두)로 마이그레이션됩니다. - Zone-Based Policy(영역 기반 정책) - 이 옵션을 선택하면 소스 및 대상 네트워크 개체 또는 그룹에 대한 라우팅 메커니즘을 통해 예측 경로 조회를 기반으로 소스 및 대상 영역이 도출됩니다. 참고 경로 조회는 정적 경로 및 동적 경로(PBR 및 NAT 제외)로만 제한되며, 소스 및 대상 네트워크 개체 그룹의 특성에 따라 이 작업으로 인해 규칙이 급증할 수 있습니다. - 네트워크 주소 변환 • Check Point OS 버전 r75, r76, r77, r77.10, r77.20 및 r77.30을 지원합니다.

Secure Firewall 마이그레이션 툴 라이선싱

Secure Firewall 마이그레이션 툴 애플리케이션은 무료이며 라이선스가 필요하지 않습니다. 그러나 Firewall Threat Defense 디바이스를 성공적으로 등록하고 정책을 구축하려면 관련 Firewall Threat Defense 기능에 필요한 라이선스가 Firewall Management Center에 있어야 합니다.

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

Threat Defense 디바이스의 요구 사항 및 사전 요건

Management Center로 마이그레이션할 때 대상 Threat Defense 디바이스를 추가해야 하는 것은 아닙니다. 나중에 Threat Defense 디바이스에 구축하도록 정책을 Management Center로 마이그레이션할 수 있습니다.

관리 센터에 위협 방어 장치가 추가된 경우 Check Point 구성을 Threat Defense로 마이그레이션하려면 다음 요구 사항 및 사전 요건을 고려합니다.

- 대상 Threat Defense 디바이스를 Management Center에 등록해야 합니다.
- 대상 위협 방어 디바이스는 고가용성 구성에 있을 수 있습니다.
- Threat Defense 디바이스는 독립형 디바이스 또는 컨테이너 인스턴스일 수 있습니다. 클러스터에 속해선 안 됩니다.
 - 대상 네이티브 Firewall Threat Defense 디바이스에서 최소한 Check Point와 같은 수의 물리적 데이터 또는 포트 채널 인터페이스 또는 하위 인터페이스('관리 전용' 제외)를 사용해야 합니다. 그렇지 않은 경우 대상 Firewall 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 Check Point와 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.

Check Point 구성 지원

지원되는 체크 포인트 구성

- 인터페이스(물리적, VLAN 및 결합 인터페이스)
- 네트워크 개체 및 그룹: Secure Firewall 마이그레이션 툴은 모든 Check Point 네트워크 개체를 Threat Defense로 마이그레이션할 수 있도록 지원합니다.
- 서비스 개체
- 네트워크 주소 변환
- 이중 유형 IP 주소를 사용하는 네트워크 개체가 포함된 수동 NAT 규칙
- IPv6 변환 지원(인터페이스, 정적 경로, 개체, ACL 및 NAT) 및 IPv6를 사용하는 영역 기반 ACL 제외
- 전역 ACL을 영역 기반 ACL로 변환하도록 지원되고 전역적으로 적용되는 액세스 규칙
- 정적 경로 - 범위가 로컬로 설정된 경로 및 다음 홉 IP 주소가 없는 정적 경로에 대한 이그레스 인터페이스인 논리적 인터페이스를 사용하는 경로 제외
- 추가 로깅 유형이 있는 ACL
- 부정 매개변수가 있는 ACE
- Check Point r80-r82 이상 버전용 정책 기반 사이트 간 VPN: IPv4 및 PSK(사전 공유 키) 기반 인증. 라이브 연결 옵션을 사용하여 VPN 구성을 마이그레이션하는 것이 좋습니다.
- ID 기반 ACL 정책
- 사용자 기반 액세스 제어 정책 규칙



참고

Check Point에 해당 NAT 규칙이 있는 Check Point에 설정된 ACE의 경우, Secure Firewall 마이그레이션 툴은 실제 IP 주소를 마이그레이션된 해당 ACE 규칙의 변환된 IP 주소에 매핑하지 않습니다. ACE 규칙에 대한 참조 정보가 NAT 규칙에 대한 참조 정보가 없으므로 Secure Firewall 마이그레이션 툴은 IP 주소를 매핑하지 않습니다. 따라서 방화벽 관리 센터에서 마이그레이션된 ACE 및 NAT 구성을 검증하는 동안에는 위협 방어 패킷 플로우에 해당하는 ACE 규칙을 확인하고 수동으로 변경해야 합니다.



참고

Secure Firewall 마이그레이션 툴은 서비스 개체(소스 및 대상, 그리고 개체 그룹에서 호출되는 동일한 유형의 개체와 결합된 포트 조합으로 구성된 개체)를 마이그레이션하지 않지만, 참조된 ACL 및 NAT 규칙은 전체 기능으로 마이그레이션됩니다.

지원되지 않는 Check Point 구성에 대한 자세한 내용은 [지원되지 않는 Check Point 구성](#)을 참조하십시오.

부분적으로 지원되는 Check Point 구성

Secure Firewall 마이그레이션 툴은 다음 Check Point 구성의 마이그레이션을 부분적으로 지원합니다. 이러한 구성 중 일부에는 고급 옵션을 포함하며 고급 옵션 없이 마이그레이션할 수 있는 규칙이 있습니다. 방화벽 관리 센터에서 이러한 고급 옵션을 지원하는 경우 마이그레이션이 완료된 후 수동으로 구성할 수 있습니다.

- 순위 및 ping 매개변수가 있는 정적 경로가 부분적으로 마이그레이션됩니다.
- 모드, XOR, 액티브 백업, 라운드 로빈 유형의 결합 인터페이스는 Secure Firewall 마이그레이션 툴에 의해 방화벽 관리 센터에서 LACP 유형으로 부분적으로 마이그레이션됩니다.
- 물리 인터페이스나 결합 인터페이스와 같은 상위 인터페이스의 일부인 별칭 인터페이스 구성의 경우, 별칭 인터페이스 구성은 무시되고 상위 인터페이스의 속성은 있는 그대로 마이그레이션됩니다.
- 제외 유형의 네트워크 개체 그룹은 의미를 그대로 유지하기 위해 ACL을 통해 지원됩니다.
- 로깅 유형 추가가 있는 ACL과 시간 범위가 포함된 ACL.

지원되는 Check Point 구성

Secure Firewall 마이그레이션 툴은 다음 Check Point 구성을 지원하지 않습니다. 방화벽 관리 센터에서 이러한 구성을 지원하는 경우 마이그레이션이 완료된 후 수동으로 구성을 구성할 수 있습니다.

- 별칭, 브리지, 6IN4 터널, 루프백 및 PPPoE 인터페이스
- 네트워크 개체 및 그룹:
 - UTM-1 Edge 게이트웨이
 - Check Point 호스트
 - 게이트웨이 클러스터
 - 외부에서 관리되는 게이트웨이 또는 호스트
 - OSE(Open Security Extension) 디바이스
 - 논리적 서버
 - 동적 개체
 - VoIP 도메인
 - Zone
 - CP 보안 게이트웨이
 - CP 관리 서버

- 제외 유형의 네트워크 개체 그룹
- 서비스 개체:
 - RPC
 - DCE-RPC
 - 복합 TCP
 - GTP
 - 기타 Check Point 특정 서비스 개체
- 다음이 포함된 ACL 정책:
 - 지원되지 않는 ACE 작업 유형(클라이언트 인증, 세션 인증, 사용자 인증 및 기타 맞춤형 인증 유형)은 허용 작업 유형을 사용하여 마이그레이션되지만, 비활성화됨 상태
 - IPv6 경로 조회를 사용하는 영역 기반 정책
 - 전역 다중 도메인 시스템 규칙을 마이그레이션할 수 없음



참고 Check Point 다중 도메인 구축의 글로벌 다중 도메인 시스템 설정을 내보낼 수 없습니다. 따라서 특정 CMA와 관련된 구성을 내보내고 마이그레이션만 할 수 있습니다.

- 지원되지 않는 ICMP 유형 및 코드가 포함된 개체
- 터널링 프로토콜 기반 액세스 제어 정책 규칙
- 암시적 ACL 규칙
- 원격 액세스 VPN
- 영역 기반 ACE 선택하고 100보다 큰 값을 가진 범위 개체를 갖는 경우 ACE에 대한 영역은 마이그레이션되고 ACE 이름 및 적절한 설명에 추가되는 no-lookup을 사용하여 **Any(모두)**로 표시됩니다.
- 선택된 영역 기반 ACE가 IPv6 주소를 가진 ACE에 대한 영역이 모두로 표시되고 적절한 설명과 함께 ACE 지원되지 않습니다.

지원되지 않는 **NAT** 규칙

Secure Firewall 마이그레이션 툴은 다음 NAT 규칙을 지원하지 않습니다.

- 게이트웨이 뒤에 숨겨진 자동 NAT 규칙
- Check Point 보안 게이트웨이를 사용하는 수동 NAT 규칙.

- 상속된 개체가 IPv6 구성인 개체 그룹을 포함하는 수동 NAT 규칙
- 서비스 그룹이 있는 수동 NAT 규칙
- IPv6 NAT 규칙

지원되지 않는 정적 경로

- **netstat -rnm**에서 이그레스 인터페이스를 찾을 수 없는 경우의 정적 경로
- 논리적 게이트웨이를 종료 인터페이스로 사용하는 정적 경로
- ECMP 유형의 정적 경로
- 로컬 범위 속성이 종료 인터페이스로 있는 정적 경로

지침 및 제한 사항

변환 중에 Secure Firewall 마이그레이션 툴은 지원되는 모든 개체 및 규칙에 대해 일대일 매핑을 생성합니다(규칙 또는 정책에 사용되는지 여부). 그러나 Secure Firewall 마이그레이션 툴은 사용되지 않는 개체(ACL에서 참조되지 않는 개체)의 마이그레이션을 제외할 수 있는 최적화 기능을 제공합니다.

Secure Firewall 마이그레이션 툴은 지원되지 않는 개체 및 규칙을 지정된 대로 처리합니다.

- 지원되지 않는 개체 및 경로는 마이그레이션되지 않습니다.
- 지원되지 않는 ACL 규칙은 비활성화된 규칙으로 Management Center에 마이그레이션됩니다.

Check Point 구성 제한 사항

소스 Check Point 구성을 마이그레이션하는 경우 다음과 같은 제한 사항이 있습니다.

- 시스템 컨피그레이션은 마이그레이션되지 않습니다.
- 방화벽의 라이브 연결 Check Point(r80-r82) 이상 버전에 대해서만 지원됩니다.
- 모든 명시적 보안 정책(r77.30 이하 버전의 경우 Security_Policy.xml에서 사용 가능하고 r80-r82 이상 버전의 경우 보안 정책 파일에서 사용 가능)은 Management Center의 ACP로 마이그레이션됩니다. 암시적 규칙은 내보낸 구성의 일부가 아니므로 Check Point Smart 대시보드의 규칙은 마이그레이션되지 않습니다.



참고

- Check Point(r80-r82) 및 이후 버전의 경우, L4 보안 계층 정책에 별도의 애플리케이션 계층 정책이 연결되어 있으면, Secure Firewall 마이그레이션 도구는 해당 정책을 지원되지 않는 항목으로 마이그레이션합니다. 또한 이러한 경우 ACE 설정이 포함된 파일이 두 개입니다. 하나는 보안 레이어용이고 다른 하나는 애플리케이션 레이어용입니다. Secure Firewall 마이그레이션 툴은 구성 zip 파일의 *index.json*에 있는 액세스 레이어에서 사용 가능한 우선순위 정보를 기반으로 마이그레이션합니다.
- 멀티 도메인 배포(Multi-Domain Deployment)가 설정되어 있고, 글로벌 정책과 고객 관리형 애드온(CMA) 전용 정책이 모두 구성된 Check Point r80-r82 및 이후 버전의 경우, Secure Firewall 마이그레이션 도구가 Check Point 구성을 마이그레이션하는 순서는 소스 구성의 순서와 약간 다를 수 있습니다. 또한 이러한 경우 ACE 설정이 포함된 파일이 두 개입니다. 하나는 전역 정책용이고 다른 하나는 CMA 정책용입니다. 도메인 계층 아래에 구성된 ACE는 지원되지 않음으로 마이그레이션됩니다.
- 멀티 도메인 시스템에서 작업이 도메인 레이어인 CMA에 대해 설정된 ACE 규칙의 순서 정의가 추출된 설정에서 불완전합니다. 따라서 소스 구성에서 특정 CMA 정책에 전역 정책이 연결되어 있는 경우, 추출된 구성에서 규칙 번호 인덱스를 확인하여 순서가 올바른지 확인합니다.
- 동적 라우팅 및 위협 방어에 대한 VPN과 같은 일부 Check Point 구성은 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션할 수 없습니다. 이러한 컨피그레이션은 수동으로 마이그레이션해야 합니다.
- Check Point 브리지, 터널 및 관리 센터에 대한 별칭 인터페이스는 마이그레이션할 수 없습니다.
- 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 동일한 개체 내에 구성된 소스 및 대상 포트를 가진 서비스 개체 또는 그룹을 분리합니다. 이러한 액세스 제어 규칙에 대한 참조는 정확히 동일한 의미의 Management Center 규칙으로 변환됩니다.

Check Point 마이그레이션 지침

Check Point 로그 옵션의 마이그레이션은 위협 방어의 모범 사례를 따릅니다. 규칙에 대한 로그 옵션은 소스 Check Point 구성에 따라 활성화되거나 비활성화됩니다. **drop**(삭제) 또는 **reject**(거부) 작업이 있는 규칙의 경우 Secure Firewall 마이그레이션 툴은 연결 시작 시 기록을 구성합니다. 작업이 **permit**(허용)인 경우 Secure Firewall 마이그레이션 툴은 연결 종료 시 기록을 구성합니다.

개체 마이그레이션 지침

위협 방어에서 포트 개체라고 하는 서비스 개체에는 개체에 대한 구성 지침이 다릅니다. 예를 들어 Check Point에서는 한 개체의 이름이 소문자, 다른 개체의 이름이 대문자로 되어 있다면 하나 이상의 서비스 개체가 동일한 이름을 가질 수 있습니다. 그러나 Threat Defense에서와 같이 대소문자에 관계 없이 각 개체가 고유한 이름을 가져야 합니다. Secure Firewall 마이그레이션 툴은 모든 Check Point 개체를 분석하고 다음 방법 중 하나로 마이그레이션을 처리합니다.

- 각 Check Point 개체에는 고유한 이름 및 구성이 있습니다. Secure Firewall 마이그레이션 툴은 변경 없이 개체를 마이그레이션합니다.
- Check Point 서비스 개체의 이름에 Management Center에서 지원하지 않는 특수 문자가 하나 이상 포함되어 있습니다. Secure Firewall 마이그레이션 툴은 개체 이름의 특수 문자 이름을 "_" 문자로 변경하여 Management Center 개체 명명 기준을 충족합니다.
- Check Point 서비스 개체는 Management Center의 기존 개체와 동일한 이름 및 구성을 갖습니다. Secure Firewall 마이그레이션 툴은 Threat Defense 구성에 Management Center 개체를 재사용하고 Check Point 개체는 마이그레이션하지 않습니다.
- Check Point 서비스 개체는 Management Center에 있는 기존 개체와 이름은 같지만 구성이 다릅니다. Secure Firewall 마이그레이션 툴은 개체 충돌을 보고하며 마이그레이션용 Check Point 서비스 개체의 이름에 고유한 접미사를 추가하여 충돌을 해결할 수 있습니다.
- 여러 Check Point 서비스 개체는 이름은 같지만 대소문자가 다릅니다. Secure Firewall 마이그레이션 툴이 Threat Defense 개체 명명 기준에 맞게 이름을 바꿉니다.

Firewall Threat Defense 디바이스 관련 지침 및 제한 사항

Check Point 구성을 Firewall Threat Defense로 마이그레이션하려는 경우 다음 지침 및 제한 사항을 고려하십시오.

- 경로, 인터페이스 등 기존 디바이스별 구성이 Firewall Threat Defense에 있는 경우 푸시 마이그레이션 중에 Secure Firewall 마이그레이션 툴이 디바이스를 자동으로 정리하고 Check Point 구성에서 덮어씁니다.



참고 디바이스(대상 Firewall Threat Defense) 컨피그레이션 데이터의 원치 않는 손실을 방지하려면 마이그레이션 전에 디바이스를 수동으로 정리하는 것이 좋습니다.

마이그레이션 중에 Secure Firewall 마이그레이션 툴이 인터페이스 컨피그레이션을 재설정합니다. 정책에서 이러한 인터페이스를 사용하는 경우 Secure Firewall 마이그레이션 툴이 해당 인터페이스를 재설정할 수 없으므로 마이그레이션이 실패합니다.

- Secure Firewall 마이그레이션 툴은 Check Point 구성에 따라 Firewall Threat Defense 디바이스의 네이티브 인스턴스에서 하위 인터페이스를 생성할 수 있습니다. 마이그레이션을 시작하기 전에 대상 Firewall Threat Defense 디바이스에서 인터페이스 및 포트 채널 인터페이스를 수동으로 생성합니다. 예를 들어 Check Point 구성에 다음 인터페이스 및 포트 채널이 할당된 경우 마이그레이션

이전 전에 대상 Firewall Threat Defense 디바이스에서 해당 인터페이스 및 포트 채널을 생성해야 합니다.

- 물리적 인터페이스 5개
- 포트 채널 5개
- 관리 전용 인터페이스 2개



참고 Firewall Threat Defense 디바이스의 컨테이너 인스턴스인 경우 하위 인터페이스는 Secure Firewall 마이그레이션 툴로 생성되지 않으며 인터페이스 매핑만 허용됩니다.

마이그레이션에 지원되는 플랫폼

다음 Check Point 및 Firewall Threat Defense 플랫폼은 Secure Firewall 마이그레이션 툴을 사용한 마이그레이션에 지원됩니다. 지원되는 Firewall Threat Defense 플랫폼에 대한 자세한 내용은 [Cisco Secure Firewall 호환성 가이드](#)에서 참고하십시오.



참고 Secure Firewall 마이그레이션 툴은 독립형 모드 또는 분산형 Check Point 구성을 독립형 Firewall Threat Defense 디바이스로 마이그레이션하는 것만 지원합니다.

지원되는 대상 **Firewall Threat Defense** 플랫폼

Secure Firewall 마이그레이션 툴을 사용하여 소스 Check Point 구성을 Firewall Threat Defense 플랫폼의 다음과 같은 독립형 또는 컨테이너 인스턴스로 마이그레이션할 수 있습니다.

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 220 Series
- Secure Firewall 3100 Series
- Secure Firewall 3200 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- Secure Firewall 6100 Series
- 다음을 포함하는 Firepower 9300 Series:

- 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 Firewall Threat Defense Virtual 사전 요건 및 사전 스테이징에 대한 자세한 내용은 [Cisco Secure Firewall Threat Defense Virtual 시작하기](#) 및 Azure를 참고하십시오.
- AWS 클라우드의 Firewall Threat Defense Virtual 사전 요구 사항 및 사전 스테이징에 대한 자세한 내용은 [Threat Defense Virtual 사전 요건](#)을 참고하십시오.

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



참고

Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션을 성공적으로 수행하려면 먼저 Firewall Management Center 또는 Threat Defense Virtual을 사전 스테이징하는 사전 요건을 충족해야 합니다.



참고

Secure Firewall 마이그레이션 툴을 사용하려면 소스 구성을 추출하거나 (CP(r80-r82) Live Connect) 수동으로 업로드한 구성을 클라우드의 Firewall Management Center에 마이그레이션하기 위해 클라우드에서 호스팅되는 모든 디바이스에 대한 네트워크 연결이 필요합니다. 따라서 Secure Firewall 마이그레이션 툴을 사용하기 전에 사전 요건으로 IP 네트워크 연결을 사전 스테이징해야 합니다.

마이그레이션에 지원되는 대상 **Management Center**

Secure Firewall 마이그레이션 툴은 Management Center 및 클라우드 제공 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, 34 페이지에 설명된 대로 마이그레이션에 지원되는 Management Center 소프트웨어 버전.
- Check Point 마이그레이션에 지원되는 Firewall Management Center 소프트웨어 버전은 6.2.3.3 이상입니다.
- 다음에 설명된 대로 Check Point 인터페이스에서 마이그레이션하려는 모든 기능을 포함하는 Firewall Threat Defense용 스마트 라이선스를 얻고 설치해야 합니다.
 - Cisco.com에 있는 [Cisco 스마트 어카운트](#)의 Getting Started(시작하기) 섹션
 - [Cisco Smart Software Manager](#)에 Firewall Management Center를 등록합니다.
 - [Firewall 시스템 라이선싱](#)
 - Firewall Management Center에서 REST API를 활성화해야 합니다.

Firewall Management Center 웹 인터페이스에서 **System(시스템) > Configuration(구성) > Rest API Preferences(Rest API 환경 설정) > Enable Rest API(Rest API 활성화)**로 이동하여 **Enable Rest API(Rest API 활성화)** 확인란을 선택합니다.



중요 REST API를 활성화하려면 Firewall Management Center에서 관리자 사용자 역할이 있어야 합니다. Management Center 사용자 역할에 대한 자세한 내용은 [User Roles\(사용자 역할\)](#)를 참조하십시오.

클라우드 제공 **Firewall Management Center**

클라우드 제공 Firewall Management Center는 Threat Defense 디바이스를 위한 관리 플랫폼이며, Security Cloud Control(이전에는 Cisco Defense Orchestrator)를 통해 제공됩니다. 클라우드 제공 Firewall Management Center는 Management Center와 동일한 여러 기능을 제공합니다.

Security Cloud Control에서 클라우드 제공 Firewall Management Center에 액세스할 수 있습니다. Security Cloud Control은 보안 디바이스 커넥터(SDC)를 통해 클라우드 제공 Firewall Management Center에 연

결합니다. 클라우드 제공 Firewall Management Center에 대한 자세한 내용은 [클라우드 제공 Firewall Management Center를 사용하여 Cisco Secure Firewall Threat Defense 디바이스 관리](#)를 참고하십시오.

Secure Firewall 마이그레이션 툴은 클라우드 제공 Firewall Management Center를 마이그레이션 대상 Management Center로 지원합니다. 마이그레이션 대상 Management Center로 클라우드 제공 Firewall Management Center를 선택하려면 Security Cloud Control 지역을 추가하고 Security Cloud Control 포털에서 API 토큰을 생성해야 합니다.

Security Cloud Control 지역

Security Cloud Control는 3개의 서로 다른 지역에서 사용할 수 있으며, 지역은 URL 확장명으로 식별할 수 있습니다.

표 1: Security Cloud Control 지역 및 URL

지역	Security Cloud Control URL
유럽	https://eu.manage.security.cisco.com/
미국	https://us.manage.security.cisco.com/
APJC	https://apj.manage.security.cisco.com/
호주	https://au.manage.security.cisco.com/
인도	https://in.manage.security.cisco.com/

마이그레이션에 지원되는 소프트웨어 버전

항목은 지원되는 Secure Firewall 마이그레이션 툴, Check Point 및 마이그레이션용 Firewall Threat Defense 버전을 나열합니다.

지원되는 Secure Firewall 마이그레이션 툴 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.

지원되는 Check Point 버전

Secure Firewall 마이그레이션 툴은 Check Point OS 버전 r75-r77.30 및 r80-r82.40을 실행하는 Firewall Threat Defense로의 마이그레이션을 지원합니다. **Select Source(소스 선택)** 페이지에서 적절한 Check Point 버전을 선택합니다.

Secure Firewall 마이그레이션 툴은 Check Point 플랫폼 Gaia 및 VSX(Virtual System Extension) 구축에서의 마이그레이션을 지원합니다.

소스 **Check Point** 방화벽 컨피그레이션에 지원되는 **Firewall Management Center** 버전

Check Point 방화벽의 경우 Secure Firewall 마이그레이션 툴은 6.2.3.3 이상 버전을 실행하는 Firewall Management Center에서 관리되는 Firewall Threat Defense 디바이스로의 마이그레이션을 지원합니다.



참고 6.7 Firewall Threat Defense 디바이스로의 마이그레이션은 현재 지원되지 않습니다. 따라서 디바이스가 Firewall Management Center 액세스용 데이터 인터페이스로 구성된 경우 마이그레이션이 실패할 수 있습니다.

지원되는 **Firewall Threat Defense** 버전

Secure Firewall 마이그레이션 툴에서는 Firewall Threat Defense 6.5 이상 버전을 실행하는 디바이스로의 마이그레이션을 권장합니다.

의 운영체제 및 호스팅 환경 요구 사항을 포함한 Cisco Firewall 소프트웨어 및 하드웨어 호환성에 대한 자세한 내용은 [Cisco Firewall 호환성 가이드](#)를 참고하십시오.

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.