



Cisco Secure Firewall 마이그레이션 툴을 사용하여 Check Point 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션하기

최종 변경: 2026년 10월 8일

Americas Headquarters

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022– Cisco Systems, Inc. 모든 권리 보유.



목 차

장 1

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

장 2

Check Point 에서 Threat Defense 마이그레이션 워크플로우	37
엔드 투 엔드 절차	37
마이그레이션 사전 요건	39
Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드	40
체크 포인트 컨피그레이션 파일 내보내기	40
Check Point r77 구성 파일 내보내기	41
마이그레이션 실행	44
Secure Firewall 마이그레이션 툴 실행	44
Secure Firewall 마이그레이션 툴에서 데모 모드 사용	47
Check Point r80-r82 구성 파일 내보내기	48
Live Connect를 사용한 구성 추출을 위한 Check Point(r80-r82) 디바이스 사전 스테이징	48
Check Point r80-r82 구성 파일 내보내기 절차	57

다른 구성 파일 추출	60
Check Point 컨피그레이션 파일 업로드	61
Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정	62
마이그레이션 전 보고서 검토	65
Check Point Firewall 구성과 Firewall Threat Defense 인터페이스 매핑	66
Check Point 인터페이스를 보안 영역 및 인터페이스 그룹에 매핑	67
최적화, 구성 검토 및 검증	69
마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시	74
Check Point에 대한 마이그레이션 후 보고서 검토 및 마이그레이션 완료	76
Secure Firewall 마이그레이션 툴 제거	77
샘플 마이그레이션: Check Point 를 Threat Defense 2100으로	77
유지 보수 기간 작업별	78
유지 보수 기간 작업	79

장 3	Cisco Success Network - 텔레메트리 데이터	81
	Cisco Success Network - 텔레메트리 데이터	81

장 4	마이그레이션 문제 해결	91
	Secure Firewall 마이그레이션 툴 문제 해결	91
	문제 해결에 사용되는 로그 및 기타 파일	92
	Check Point 파일 업로드 실패 문제 해결	92
	Check Point 문제 해결 예: 개체 그룹의 멤버를 찾을 수 없음(r75-r77.30만 해당)	93
	Live Connect의 Check Point(r80-r82) 문제 해결 예	94



1 장

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 -rnv`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.xml`에서 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 Center](#)를 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.



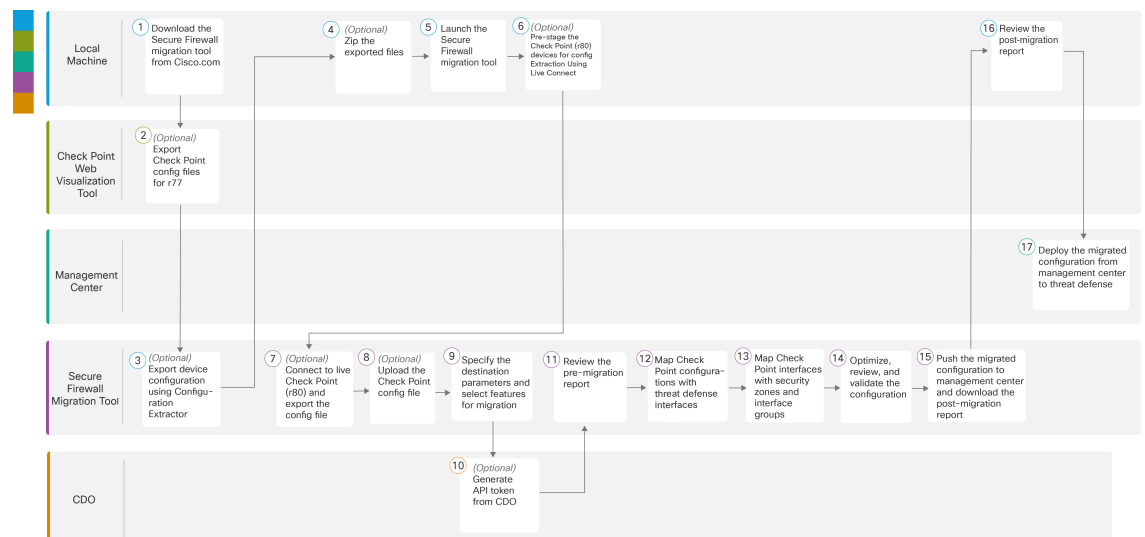
2 장

Check Point에서 Threat Defense 마이그레이션 워크플로우

- 엔드 투 엔드 절차, 37 페이지
- 마이그레이션 사전 요건, 39 페이지
- 마이그레이션 실행, 44 페이지
- Secure Firewall 마이그레이션 툴 제거, 77 페이지
- 샘플 마이그레이션: Check Point 를 Threat Defense 2100으로 , 77 페이지

엔드 투 엔드 절차

다음 순서도는 Secure Firewall 마이그레이션 툴을 사용하여 Check Point 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	Check Point 웹 시각화 툴	(선택 사항) r77에 대한 Check Point 구성 파일 내보내기: r77에 대한 Check Point 구성 파일을 내보내려면 Check Point r77 구성 파일 내보내기, 41 페이지를 참조하십시오. Secure Firewall 마이그레이션 툴의 라이브 연결 기능을 사용하여 r80-r82용 구성 파일을 내보내려면 5단계로 건너뛩니다.
③	로컬 컴퓨터	로컬 머신에서 Secure Firewall 마이그레이션 툴을 실행하고 요구 사항에 따라 Source Firewall Vendor(소스 방화벽 벤더) 드롭다운에서 Check Point(r75-r77) 또는 Check Point(r80-r82)를 선택합니다. 자세한 정보는 Secure Firewall 마이그레이션 툴 시작을 참조하십시오.
④	Secure Firewall 마이그레이션 툴	(선택 사항) Check Point에서 디바이스 설정 내보내기(r75-r77): 보안 게이트웨이 연결을 통해 Configuration Extractor(구성 추출기)를 사용하여 r77에 대한 디바이스 설정을 내보내려면 구성 추출기를 사용하여 디바이스 구성 내보내기, 42 페이지를 참조하십시오.
⑤	로컬 컴퓨터	(선택 사항) 내보낸 파일 압축: r77에 대해 내보낸 모든 설정 파일을 선택하고 zip 파일로 압축합니다. 자세한 단계는 내보낸 파일 압축을 참조하십시오.
⑥	로컬 컴퓨터	구성 추출을 위한 Check Point (r80-r82) 디바이스 사전 스테이징: 방화벽에서 Live Connect를 사용하기 전에 Check Point(r80-r82) 디바이스에 자격 증명을 구성해야 합니다. Check Point(r80-r82) 디바이스의 사전 스테이징 자격 증명은 구성 추출을 위한 Check Point(r80-r82) 디바이스 사전 스테이징을 참조하십시오. 이 단계는 r80-r82 디바이스에 대한 구성 파일을 마이그레이션하려는 경우에만 필요합니다. r77 디바이스의 구성을 마이그레이션하려는 경우 8단계로 건너뛩니다.
⑦	Secure Firewall 마이그레이션 툴	(선택 사항) 라이브 Check Point(r80-r82)에 연결하고 구성 파일 내보내기: 라이브 연결 기능을 사용하여 r80-r82에 대한 Check Point 구성 파일을 내보내려면 r80-r82용 Check Point 구성 파일을 내보내는 절차를 참조하십시오.
⑧	Secure Firewall 마이그레이션 툴	(선택 사항) Check Point 구성 파일 업로드: Check Point 구성 파일 업로드에 대한 자세한 단계는 Check Point 구성 파일 업로드를 참조하십시오.
⑨	Secure Firewall 마이그레이션 툴	이 단계에서 마이그레이션의 대상 매개변수를 지정할 수 있습니다. 자세한 단계는 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정을 참조하십시오.

	업무 환경	단계
⑩	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.
⑪	Secure Firewall 마이그레이션 툴	마이그레이션 전 보고서를 다운로드한 위치로 이동하여 보고서를 검토합니다. 자세한 단계는 마이그레이션 전 보고서 검토 를 참고하십시오.
⑫	Secure Firewall 마이그레이션 툴	Secure Firewall 마이그레이션 툴을 사용하면 Check Point 구성을 Threat Defense 인터페이스와 매핑할 수 있습니다. 자세한 단계는 Secure Firewall Device Manager Threat Defense 인터페이스와 Check Point 구성 매핑 을 참고하십시오.
⑬	Secure Firewall 마이그레이션 툴	Check Point 구성이 올바르게 마이그레이션되도록 하려면 Check Point 인터페이스를 적절한 위협 방어 인터페이스 개체, 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 단계는 Check Point 인터페이스를 보안 영역 및 인터페이스 그룹에 매핑 을 참고하십시오.
⑭	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 검증 을 참고하십시오.
⑮	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 푸시 를 참고하십시오.
⑯	로컬 컴퓨터	마이그레이션 후 보고서를 다운로드한 위치로 이동하여 보고서를 검토합니다. 자세한 단계는 마이그레이션 후 보고서 검토 및 마이그레이션 완료 를 참고하십시오.
⑰	Management Center	Management Center에서 Threat Defense로 마이그레이션된 구성을 구축합니다. 자세한 단계는 마이그레이션 후 보고서 검토 및 마이그레이션 완료 를 참고하십시오.

마이그레이션 사전 요건

Check Point 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 사용하는 경우 4단계로 건너뛵니다.

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 다운로드합니다.

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.

다음에 수행할 작업

[체크 포인트 컨피그레이션 파일 내보내기](#)

체크 포인트 컨피그레이션 파일 내보내기

다음에 대한 Check Point 구성을 내보낼 수 있습니다.

- [Check Point R77 구성 파일 내보내기](#)
- [Check Point r80-r82 구성 파일 내보내기](#)

Check Point r77 구성 파일 내보내기

Check Point r77 컨피그레이션 파일을 내보내려면 다음과 같이 합니다.

- [Check Point WVT\(Web Visualization Tool\)](#)를 사용하여 컨피그레이션 내보내기
- [구성 추출기를 사용하여 디바이스 구성 내보내기, 42 페이지](#)
- [내보낸 파일 압축](#)

Check Point WVT(Web Visualization Tool)를 사용하여 컨피그레이션 내보내기

프로시저

단계 1 Check Point 관리 서버에 액세스할 수 있는 워크스테이션에서 명령 프롬프트를 엽니다.

단계 2 [Check Point 포털](#)에서 Check Point 방화벽 버전에 해당하는 WVT를 다운로드합니다.

단계 3 WVT zip 파일의 압축을 풉니다.

단계 4 Check Point WVT 툴이 추출된 폴더와 동일한 루트 폴더 아래에 새 하위 폴더를 생성합니다.

단계 5 명령 프롬프트의 디렉토리를 WVT가 저장된 디렉토리로 변경하고 다음 명령을 실행합니다.

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name | -a certificate_file] [-p password] [-o output_file_path] [-t table_names] [-c | -m gateway | -l package_names] [-gr] [-go] [-w Web_Visualization_Tool_installation_directory]
```

예를 들면 다음과 같습니다.

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 172.16.0.1 -u admin -p admin123 -o Outputs
```

이러한 명령을 실행하면 총 7개의 파일이 *Outputs* 디렉토리에 생성됩니다. 여기서 각 항목은 다음을 나타냅니다.

명령	설명
C:\Web_Visualisation_Tool	WVT 툴의 루트 디렉토리입니다.
172.16.0.1	Check Point 관리 서버의 IP 주소입니다.
admin	Check Point 관리 서버의 사용자 이름입니다.
Admin123	Check Point 관리 서버의 비밀번호입니다.
출력	출력 파일을 저장할 상대 경로입니다.



참고 보안 정책 및 NAT 정책 파일의 이름은 각각 Security_Policy.xml 및 NAT_Policy.xml이어야 합니다. 파일 이름이 다를 경우 수동으로 이름을 바꿉니다.

보안 및 NAT 정책 파일이 여러 개인 경우 마이그레이션하려는 Check Point 디바이스의 Security_Policy.xml 및 NAT_Policy.xml 파일만 선택하고 유지하십시오.

다음에 수행할 작업

[FMT-CP-Config-Extractor_v2.3.4-5381](#) 툴을 사용하여 디바이스 컨피그레이션 내보내기

구성 추출기를 사용하여 디바이스 구성 내보내기

프로시저

단계 1 Select Source Configuration(소스 구성 선택) 페이지에서 **Check Point(r75-r77)**를 선택하고 **Start Migration(마이그레이션 시작)**을 클릭합니다.

단계 2 Configuration Extractor(구성 추출기) 창에서 **Connect(연결)**을 클릭하여 Secure Firewall 마이그레이션 툴을 사용하여 정책을 마이그레이션할 Check Point 보안 게이트웨이에 연결합니다.

연결하려면 다음 정보가 필요합니다.

- a) IP 주소
- b) Port(포트)
- c) 관리자 사용자 이름
- d) 관리자 비밀번호
- e) 전문가 비밀번호
- f) (선택 사항) 가상 ID 번호

단계 3 로컬 시스템에 다운로드된 networking.txt 파일이 표시될 때까지 기다립니다.

다음 명령은 구성 추출기에 의해 백그라운드에서 실행되며 networking.txt 파일로 다운로드됩니다.

- show hostname
- show version product
- show interfaces
- fw vsx stat
- show management interface
- show configuration bonding
- show configuration bridging

- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

예를 들어 172.16.0.1은 정책을 마이그레이션할 Check Point 방화벽 게이트웨이의 IP 주소입니다.

단계 4 가상 ID가 있는 Check Point VSX(Virtual System eXtension) 버전 R77에서 구성을 내보내려는 경우 다음 명령이 백그라운드에서 실행됩니다.

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **fw vsx stat <vsid>**
- **set virtual system <vsid>**



팁 vsid는 가상 시스템 ID를 나타냅니다.

- **fw getifs**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

단계 5 .txt 파일을 Outputs 폴더로 이동합니다.

다음에 수행할 작업

내보낸 파일 압축

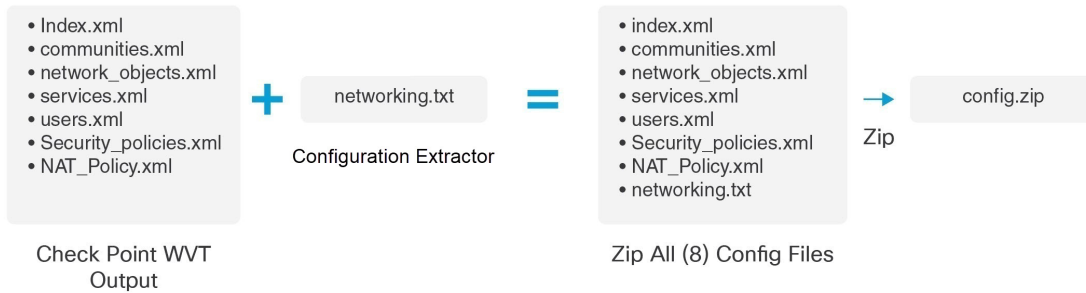
내보낸 파일 압축

프로시저

8개 파일(WVT(Web Visualization Tool)의 파일 7개와 구성 추출기의 .txt 파일 1개)을 모두 선택하고 zip 파일로 압축합니다.



참고 마이그레이션을 위해 파일을 압축하기 전에 Security_Policy.xml 및 NAT_Policy.xml 파일이 Threat Defense로 마이그레이션하려는 Check Point 디바이스용 파일인지 확인합니다.



참고 .tar 또는 기타 압축 파일 형식은 지원되지 않습니다.

다음에 수행할 작업

Check Point 컨피그레이션 파일 업로드

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, [Check Point 구성 파일 업로드](#)로 건너뛰십시오.



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, 33 페이지](#) 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.

- Check Point 컨피그레이션을 컴퓨터로 내보낸 경우 [Upload the Check Point Configuration File\(Check Point 컨피그레이션 파일 업로드\)](#)을 진행합니다.
- Secure Firewall 마이그레이션 툴을 사용하여 Check Point(r77)에서 정보를 추출해야 하는 경우 [Check Point r77 구성 파일 내보내기](#)로 진행합니다.
- Secure Firewall 마이그레이션 툴을 사용하여 Check Point(r80-r82)에서 정보를 추출해야 하는 경우 [Check Point r80-r82 구성 파일 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 또는와 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 요약を確認하고 **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.

Check Point r80-r82 구성 파일 내보내기



참고 Check Point r80-r82 구성 내보내는 Secure Firewall 마이그레이션 툴의 Live Connect 기능에서만 지원됩니다.

마이그레이션에 필요한 자격 증명을 Check Point 디바이스에 구성하고 Check Point 컨피그레이션 파일을 내보내려면 다음과 같이 합니다.

- [Live Connect를 사용한 구성 추출을 위한 Check Point\(r80-r82\) 디바이스 사전 스테이징](#)
- [Check Point r80-r82 구성 파일 내보내기 절차](#)

Live Connect를 사용한 구성 추출을 위한 Check Point(r80-r82) 디바이스 사전 스테이징



참고 Check Point 관리 센터의 명령줄(CLI)이 CLISH 모드인지 확인하십시오. 전문가 모드에 있는 경우, Live Connect를 통해 구성 내보내기를 진행하기 전에 전문가 모드를 종료하고 CLISH 모드로 전환합니다.

다음 단계 중 하나를 사용하여 마이그레이션 전에 Check Point(r80-r82) 디바이스에 자격 증명을 구성할 수 있습니다.

- [Distributed Check Point Deployment\(분산된 Check Point 구축\)](#) - 독립적인 Check Point 보안 게이트웨이 및 Check Point 보안 관리자가 있는 경우
- [Standalone Check Point Deployment\(독립형 Check Point 구축\)](#) - Check Point 보안 게이트웨이 및 Check Point 보안 관리자를 단일 디바이스로 사용하는 경우
- [Multi-Domain Check Point Deployment\(멀티 도메인 Check Point 구축\)](#) - 멀티 도메인 구축이 설정된 Check Point 보안 게이트웨이 및 Check Point 보안 관리자가 있는 경우

분산형 Check Point 구축에서 내보내기

Check Point 컨피그레이션을 추출하려면 Secure Firewall 마이그레이션 툴에서 Live Connect를 사용하기 전에 Check Point(r80-r82) 디바이스에 자격 증명을 구성해야 합니다.

분산형 Check Point 구축에서 자격 증명을 사전 스테이징하는 절차에는 다음 단계가 포함됩니다.

프로시저

단계 1 Gaia 콘솔 Check Point 보안 게이트웨이에서 다음을 생성합니다.

- a) 웹 브라우저에서 HTTPS 세션을 통해 Check Point Gaia 콘솔 애플리케이션을 열어 Check Point 보안 게이트웨이에 연결합니다.
- b) **User Management(사용자 관리)** 탭으로 이동하고 **Users(사용자) > Add(추가)**를 선택합니다.
- c) **Add User(사용자 추가)** 창에서 다음 세부 사항으로 새 사용자 이름과 비밀번호를 생성합니다.
 - **Shell(셸)** 드롭다운에서 `/etc/cli.sh`를 선택합니다.
 - **Available Roles(사용 가능한 역할)**에서 `adminRole`을 선택합니다.
 - 나머지 필드에서 기본값을 유지합니다.
 - **Ok(확인)**를 클릭합니다.
- d) Check Point 보안 게이트웨이에 SSH로 연결하고 다음 명령을 사용하여 새 비밀번호를 생성합니다.
set expert-password <password>



참고

- Check Point 디바이스에 이미 전문가 비밀번호를 구성한 경우 해당 비밀번호를 재사용합니다.
- 3단계에 표시된 대로 **Connect to Check Point Security Gateway(Check Point 보안 게이트웨이에 연결)** 페이지에서 이러한 자격 증명이 필요합니다.

전문가 비밀번호를 구성하고 나면 Check Point r80-r82 게이트웨이에 대한 자격 증명의 사전 스테이징이 완료됩니다.

자세한 내용은 [그림 3](#)을 참고하십시오.

단계 2 r80-r82용 Check Point 보안 관리자에서 사용자 이름과 비밀번호를 생성합니다.

- a) SmartConsole 애플리케이션에서 다음 단계를 수행합니다.
 1. Check Point 보안 관리자에 로그인합니다.
 2. **Manage and Settings(관리 및 설정) > Permissions and Administrators(권한 및 관리자) > Administrators(관리자)**로 이동합니다.
 3. *를 클릭하여 새 사용자 이름과 비밀번호를 만들고 다음 단계를 수행합니다.
 - **Authentication Method(인증 방법)**을 **Check Point Password(Check Point 비밀번호)**로 선택합니다.
 - 새 비밀번호를 설정하려면 **Set New Password(새 비밀번호 설정)**를 클릭합니다.



참고 **User Must Change Password on the Next Login**(사용자가 다음 로그인 시 비밀번호를 변경해야 함) 체크 박스를 선택하지 않았는지 확인합니다.

- **Permission Profile**(권한 프로파일)을 **Super User**(슈퍼 사용자)로 선택합니다.
- **Expiration**(만료)을 **Never**(사용 안 함)로 선택합니다.

4. Check Point SmartConsole 애플리케이션에서 컨피그레이션 변경 사항을 저장하려면 **Publish**(게시)를 클릭합니다.

b) Check Point 보안 관리자용 Gaia 콘솔에서 다음 단계를 수행합니다.



참고 지금 생성할 사용자 이름과 비밀번호는 SmartConsole 애플리케이션의 **2a(3) 단계**에서 생성한 것과 동일해야 합니다.

1. 웹 브라우저에서 HTTPS 세션을 통해 Gaia 콘솔 애플리케이션을 열어 Check Point 보안 관리자에 연결합니다.
2. **User Management**(사용자 관리) 탭으로 이동하고 **Users**(사용자) > **Add**(추가)를 선택합니다.
3. SmartConsole 애플리케이션의 **2a(3) 단계**에서 생성한 것과 동일한 사용자 이름과 비밀번호를 생성합니다.
 - **Shell**(셸) 드롭다운에서 **/bin/bash**를 선택합니다.
 - **Available Roles**(사용 가능한 역할) 드롭다운에서 **adminRole**을 선택합니다.
 - 나머지 필드에서 기본값을 유지합니다.
 - **Ok**(확인)를 클릭합니다.
4. Check Point 보안 관리자에 SSH로 연결하고 다음 명령을 사용하여 전문가 비밀번호를 생성합니다.
set expert-password <password>



- 참고
- 이미 전문가 비밀번호를 구성한 경우 해당 비밀번호를 사용할 수 있습니다.
 - **2a(3) 단계**와 **2b(3) 단계**에서 생성한 사용자 이름 및 비밀번호는 동일해야 합니다.

Check Point 보안 관리자용 분산형 구축에서 Check Point에 대한 자격 증명의 사전 스테이징이 완료되었습니다.

4단계에 표시된 대로 **Connect to Check Point Security Manager**(Check Point 보안 관리자에 연결) 페이지에서 이러한 자격 증명이 필요합니다.

Check Point Smart Manager에서 사용자 지정 API 포트를 사용하는 경우 [Check Point r80-r82용 사용자 지정 API 포트](#)를 참고하십시오.

다음에 수행할 작업

Check Point r80-r82 구성 파일 내보내기

독립형 Check Point 구축에서 내보내기

Check Point 컨피그레이션을 추출하려면 Secure Firewall 마이그레이션 툴에서 Live Connect를 사용하기 전에 Check Point(r80-r82) 디바이스에 자격 증명을 구성해야 합니다.

독립형 Check Point 구축에서 자격 증명을 사전 스테이징하는 절차에는 다음 단계가 포함됩니다.

프로시저

단계 1 웹 브라우저에서 HTTPS 세션을 통해 Gaia 콘솔 애플리케이션을 열어 Check Point 보안 게이트웨이 및 Check Point 보안 관리자를 모두 관리하는 독립형 Check Point 디바이스에 연결합니다.

단계 2 **User Management(사용자 관리)** 탭으로 이동하고 **Users(사용자) > Add(추가)**를 선택합니다.

a) **Add User(사용자 추가)** 창에서 다음 세부 사항으로 새 사용자 이름과 비밀번호를 생성합니다.

- **Shell(셸)** 드롭다운에서 `/etc/cli.sh`를 선택합니다.
- **Available Roles(사용 가능한 역할)** 드롭다운에서 `adminRole`을 선택합니다.
- 나머지 필드에서 기본값을 유지합니다.
- **Ok(확인)**를 클릭합니다.

3단계에 표시된 대로 **Connect to Check Point Security Gateway(Check Point 보안 게이트웨이에 연결)** 페이지에서 이러한 자격 증명이 필요합니다.

자세한 내용은 [그림 3](#)을 참고하십시오.

b) **Add User(사용자 추가)** 창에서 다음 세부 사항으로 또 다른 사용자 이름과 비밀번호를 생성합니다.

- **Shell(셸)** 드롭다운에서 `/bin/bash`를 선택합니다.
- **Available Roles(사용 가능한 역할)** 드롭다운에서 `adminRole`을 선택합니다.
- 나머지 필드에서 기본값을 유지합니다.
- **Ok(확인)**를 클릭합니다.

단계 3 Check Point 디바이스의 r80-r82용 SmartConsole 애플리케이션에서 다음을 생성합니다.



참고 지금 생성할 사용자 이름과 비밀번호가 이전 단계의 Check Point Gaia 콘솔에서 생성한 것과 동일한지 확인합니다.

- Check Point 디바이스의 SmartConsole 애플리케이션에 로그인합니다.
- Manage and Settings**(관리 및 설정) > **Permissions and Administrators**(권한 및 관리자) > **Administrators**(관리자)로 이동합니다.
- *를 클릭하여 다음 세부 사항으로 새 사용자 이름과 비밀번호를 생성합니다.
 - Authentication Method**(인증 방법)을 **Check Point Password**(Check Point 비밀번호)로 선택합니다.
 - 새 비밀번호를 설정하려면 **Set New Password**(새 비밀번호 설정)를 클릭합니다.



참고 **User Must Change Password on the Next Login**(사용자가 다음 로그인 시 비밀번호를 변경해야 함) 체크 박스를 선택하지 않았는지 확인합니다.

- Permission Profile**(권한 프로파일)을 **Super User**(슈퍼 사용자)로 선택합니다.
- Expiration**(만료)을 **Never**(사용 안 함)로 선택합니다.

2단계의 **b 단계**와 3단계의 **c 단계**에서 생성한 사용자 이름 및 비밀번호는 동일해야 합니다.

4단계에 표시된 대로 **Connect to Check Point Security Manager**(Check Point 보안 관리자에 연결) 페이지에서 이러한 자격 증명이 필요합니다.

- Check Point SmartConsole 애플리케이션에서 컨피그레이션 변경 사항을 저장하려면 **Publish**(게시)를 클릭합니다.

단계 4 Check Point 디바이스에 SSH로 연결하고 다음 명령을 사용하여 전문가 비밀번호를 생성합니다.

```
set expert-password <password>
```



- 참고
- Check Point 디바이스에 이미 전문가 비밀번호를 구성한 경우 해당 비밀번호를 재사용합니다.
 - 2단계의 **b 단계**와 3단계의 **c 단계**에서 생성한 사용자 이름 및 비밀번호는 동일해야 합니다.

독립형 구축을 위해 Check Point 디바이스에서 자격 증명의 사전 스테이징이 완료되었습니다.

Check Point Smart Manager에서 사용자 지정 API 포트를 사용하는 경우 [Check Point r80-r82용 사용자 지정 API 포트](#)를 참고하십시오.

다음에 수행할 작업

[Check Point r80-r82 구성 파일 내보내기](#)

멀티 도메인 Check Point 구축에서 내보내기

Check Point 구성을 추출하려면 Secure Firewall 마이그레이션 툴에서 Live Connect를 사용하여 Check Point(r80-r82) 디바이스에 자격 증명을 구성해야 합니다.

멀티 도메인 Check Point 구축에서 자격 증명을 사전 스테이징하는 절차에는 다음 단계가 포함됩니다.

프로시저

단계 1 Gaia 콘솔 Check Point 보안 게이트웨이에서 다음을 생성합니다.

- a) 웹 브라우저에서 HTTPS 세션을 통해 Gaia 콘솔 애플리케이션을 열어 Check Point 보안 게이트웨이에 연결합니다.
- b) **User Management(사용자 관리)** 탭으로 이동하고 **Users(사용자) > Add(추가)**를 선택합니다.
- c) **Add User(사용자 추가)** 창에서 다음 세부 사항으로 새 사용자 이름과 비밀번호를 생성합니다.
 - **Shell(셸)** 드롭다운에서 */etc/cli.sh*를 선택합니다.
 - **Available Roles(사용 가능한 역할)** 드롭다운에서 *adminRole*을 선택합니다.
 - 나머지 필드에서 기본값을 유지합니다.
 - **Ok(확인)**를 클릭합니다.
- d) Check Point 보안 게이트웨이에 SSH로 연결하고 다음 명령을 사용하여 새 비밀번호를 생성합니다.
set expert-password <password>

멀티 도메인 구축을 위해 Check Point 보안 게이트웨이에서 자격 증명의 사전 스테이징이 완료되었습니다.
- e) (선택 사항) VSX(Virtual System Extension) 디바이스에서 구성을 내보낼 때 가상 시스템 ID를 입력할 수 있도록 **Virtual System ID(가상 시스템 ID)** 확인란을 선택합니다.

그림 1: Check Point 보안 게이트웨이에 연결 - 멀티 도메인 구축



Connect to Checkpoint Security Gateway

IP Address: 10.1.1.1

Port: 22

Admin Username: admin

Admin Password: ●●●●●●●●

Expert Password: ●●●●●●●●

☒ Virtual System ID

Virtual ID Number: 2

Login

단계 2 Check Point 보안 관리자에서 사용자 이름과 비밀번호를 생성합니다.

a) SmartConsole(mds) 애플리케이션에서 다음 단계를 수행합니다.

1. Check Point 보안 관리자에 로그인합니다.
2. **Manage and Settings**(관리 및 설정) > **Permissions and Administrators**(권한 및 관리자) > **Administrators**(관리자)로 이동합니다.
3. *를 클릭하여 다음 세부 사항으로 새 사용자 이름과 비밀번호를 생성합니다.
 - **Authentication Method**(인증 방법)을 **Check Point Password**(Check Point 비밀번호)로 선택합니다.
 - 새 비밀번호를 설정하려면 **Set New Password**(새 비밀번호 설정)를 클릭합니다.



참고 **User Must Change Password on the Next Login**(사용자가 다음 로그인 시 비밀번호를 변경해야 함) 체크 박스를 선택하지 않았는지 확인합니다.

- **Permission Profile**(권한 프로파일)을 **Multi-domain Super User**(멀티 도메인 슈퍼 사용자)로 선택합니다.
- **Expiration**(만료)을 **Never**(사용 안 함)로 선택합니다.

4. Check Point SmartConsole 애플리케이션에서 컨피그레이션 변경 사항을 저장하려면 **Publish**(게시)를 클릭합니다.

Check Point Smart Manager에서 사용자 지정 API 포트를 사용하는 경우 [Check Point r80-r82용 사용자 지정 API 포트](#)를 참고하십시오.

- b) Check Point 보안 관리자용 Gaia 콘솔에서 다음 단계를 수행합니다.



참고 지금 생성할 사용자 이름과 비밀번호는 SmartConsole 애플리케이션의 [2a\(3\) 단계](#)에서 생성한 것과 동일해야 합니다.

1. 웹 브라우저에서 HTTPS 세션을 통해 Gaia 콘솔 애플리케이션을 열어 Check Point 보안 관리자에 연결합니다.
2. **User Management**(사용자 관리) 탭으로 이동하고 **Users**(사용자) > **Add**(추가)를 선택합니다.
3. SmartConsole 애플리케이션의 [2a\(3\) 단계](#)에서 생성한 것과 동일한 사용자 이름과 비밀번호를 생성합니다.
 - **Shell**(셸) 드롭다운에서 `/bin/bash`를 선택합니다.
 - **Available Roles**(사용 가능한 역할) 드롭다운에서 `adminRole`을 선택합니다.
 - 나머지 필드에서 기본값을 유지합니다.
 - **Ok**(확인)를 클릭합니다.

4. Check Point 보안 관리자에 SSH로 연결하고 다음 명령을 사용하여 새 비밀번호를 생성합니다.

set expert-password <password>



참고

- Check Point 디바이스에 이미 전문가 비밀번호를 구성한 경우 해당 비밀번호를 재사용합니다.
- [2a\(3\) 단계](#)와 [2b\(3\) 단계](#)에서 생성한 사용자 이름과 비밀번호는 동일해야 합니다.

멀티 도메인 구축을 위해 Check Point 보안 관리자에서 자격 증명의 사전 스테이징이 완료되었습니다.

[그림 2](#)와 같이 Live Connect에 연결하려면 자격 증명이 필요합니다.

그림 2: Check Point 보안 게이트웨이에 연결 - 멀티 도메인 구축



참고

- Check Point Smart Manager에서 사용자 지정 API 포트를 사용하는 경우 [Check Point r80-r82용 사용자 지정 API 포트](#)를 참고하십시오.
- 멀티 도메인 구축을 위한 전역 정책 패키지의 추출은 불가능합니다. 따라서 Check Point CMA에서 컨피그레이션의 일부로 구성된 개체, ACE 규칙 및 NAT 규칙은 내보내기 및 마이그레이션만 가능합니다.

다음에 수행할 작업

[Check Point r80-r82 구성 파일 내보내기](#)

Check Point(r80-r82) 보안 관리자에 사용자 지정 API 포트를 사용합니까?



참고 Check Point Smart Manager에서 사용자 지정 API 포트를 사용하는 경우 다음 단계를 수행합니다.

- Live Connect의 **Check Point Security Manager(Check Point 보안 관리자)** 페이지에서 **Check Point Multi-Domain Deployment(Check Point 멀티 도메인 구축)** 체크 박스를 선택합니다.
- 멀티 도메인 구축을 사용하는 경우 Check Point CMA의 IP 주소와 API 포트 세부 정보를 추가합니다.
- 일반 구축인 경우 Check Point 보안 관리자의 IP 주소를 유지하고 사용자 지정 API 포트의 세부 정보를 입력합니다.

Check Point r80-r82 구성 파일 내보내기 절차

시작하기 전에

Check Point 디바이스를 사전에 스테이징해야 합니다. 마이그레이션 전에 Check Point(r80-r82) 디바이스에서 자격 증명을 구성하는 방법에 대한 자세한 내용은 [Live Connect를 사용한 컨피그레이션 추출을 위한 Check Point\(r80-r82\) 디바이스 사전 스테이징](#)을 참고하십시오.



- 참고
- Check Point(r80-r82) 컨피그레이션을 추출하려면 Live Connect를 사용하는 것이 좋습니다.
 - Secure Firewall 마이그레이션 툴에서 Live Connect를 통해 내보내지 않은 Check Point(r80-r82) 구성을 사용하면 구성이 지원되지 않는 상태로 마이그레이션되거나, 부분적으로 마이그레이션되거나, 마이그레이션에 실패하게 됩니다.
- 컨피그레이션 내보내기의 정보가 불완전한 경우, 특정 컨피그레이션은 마이그레이션되지 않으며 지원되지 않는 것으로 표시됩니다.

Check Point r80-r82 컨피그레이션 파일을 내보내려면 다음과 같이 합니다.

프로시저

단계 **1 Select Source Config**(소스 구성 선택) 페이지에서 Check Point(r80-r82)를 선택합니다.

단계 **2 Connect**(연결)를 클릭합니다.



참고 Live Connect는 Check Point(r80-r82)에만 사용할 수 있습니다.

단계 **3** Check Point 보안 게이트웨이에 연결합니다. 다음을 수행하십시오.

a) Check Point r80-r82 보안 게이트웨이에 다음을 입력합니다.

- IP 주소
- SSH Port(SSH 포트)
- 관리자 사용자 이름
- 관리자 비밀번호
- 전문가 비밀번호

그림 3: Check Point 보안 게이트웨이에 연결

The screenshot shows a 'Connect to Checkpoint Security Gateway' window. At the top, there are three numbered steps: 1 (active), 2, and 3. Below the title, there are input fields for 'IP Address' (containing '10.10.1.1'), 'Port' (containing '22'), 'Admin Username' (containing 'admin'), 'Admin Password' (masked with asterisks), and 'Expert Password' (masked with asterisks). A blue 'Login' button is located at the bottom center of the dialog.

b) **Login**(로그인)을 클릭합니다.

Secure Firewall 마이그레이션 툴은 인터페이스 및 경로 구성과 같은 디바이스별 구성이 포함된 *network.txt* 파일을 생성합니다. Secure Firewall 마이그레이션 툴의 현재 세션에 대한 로컬 디렉터리에 *networking.txt* 파일을 저장합니다.

단계 4 Check Point 보안 관리자에 연결합니다. 다음을 수행하십시오.

a) Check Point r80-r82 보안 관리자에 다음을 입력합니다.

- IP 주소
- SSH Port(SSH 포트)
- Smart 콘솔 사용자 이름
- Smart 콘솔 비밀번호
- 전문가 비밀번호

그림 4: Check Point 보안 관리자에 연결

b) **Login**(로그인)을 클릭합니다.

Secure Firewall 마이그레이션 툴은 Check Point 보안 관리자에서 사용 가능한 전체 네트워크 및 서비스 개체 구성을 캡처하는 *Extracted-objects.json* 파일을 생성합니다.

Secure Firewall 마이그레이션 툴의 현재 세션에 대한 로컬 디렉터리에 *Extracted-objects.json*을 저장합니다.



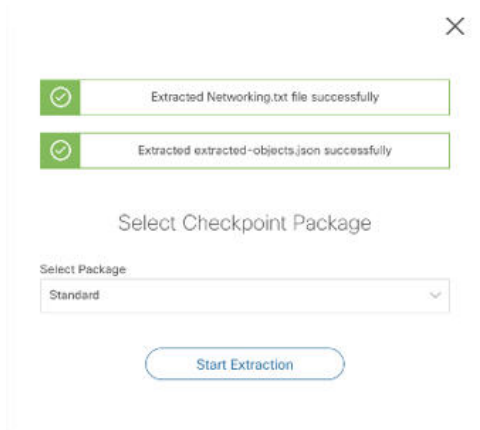
참고

Secure Firewall 마이그레이션 툴을 Check Point 보안 관리자에 연결한 경우 Check Point 보안 관리자에서 사용 가능한 정책 패키지 목록이 표시됩니다.

단계 5 Select Check Point Package(Check Point 패키지 선택) 목록에서 마이그레이션할 Check Point 정책 패키지를 선택하고 **Start Extraction**(추출 시작)을 클릭합니다.

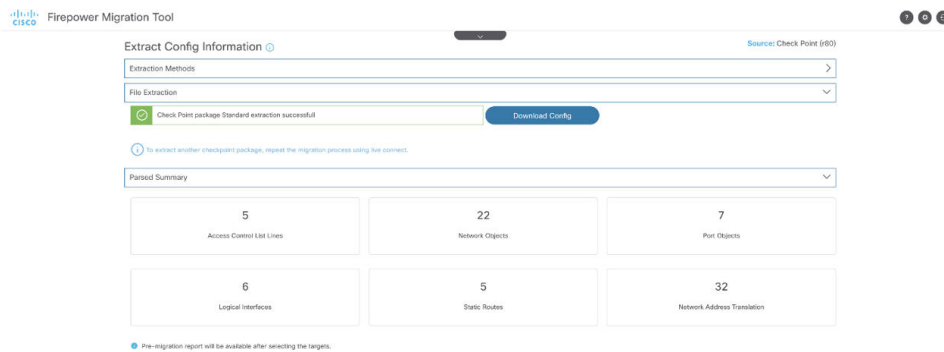
다른 구성 파일 추출

그림 5: Check Point 정책 패키지 추출



단계 6 컨피그레이션을 다운로드하고 마이그레이션을 진행합니다.

그림 6: 분산형 및 독립형 구축을 위한 Check Point 컨피그레이션 추출 완료



단계 7 Check Point(r80-r82) 컨피그레이션을 계속 진행하려면 **Next(다음)**를 클릭합니다.

다음에 수행할 작업

Check Point 컨피그레이션 파일 업로드

다른 구성 파일 추출

다른 구성 파일을 추출하려면 다음 단계를 수행하십시오.

- **Back to source selection**(소스 선택으로 돌아가기)를 클릭하여 다른 정책 패키지에 대한 새 구성을 추출하거나 다른 Check Point(r80-r82) 방화벽에 연결합니다.
- 추출된 Check Point(r80-r82) 구성을 나중에 마이그레이션해야 하는 경우 현재 구성을 다운로드합니다.



참고 현재 구성 파일이 브라우저에서 설정한 기본 다운로드 위치에 다운로드됩니다.

조립 라인 접근 방식을 사용하여 r80-r82 구성을 추출할 수 있습니다.

- 라이브 연결을 수행하여 방화벽의 각 패키지 또는 다른 방화벽에 대한 Check Point(r80-r82) 설정 파일을 추출합니다.
- 여러 구성을 위한 저장소를 생성합니다.
- 나중에 마이그레이션을 진행하려면 수동 업로드를 사용하는 나중에 마이그레이션 시작 옵션을 사용합니다.

Check Point 컨피그레이션 파일 업로드

시작하기 전에

컨피그레이션 파일을 .zip 형식으로 내보냅니다.

프로시저

단계 1 **Extract Config Information**(컨피그레이션 정보 추출) 화면의 **Manual Upload**(수동 업로드) 섹션에서 **Upload**(업로드)를 클릭하여 Check Point 컨피그레이션 파일을 업로드합니다.

단계 2 컨피그레이션 파일이 저장된 위치로 이동합니다. 컨피그레이션 파일은 Check Point(r77) 용으로 추출되고 Live Connect를 사용하여 Check Point(r80-r82)용으로 다운로드됩니다. **Open**(열기)을 클릭하십시오.

Secure Firewall 마이그레이션 툴이 구성 파일을 업로드합니다. 대규모 컨피그레이션 파일의 경우 이 단계는 시간이 더 오래 걸립니다.

이제 사전 구문 분석 프로세스가 완료되었습니다.

Parsed Summary(구문 분석 요약) 섹션에 구문 분석 상태가 표시됩니다.

단계 3 업로드된 컨피그레이션 파일에서 Secure Firewall 마이그레이션 툴이 감지하고 구문 분석한 요소에 대한 요약을 검토합니다.

단계 4 **Next**(다음)를 클릭하여 대상 매개변수를 선택합니다.

다음에 수행할 작업

[마이그레이션 툴의 대상 매개변수 지정](#)

Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정

시작하기 전에

Security Cloud Control에서 호스팅되는 마이그레이션 툴의 클라우드 버전을 사용하는 경우 **3단계**로 건너뛰니다.

- 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.

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

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

- Connect**(연결)를 클릭하고 **2단계**로 진행합니다.

- 클라우드 제공 Firewall Management Center로 마이그레이션하려면 다음을 수행합니다.

- Cloud** 사용 **FMC** 라디오 버튼을 클릭합니다.
- 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 Check Point 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 Check Point 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. Check Point 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 Check Point 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 Check Point 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 Check Point 구성에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.
- Check Point의 경우 **Shared Configuration**(공유 컨피그레이션)에서 관련 **Access Control**(액세스 제어) 옵션을 선택합니다.
 - 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 NAT는 고려되지 않음)로 제한되며, 소스 및 대상 네트워크 개체 그룹의 특성에 따라 이 작업으로 인해 규칙이 급증할 수 있습니다.

라우팅 정보는 `networking.txt` 파일에서 가져옵니다. 이 파일은 `netstat -rnv` 명령을 사용하여 라우팅 테이블을 수집하는

FMT-CP-Config-Extractor_v4.0.1-8248 툴의 출력입니다. 자세한 내용은 [FMT-CP-Config-Extractor_v4.0.1-8248 툴을 사용하여 디바이스 컨피그레이션 내보내기](#)를 참고하십시오.

영역 기반 정책에 대한 IPv6 경로 조회는 이 릴리스에서 지원되지 않습니다. 전역 정책 또는 영역 기반 정책의 모든 규칙이 성공적으로 마이그레이션되었는지 확인합니다.

Device Configuration(디바이스 구성)에서 Check Point 방화벽에서 마이그레이션할 인터페이스, 경로, 사이트 간 VPN 터널 구성을 선택합니다. 정책 기반(암호화 맵) 사이트 간 VPN 터널 구성만 마이그레이션할 수 있습니다.

- (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 Check Point 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 요약을 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.

다음에 수행할 작업

[마이그레이션 전 보고서 검토, 65 페이지](#)

마이그레이션 전 보고서 검토

프로시저

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

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.



참고 마이그레이션 전 보고서의 각 표에는 30개의 항목이 표시됩니다. 항목이 30개 이상인 경우, 표 오른쪽 상단의 아이콘을 클릭하여 CSV 파일을 다운로드해야 합니다.

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

- **Overall Summary**(전반적인 요약) - Firepower Threat Defense로 성공적으로 마이그레이션할 수 있는 지원 Check Point 구성 요소의 전체 요약입니다. 예를 들면 Policy Names(정책 이름), Rule Counts(규칙 수) 등이 있습니다.
- **Configuration Lines with Errors**(오류가 있는 구성 라인) — 마이그레이션 툴의 구문 분석 문제로 인해 성공적으로 마이그레이션되지 못한 Check Point 구성 요소에 대한 정보입니다. 마이그레이션을 진행하기 전에 Check Point 디바이스에서 이러한 오류를 수정하고, 새로운 구성 파일을 생성한 다음, 이 파일을 마이그레이션 툴로 업로드합니다.
- **Ignored Configuration**(무시된 구성) - 마이그레이션 중에 FMT에서 무시되고 대상 시스템으로 전달되지 않는 모든 Check Point 구성 요소 목록입니다.

Firewall Management Center 및 Firewall Threat Defense에서 지원되는 기능에 대한 자세한 내용은 [Firepower Management Center 구성 가이드](#)를 참고하십시오.

단계 3 **Pre-Migration Report**(마이그레이션 전 보고서)에서 시정 조치를 권장하는 경우, 계속하기 전에 Check Point에서 수정 작업을 완료하고 Check Point 구성 파일을 다시 내보낸 다음 업데이트된 구성 파일을 업로드하십시오.

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

Check Point Firewall 구성과 Firewall Threat Defense 인터페이스 매핑

Firewall Threat Defense 디바이스에는 Check Point 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.

Map FTD Interface(FTD 인터페이스 매핑) 화면에서 Secure Firewall 마이그레이션 툴로 Firewall Threat Defense 디바이스의 인터페이스 목록을 검색합니다. 기본적으로 Secure Firewall 마이그레이션 툴은 인터페이스 ID에 따라 Check Point의 인터페이스와 Firewall Threat Defense 디바이스를 매핑합니다. 예를 들어, Check Point 인터페이스의 '관리 전용' 인터페이스는 Firewall Threat Defense 디바이스의 '관리 전용' 인터페이스에 자동으로 매핑되며 이를 변경할 수 없습니다.

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

- 대상 Firewall Threat Defense가 네이티브 유형인 경우:
 - Firewall Threat Defense에서 같거나 더 많은 수의 Check Point 인터페이스 또는 PC(Port Channel) 데이터 인터페이스(Check Point 구성의 관리 전용 및 하위 인터페이스 제외)를 사용해야 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 Check Point 인터페이스, 물리적 하위 인터페이스, 포트 채널 또는 포트 채널 하위 인터페이스(Check Point 구성의 관리 전용 인터페이스 제외)를 사용해야 합니다.

스 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 Check Point 보다 100개 적을 경우 대상 Firewall Threat Defense에서 추가 물리적 인터페이스 또는 물리적 하위 인터페이스를 생성할 수 있습니다.

- 하위 인터페이스는 Secure Firewall 마이그레이션 툴로 생성되지 않습니다. 물리적 인터페이스, 포트 채널 또는 하위 인터페이스 간의 인터페이스 매핑만 허용됩니다.

시작하기 전에

Firewall Management Center에 연결하고 대상을 Firewall Threat Defense로 선택했는지 확인합니다. 자세한 내용은 [Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 62 페이지](#)를 참조하십시오.



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 Check Point 인터페이스에 매핑할 인터페이스를 선택합니다.

관리 인터페이스의 매핑은 변경할 수 없습니다. Firewall Threat Defense 인터페이스가 Check Point 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 Check Point 구성의 모든 하위 인터페이스에 대해 Firewall Threat Defense 디바이스의 하위 인터페이스를 매핑합니다.

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

다음에 수행할 작업

Check Point 인터페이스를 적절한 Firewall Threat Defense 인터페이스 개체, 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 내용은 [보안 영역 및 인터페이스 그룹에 Check Point 인터페이스 매핑](#)을 참조하십시오.

Check Point 인터페이스를 보안 영역 및 인터페이스 그룹에 매핑

Check Point 구성이 올바르게 마이그레이션되도록 하려면 Check Point 인터페이스를 적절한 Firewall Threat Defense 인터페이스 개체, 보안 영역과 인터페이스 그룹에 매핑합니다. Check Point 구성에서 액세스 제어 정책 및 NAT 정책은 인터페이스 이름(nameif)을 사용합니다. Firewall Management Center

에서 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.
- 인터페이스 그룹 — 하나의 인터페이스가 여러 인터페이스 그룹에 속할 수 있습니다.

Secure Firewall 마이그레이션 툴을 사용하면 보안 영역 및 인터페이스 그룹이 있는 인터페이스를 일대일로 매핑할 수 있습니다. 보안 영역 또는 인터페이스 그룹이 인터페이스에 매핑된 경우 Firewall Management Center에서 허용하더라도 다른 인터페이스에 매핑할 수 없습니다. Firewall Management Center의 보안 영역 및 인터페이스 그룹에 대한 자세한 내용은 *Cisco Secure Firewall Management Center* 디바이스 환경 설정 설명서 의 에서 [보안 영역 및 인터페이스 그룹](#)을 참조하십시오.

프로시저

- 단계 1 Map Security Zones and Interface Groups(보안 영역 및 인터페이스 그룹 매핑)** 화면에서 사용 가능한 인터페이스, 보안 영역 및 인터페이스 그룹을 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.
 - Security Zones(보안 영역)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.
 - Interface Groups(인터페이스 그룹)** 열에서 해당 인터페이스의 인터페이스 그룹을 선택합니다.
- 단계 3** Firewall Management Center에 존재하는, 즉 Check Point(r80-r82) 구성 파일에서 보안 영역 유형 개체로 사용 가능하고 드롭다운 목록에서 사용 가능한 보안 영역 및 인터페이스 그룹에 인터페이스를 매핑하려면 다음과 같이 합니다.
 - Security Zones(보안 영역)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.
 - Interface Groups(인터페이스 그룹)** 열에서 해당 인터페이스의 인터페이스 그룹을 선택합니다.
- 단계 4** 보안 영역 및 인터페이스 그룹을 수동으로 매핑하거나 자동으로 생성할 수 있습니다.
- 단계 5** 보안 영역 및 인터페이스 그룹을 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 영역 또는 인터페이스 그룹을 추가합니다.
- Security Zone(보안 영역)** 열에 보안 영역 이름을 입력합니다. 허용되는 최대 문자 수는 48자입니다. 마찬가지로 인터페이스 그룹을 추가할 수 있습니다.
- Close(닫기)**를 클릭합니다.

자동 생성을 통해 보안 영역 및 인터페이스 그룹을 매핑하려면 다음과 같이 합니다.

- Auto-Create(자동 생성)**를 클릭합니다.
- Auto-Create(자동 생성)** 대화 상자에서 **Interface Groups(인터페이스 그룹)** 및 **Zone Mapping(영역 매핑)** 중 하나 또는 둘 다를 선택합니다.
- Auto-Create(자동 생성)**를 클릭합니다.

Secure Firewall 마이그레이션 툴은 이러한 보안 영역에 Check Point 인터페이스와 같은 이름(예: **outside(외부)** 또는 **inside(내부)**)을 지정하고 이름 뒤에 "(A)"를 표시하여 Secure Firewall 마이그레이션 툴에서 생성되었음을 나타냅니다. 인터페이스 그룹에는 **outside_ig** 또는 **inside_ig**와 같은 **_ig** 접미사가 추가됩니다. 또한 보안 영역 및 인터페이스

스 그룹은 Check Point 인터페이스와 동일한 모드를 사용합니다. 예를 들어 Check Point 논리적 인터페이스가 L3 모드인 경우 인터페이스에 대해 생성된 보안 영역 및 인터페이스 그룹도 L3 모드입니다.

단계 6 모든 인터페이스를 적절한 보안 영역 및 인터페이스 그룹에 매핑했으면 **Next(다음)**를 클릭합니다.

최적화, 구성 검토 및 검증

마이그레이션된 Check Point 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 툴을 닫으면 진행 상황이 저장되고 나중에 마이그레이션을 재개할 수 있습니다. 이 화면 전에 Secure Firewall 마이그레이션 툴을 닫으면 진행 상황이 저장되지 않습니다. 구문 분석 후 오류가 발생한 경우 Secure Firewall 마이그레이션 툴을 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 Check Point 에 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.

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 Firewall Management Center에 있는 경우 중복 개체를 생성하는 대신 정책이 재사용됩니다.
- 일치하지 않는 개체 - 이름은 비슷하지만 콘텐츠가 다른 개체가 있는 경우 마이그레이션 푸시 전에 Secure Firewall 마이그레이션 툴에서 개체 이름을 수정합니다.

프로시저

단계 1 (선택 사항) **Optimize, Review and Validate Configuration**(구성 최적화, 검토 및 검증) 화면에서 **Access Control**(액세스 제어) > **ACP**의 **Optimize ACL**(ACL 최적화)을 클릭하여 최적화 코드를 실행하고 다음을 수행합니다.

- a) 식별된 ACL 최적화 규칙을 다운로드하려면 **Download Report**(보고서 다운로드)를 클릭합니다.
- b) 규칙을 선택하고 **Actions**(작업) > **Migrate as disabled**(비활성화된 항목으로 마이그레이션) 또는 **Do not migration**(마이그레이션하지 않음)을 선택하고 작업 중 하나를 적용합니다.
- c) **Save**(저장)를 클릭합니다.
마이그레이션 작업이 **Do not migrate**(마이그레이션하지 않음)에서 **disabled**(비활성화됨)로 또는 그 반대로 변경됩니다.

다음 옵션을 사용하여 규칙의 대량 선택을 수행할 수 있습니다.

- **Migrate**(마이그레이션) - 기본 상태로 마이그레이션합니다.
- **Do not Migrate**(마이그레이션 안 함) - ACL 마이그레이션을 무시합니다.
- **Migrate as disabled**(비활성화된 상태로 마이그레이션) - **State**(상태) 필드가 **Disable**(비활성화)로 설정된 ACL을 마이그레이션합니다.
- **Migrate as enabled**(활성화된 상태로 마이그레이션) - **State**(상태) 필드가 **Enable**(활성화)로 설정된 ACL을 마이그레이션합니다.

단계 2 **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.

마이그레이션된 액세스 정책 규칙은 ACL 이름을 접두사로 사용하고 ACL 규칙 번호를 추가하므로 Check Point 컨피그레이션 파일에 다시 쉽게 매핑할 수 있습니다. 예를 들어 Check Point ACL의 이름이 "inside_access"인 경우 ACL의 첫 번째 규칙(또는 ACE) 라인은 "inside_access_# 1"로 지정됩니다. TCP 또는 UDP 조합, 확장된 서비스 개체 또는 기타 사유로 인해 규칙을 확장해야 하는 경우 Secure Firewall 마이그레이션 툴이 이름에 번호가 지정된 접미사를 추가합니다. 예를 들어 허용 규칙이 마이그레이션을 위해 두 개의 규칙으로 확장되는 경우 이름이 "inside_access_#1-1" 및 "inside_access_#1-2"로 지정됩니다.

지원되지 않는 개체를 포함하는 규칙의 경우 Secure Firewall 마이그레이션 툴이 이름에 "_UNSUPPORTED" 접미사를 추가합니다.

- 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 푸시됩니다.

단계 3 다음 탭을 클릭하고 컨피그레이션 항목을 검토합니다.

- 액세스 제어
- 개체(네트워크 개체, 포트 개체, VPN 개체)
- NAT
- 인터페이스
- 경로
- 사이트 간 VPN 터널

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

단계 8 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 9 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 10 **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 11 검증이 완료되고 **Validation Status(검증 상태)** 대화 상자에 **Successfully Validated(검증 성공)** 메시지가 표시되면 마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시, 74 페이지로 진행합니다.

마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시

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

마이그레이션 프로세스의 이 단계에서는 마이그레이션된 컨피그레이션을 Firewall Management Center에 보냅니다. Firewall Threat Defense 디바이스에 컨피그레이션이 구축되지는 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 Check Point 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.

Check Point에 대한 마이그레이션 후 보고서 검토 및 마이그레이션 완료

프로시저

단계 1 마이그레이션 후 보고서를 다운로드한 위치로 이동합니다.

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



참고 마이그레이션 전 보고서의 각 표에는 30개의 항목이 표시됩니다. 항목이 30개 이상인 경우, 표 오른쪽 상단의 아이콘을 클릭하여 CSV 파일을 다운로드해야 합니다.

- **Migration Summary**(마이그레이션 요약) - Check Point에서 Firepower Threat Defense로 성공적으로 마이그레이션된 구성의 요약입니다.
또한 마이그레이션 전과 마이그레이션 후의 상태 차이를 보여주는 비교 차트를 확인할 수 있습니다.
- **Selective Policy Migration**(선택적 정책 마이그레이션) - 마이그레이션 및 인터페이스 매핑을 위해 선택한 특정 Check Point 기능의 세부 정보를 확인할 수 있습니다.

• **Migration Conversions**(마이그레이션 변환) - 다음을 포함하는 변환 및 푸시 세부 정보입니다.

- 네트워크/서비스 개체 처리
- 이유가 포함된 부분적으로 마이그레이션된 구성 목록
- 이유가 포함된 지원되지 않는 구성 목록
- 확장된 액세스 제어 규칙

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: Check Point 를 Threat Defense 2100으로



참고

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

- [유지 보수 기간 작업별](#)
- [유지 보수 기간 작업, 79 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 Check Point 웹 시각화 툴 및 FMT-CP-Config-Extractor_v4.0.1-8248 툴을 사용하여 마이그레이션하려는 Check Point 디바이스 컨피그레이션을 수집하고 Check Point 컨피그레이션 파일의 사본을 저장합니다.
- 단계 2 Check Point 컨피그레이션 zip 파일을 검토합니다.
- 단계 3 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 4 Firewall Management Center에서 관리할 Firepower 2100 Series 디바이스를 등록합니다.
자세한 내용은 [Management Center에 디바이스 추가](#)를 참고하십시오.
- 단계 5 (선택 사항) 소스 Check Point 컨피그레이션에 결합 인터페이스가 있는 경우 대상 Firepower 2100 Series 디바이스에서 포트 채널(EtherChannels)을 생성합니다.
자세한 내용은 [EtherChannel 및 이중 인터페이스 구성](#)을 참고하십시오.
- 단계 6 <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, 40 페이지](#)을 참고하십시오.
- 단계 7 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, 62 페이지](#)을 참고하십시오.
- 단계 8 Check Point 인터페이스와 Firewall Threat Defense 인터페이스를 매핑합니다.



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

예를 들어 Check Point의 결합 인터페이스를 Firewall Threat Defense의 물리적 인터페이스에 매핑할 수 있습니다.
자세한 내용은 [Threat Defense 인터페이스와 Check Point 인터페이스 매핑](#)을 참고하십시오.

단계 9 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 Check Point 논리적 인터페이스를 보안 영역에 수동으로 매핑합니다.

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

단계 10 이 가이드의 지침에 따라 마이그레이션할 컨피그레이션을 순차적으로 검토 및 검증한 다음 컨피그레이션을 Firewall Management Center로 푸시합니다.

단계 11 마이그레이션 후 보고서를 검토하고 Firewall Threat Defense에 다른 컨피그레이션을 수동으로 설정하고 구축한 다음 마이그레이션을 완료합니다.

자세한 내용은 [Check Point에 대한 마이그레이션 후 보고서 검토 및 마이그레이션 완료, 76 페이지](#)를 참고하십시오.

단계 12 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, 78 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 Gaia 콘솔을 통해 Check Point 보안 게이트웨이에 연결합니다.

단계 2 Gaia 콘솔을 통해 원하는 보안 게이트웨이의 Check Point 인터페이스를 선택합니다.

단계 3 (선택 사항) Firewall Management Center에 액세스하고 Firepower 2100 Series 디바이스에 대해 Secure Firewall 마이그레이션 툴로 마이그레이션되지 않아 수동으로 마이그레이션해야 하는 유동 라우팅, 플랫폼 설정 및 기타 기능을 구성합니다.

단계 4 주변 스위칭 인프라에서 ARP(Address Resolution Protocol) 캐시를 지웁니다.

단계 5 주변 스위칭 인프라에서 Firepower 2100 Series 디바이스 인터페이스 IP 주소에 대한 기본 ping 테스트를 수행하여 액세스 가능한지 확인합니다.

단계 6 레이어 3 라우팅이 필요한 디바이스에서 Firepower 2100 Series 디바이스 인터페이스 IP 주소에 대한 기본 ping 테스트를 수행합니다.

단계 7 Firepower 2100 Series 디바이스에 새 IP 주소를 할당하고 Check Point에 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 8 Firepower 2100 디바이스에 대해 관리 Firewall Management Center 내에서 포괄적인 테스트 계획을 실행하고 로그를 모니터링합니다.



CHAPTER 3

Cisco Success Network - 텔레메트리 데이터

• Cisco Success Network - 텔레메트리 데이터, 81 페이지

Cisco Success Network - 텔레메트리 데이터

Cisco Success Network는 Secure Firewall 마이그레이션 툴에서 상시 사용 정보 및 메트릭 수집 기능으로, 마이그레이션 툴과 Cisco cloud 간의 보안 클라우드 연결을 통해 사용량 통계를 수집하고 전송합니다. 이러한 통계는 사용되지 않은 기능에 대한 추가 지원을 제공하고 제품을 개선하는 데 도움이 됩니다. Secure Firewall 마이그레이션 툴에서 마이그레이션 프로세스를 시작할 때 해당 텔레메트리 데이터 파일이 생성되고 정해진 위치에 저장됩니다.

마이그레이션된 Check Point 구성을 Firewall Management Center 또는 Multicloud Defense로 푸시하면 푸시 서비스가 해당 위치에서 텔레메트리 데이터 파일을 읽고 데이터가 클라우드에 성공적으로 업로드된 후 이 파일을 삭제합니다.

마이그레이션 툴은 스트리밍 텔레메트리 데이터에 대해 선택할 수 있는 두 가지 옵션 - **Limited**(제한적) 및 **Extensive**(확장)를 제공합니다.

Cisco Success Network를 **Limited**(제한적)로 설정하면 다음 텔레메트리 데이터 포인트가 수집됩니다.

표 2: 제한된 텔레메트리

데이터 포인트	설명	예제 값
시간	텔레메트리 데이터가 수집되는 시간 및 날짜	2025-04-11 14:17:24
Source Type(소스 유형)	소스 디바이스 유형	Check Point
Source Device Version(소스 디바이스 버전)	Check Point 디바이스의 버전	r81.20
소스 버전	Check Point의 버전	r81

데이터 포인트	설명	예제 값
Target Management Version(대상 관리 버전)	Management Center의 대상 버전	6.23 이상
Target Management Type(대상 관리 유형)	대상 매니지드 디바이스, 즉 Management Center의 유형	Management Center
Target Device Version(대상 디바이스 버전)	대상 디바이스의 버전	7.6
Target Device Model(대상 디바이스 모델)	대상 디바이스의 모델	Cisco Secure Firewall 3105 Threat Defense
Migration Tool Version(마이그레이션 툴 버전)	마이그레이션 툴의 버전	7.7-12208
Migration Status(마이그레이션 상태)	Management Center로의 Check Point 구성 마이그레이션 상태	성공

다음 표는 **Cisco Success Network**가 **Extensive(확장)**로 설정된 경우 텔레메트리 데이터 포인트에 대한 정보, 설명 및 샘플 값을 제공합니다.

표 3: 광범위한 텔레메트리

데이터 포인트	설명	예제 값
운영 체제	Secure Firewall 마이그레이션 툴을 실행하는 운영체제입니다. Windows7/Windows10 64비트/macOS High Sierra일 수 있습니다.	Windows 7
브라우저	Secure Firewall 마이그레이션 툴을 실행하는 데 사용되는 브라우저입니다. Mozilla/5.0 또는 Chrome/68.0.3440.106 또는 Safari/537.36일 수 있습니다.	Mozilla/5.0

표 4: 소스 Check Point 정보

데이터 포인트	설명	예제 값
시간	텔레메트리 데이터가 수집되는 시간 및 날짜	2023-04-25 10:39:19
Source Type(소스 유형)	소스 디바이스 유형	Check Point
Source Device Serial Number(소스 디바이스 일련 번호)	Check Point의 일련 번호	디바이스의 일련 번호(있는 경우)
Source Device Model Number(소스 디바이스 모델 번호)	Check Point의 모델 번호	
Source Device Version(소스 디바이스 버전)	Check Point의 버전	R77.30

데이터 포인트	설명	예제 값
Source Config Counts(소스 컨피그레이션 수)	소스 컨피그레이션의 총 라인 수	504
방화벽 모드	Check Point에 구성된 방화벽 모드(라우팅 또는 투명)	ROUTED
Context Mode(상황 모드)	Check Point의 컨텍스트 모드. 단일 컨텍스트 또는 멀티 컨텍스트일 수 있습니다.	SINGLE
Check Point 컨피그레이션 통계:		
ACL Counts(ACL 수)	액세스 그룹에 연결된 ACL의 수	46
Access Rules Counts(액세스 규칙 수)	액세스 규칙의 총 수	46
NAT Rule Counts(NAT 규칙 수)	NAT 규칙의 총 수	17
Network Object Counts(네트워크 개체 수)	Check Point에 구성된 네트워크 개체의 수	34
Network Object Group Counts(네트워크 개체 그룹 수)	Check Point의 네트워크 개체 그룹 수	6
Port Object Counts(포트 개체 수)	포트 개체의 수	85
Port Object Group Counts(포트 개체 그룹 수)	포트 개체 그룹의 수	37
Unsupported Access Rules Count(지원되지 않는 액세스 규칙 수)	지원되지 않는 액세스 규칙의 총 수	3
Unsupported NAT Rule Count(지원되지 않는 NAT 규칙 수)	지원되지 않는 NAT 액세스 규칙의 총 수	0
FQDN Based Access Rule Counts(FQDN 기반 액세스 규칙 수)	FQDN 기반 액세스 규칙의 수	7
Time range Based Access Rule Counts(시간 범위 기반 액세스 규칙 수)	시간 범위 기반 액세스 규칙의 수	1
SGT Based Access Rule Counts(SGT 기반 액세스 규칙 수)	SGT 기반 액세스 규칙의 수	0
툴에서 구문 분석할 수 없는 컨피그레이션 라인 요약		
Unparsed Config Count(구문 분석되지 않은 컨피그레이션 수)	파서에서 인식할 수 없는 컨피그레이션 라인의 수	68

데이터 포인트	설명	예제 값
Total Unparsed Access Rule Counts(구문 분석되지 않은 총 액세스 규칙 수)	구문 분석되지 않은 액세스 규칙의 총 수	3

표 5: 대상 매니지드 디바이스(Firewall Management Center) 정보

데이터 포인트	설명	예제 값
Target Management Version(대상 관리 버전)	Firewall Management Center의 대상 버전	6.2.3.3(빌드 76)
Target Management Type(대상 관리 유형)	대상 매니지드 디바이스의 유형, 즉 Firewall Management Center	Management Center
Target Device Version(대상 디바이스 버전)	대상 디바이스의 버전	75
Target Device Model(대상 디바이스 모델)	대상 디바이스의 모델	VMware용 Cisco Secure Firewall Threat Defense
Migration Tool Version(마이그레이션 툴 버전)	마이그레이션 툴의 버전	1.1.0.1912

표 6: 마이그레이션 요약

데이터 포인트	설명	예제 값
액세스 제어 정책		
Name(이름)	액세스 제어 정책의 이름	Doesn't Exist
Access Rule Counts(액세스 규칙 수)	마이그레이션된 ACL 규칙의 총 수	0
Partially Migrated ACL Rule Counts(부분적으로 마이그레이션된 ACL 규칙 수)	부분적으로 마이그레이션된 ACL 규칙의 총 수	3
Expanded ACP Rule Counts(확장 ACP 규칙 수)	확장 ACP 규칙의 수	0
NAT 정책		
Name(이름)	NAT 정책의 이름	Doesn't Exist
NAT Rule Counts(NAT 규칙 수)	마이그레이션된 NAT 규칙의 총 개수	0
Partially Migrated NAT Rule Counts(부분적으로 마이그레이션된 NAT 규칙 수)	부분적으로 마이그레이션된 NAT 규칙의 총 수	0
추가 마이그레이션 세부 정보...		

데이터 포인트	설명	예제 값
Interface Counts(인터페이스 수)	업데이트된 인터페이스의 수	0
Sub Interface Counts(하위 인터페이스 수)	업데이트된 하위 인터페이스의 수	0
Static Routes Counts(정적 경로 수)	정적 경로의 수	0
Objects Counts(개체 수)	생성된 개체의 수	34
Object Group Counts(개체 그룹 수)	생성된 개체 그룹의 수	6
Interface Group Counts(인터페이스 그룹 수)	생성된 인터페이스 그룹의 수	0
Security Zone Counts(보안 영역 수)	생성된 보안 영역의 수	3
Network Object Reused Counts(재사용 네트워크 개체 수)	재사용된 개체의 수	21
Network Object Rename Counts(이름 변경 네트워크 개체 수)	이름이 변경된 개체의 수	1
Port Object Reused Counts(재사용 포트 개체 수)	재사용된 포트 개체의 수	0
Port Object Rename Counts(이름 변경 포트 개체 수)	이름이 변경된 포트 개체의 수	0

표 7: **Secure Firewall** 마이그레이션 툴 성능 데이터

데이터 포인트	설명	예제 값
Conversion Time(변환 시간)	Check Point 컨피그레이션 라인을 구문 분석하는 데 소요된 시간(분)	14
Migration Time(마이그레이션 시간)	전체 마이그레이션에 소요된 총 시간(분)	592
Config Push Time(컨피그레이션 푸시 시간)	최종 컨피그레이션을 푸시하는 데 소요된 시간(분)	7
Migration Status(마이그레이션 상태)	Check Point 컨피그레이션의 Firewall Management Center로의 마이그레이션 상태	성공
Error Message(오류 메시지)	Secure Firewall 마이그레이션 툴에 표시되는 오류 메시지	null
Error Description(오류 설명)	오류가 발생한 단계에 대한 설명 및 가능한 근본 원인	null

r77의 텔레메트리 Check Point 예시 파일

다음은 Check Point 컨피그레이션을 Firewall Threat Defense로 마이그레이션하는 경우 텔레메트리 데이터 파일의 예입니다.

```
{
  "metadata": {
    "contentType": "application/json",
    "topic": "migrationtool.telemetry"
  },
  "payload": {
    "Check Point_config_stats": {
      "Ipv6_access_rule_counts": 0,
      "Ipv6_bgp_count": 0,
      "Ipv6_nat_rule_count": 0,
      "Ipv6_network_counts": 24,
      "Ipv6_static_route_counts": 6,
      "access_rules_counts": 63,
      "acl_counts": 63,
      "fqdn_based_access_rule_counts": 0,
      "nat_rule_counts": 0,
      "network_object_counts": 143,
      "network_object_group_counts": 31,
      "no_of_fqdn_based_objects": 0,
      "ospfv3_count": 0,
      "port_object_counts": 370,
      "port_object_group_counts": 55,
      "sgt_based_access_rules_count": 0,
      "timerange_based_access_rule_counts": 0,
      "total_unparsed_access_rule_counts": 0,
      "tunneling_protocol_based_access_rule_counts": 0,
      "unparsed_config_count": 15,
      "unsupported_access_rules_count": 0,
      "unsupported_nat_rule_count": 0
    },
    "context_mode": "SINGLE",
    "error_description": null,
    "error_message": null,
    "firewall_mode": "ROUTED",
    "log_info_acl_count": 0,
    "migration_status": "SUCCESS",
    "migration_summary": {
      "access_control_policy": [
        [
          {
            "access_rule_counts": 63,
            "apply_file_policy_rule_counts": 0,
            "apply_ips_policy_rule_counts": 0,
            "apply_log_rule_counts": 0,
            "do_not_migrate_rule_counts": 0,
            "enable_Global-ACL-Policy": true,
            "enable_Zone-Specific-ACL-Policy": false,
            "enable_hit_count": false,
            "expanded_acp_rule_counts": 1,
            "name": "FTD-Mig-1566804327",
            "partially_migrated_acl_rule_counts": 0,
            "update_rule_action_counts": 0
          }
        ]
      ]
    },
    "interface_counts": 12,
    "interface_group_counts": 0,
    "interface_group_manually_created_counts": 0,
    "nat_Policy": [
```

```
[
  {
    "NAT_rule_counts": 0,
    "do_not_migrate_rule_counts": 0,
    "name": "Doesn't Exist",
    "partially_migrated_nat_rule_counts": 0
  }
],
"network_object_rename_counts": 0,
"network_object_reused_counts": 0,
"object_group_counts": 15,
"objects_counts": 54,
"port_object_rename_counts": 0,
"port_object_reused_counts": 5,
"security_zone_counts": 13,
"security_zone_manually_created_counts": 0,
"static_routes_counts": 22,
"sub_interface_counts": 11
},
"migration_tool_version": "2.0.3169",
"rule_change_acl_count": 0,
"source_config_counts": 0,
"source_device_model_number": "Check Point Model Not Exists",
"source_device_serial_number": null,
"source_device_version": "R77.30",
"source_type": "Check Point",
"system_information": {
  "browser": "Chrome/76.0.3809.100",
  "operating_system": "Windows NT 10.0; Win64; x64"
},
"target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
"target_device_version": "76",
"target_management_type": "6.4.0.4 (build 31)",
"target_management_version": "6.4.0.4 (build 31)",
"template_version": "1.1",
"time": "2019-08-26 12:55:40",
"tool_analytics_data": {
  "objectsplit_100_count": 0
},
"tool_performance": {
  "config_push_time": 725,
  "conversion_time": 29,
  "migration_time": 1020
}
},
"version": "1.0"
}
```

r80의 텔레메트리 Check Point 예시 파일

다음은 Check Point 컨피그레이션을 Firewall Threat Defense로 마이그레이션하는 경우 텔레메트리 데이터 파일의 예입니다.

```
{
  "Check Point_config_stats": {
    "Ipv6_access_rule_counts": 0,
    "Ipv6_bgp_count": 0,
    "Ipv6_nat_rule_count": 0,
    "Ipv6_network_counts": 3,
    "Ipv6_static_route_counts": 0,
    "access_rules_counts": 726,
    "acl_category_count": 0,

```

```

"acl_counts":726,
"fqdn_based_access_rule_counts":0,
"nat_rule_counts":335,
"network_object_counts":7645,
"network_object_group_counts":268,
"no_of_fqdn_based_objects":0,
"port_object_counts":1051,
"port_object_group_counts":66,
"s2s_vpn_tunnel_counts":0,
"sgt_based_access_rules_count":0,
"timerange_based_access_rule_counts":0,
"total_unparsed_access_rule_counts":0,
"tunneling_protocol_based_access_rule_counts":0,
"unparsed_config_count":234,
"unsupported_access_rules_count":0,
"unsupported_nat_rule_count":0},
"context_mode":"SINGLE",
"error_description":"No data.",
"error_message":"push failed for object network",
"firewall_mode":"ROUTED",
"log_info_acl_count":0,
"migration_status":"FAIL",
"migration_summary":{
  "access_control_policy":[
    [
      {
        "access_rule_counts":0,
        "apply_file_policy_rule_counts":0,
        "apply_ips_policy_rule_counts":0,
        "apply_log_rule_counts":0,
        "do_not_migrate_rule_counts":0,
        "enable_Global-ACL-Policy":true,
        "enable_Zone-Specific-ACL-Policy":false,
        "enable_hit_count":false,
        "expanded_acp_rule_counts":1,
        "name":"Doesn't Exist",
        "partially_migrated_acl_rule_counts":0,
        "total_acl_element_counts":389416,
        "update_rule_action_counts":0
      }
    ]
  ],
  "interface_counts":11,
  "interface_group_counts":0,
  "interface_group_manually_created_counts":0,
  "nat_Policy":[
    [
      {
        "NAT_rule_counts":0,
        "do_not_migrate_rule_counts":0,
        "name":"Doesn't Exist",
        "partially_migrated_nat_rule_counts":0
      }
    ]
  ],
  "network_object_rename_counts":0,
  "network_object_reused_counts":0,
  "object_group_counts":222,"objects_counts":7148,
  "port_object_rename_counts":2,
  "port_object_reused_counts":30,
  "prefilter_control_policy":[
    [
      {
        "do_not_migrate_rule_counts":0,

```

```

        "name":null,
        "partially_migrated_acl_rule_counts":0,
        "prefilter_rule_counts":0
    }
    ],
    "security_zone_counts":11,
    "security_zone_manually_created_counts":0,
    "static_routes_counts":0,
    "sub_interface_counts":8,
    "time_out":false},
    "migration_tool_version":"2.1.4283",
    "mtu_info":{"interface_name":null,
    "mtu_value":null},
    "rule_change_acl_count":0,
    "selective_policy":
    {
        "acl":true,
        "acl_policy":true,
        "application":false,
        "csm":false,
    "interface":true,
    "interface_groups":true,
    "migrate_tunneled_routes":false,
    "nat":true,
    "network_object":true,
    "policy_assignment":true,
    "populate_sz":false,
    "port_object":true,
    "routes":true,
    "security_zones":true,
    "unreferenced":true},
    "source_config_counts":0,
    "source_device_model_number":"Check Point Model Not Exists",
    "source_device_serial_number":null,
    "source_device_version":"R77.30",
    "source_type":"Check Point",
    "system_information":
    {
        "browser":"Chrome/80.0.3987.163","operating_system":
        "Macintosh; Intel Mac OS X 10_15_4"},
        "target_device_model":"Cisco Firepower 4110 Threat Defense",
        "target_device_version":"76",
        "target_management_type":"6.5.0 (build 63)",
        "target_management_version":"6.5.0 (build 63)",
        "template_version":"1.1",
        "time":"2020-04-16 04:50:05",
        "tool_analytics_data":{"objectsplit_100_count":6},
        "tool_performance":
        {
            "config_push_time":1457,
            "conversion_time":279,
            "migration_time":2637
        }
    }
}

```




4 장

마이그레이션 문제 해결

- Secure Firewall 마이그레이션 툴 문제 해결, 91 페이지
- 문제 해결에 사용되는 로그 및 기타 파일, 92 페이지
- Check Point 파일 업로드 실패 문제 해결, 92 페이지

Secure Firewall 마이그레이션 툴 문제 해결

마이그레이션은 일반적으로 Check Point 컨피그레이션 파일을 업로드하는 동안이나 마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시하는 동안 실패합니다.

Check Point 컨피그레이션에서 마이그레이션 프로세스가 실패하는 몇 가지 일반적인 시나리오는 다음과 같습니다.

- Check Point Config.zip에서 파일이 누락되었습니다.
- Secure Firewall 마이그레이션 툴이 Check Point Config.zip에서 잘못된 파일을 감지했습니다.
- Check Point 컨피그레이션 파일이 .zip 이외의 압축 파일 형식인 경우.

Secure Firewall 마이그레이션 툴 지원 번들

Secure Firewall 마이그레이션 툴은 로그 파일, DB, 구성 파일과 같은 중요한 문제 해결 정보를 추출하도록 지원 번들을 다운로드하는 옵션을 제공합니다. 다음을 수행하십시오.

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.

문제 해결에 사용되는 로그 및 기타 파일

다음 파일에서 문제를 식별하고 해결하는 데 유용한 정보를 찾을 수 있습니다.

파일	위치
로그 파일	<migration_tool_folder>\logs
마이그레이션 전 보고서	<migration_tool_folder>\resources
마이그레이션 후 보고서	<migration_tool_folder>\resources
구문 분석되지 않은 파일	<migration_tool_folder>\resources

Check Point 파일 업로드 실패 문제 해결

Check Point 컨피그레이션 파일이 업로드되지 않는 경우 일반적인 이유는 Secure Firewall 마이그레이션 툴이 파일에서 하나 이상의 라인을 구문 분석할 수 없기 때문입니다.

다음 위치에서 업로드 및 구문 분석 실패를 일으킨 오류에 대한 정보를 찾을 수 있습니다.

- **Unparsed file**(구문 분석되지 않은 파일) - 파일의 끝을 확인하여 성공적으로 구문 분석된 Check Point 컨피그레이션 파일의 마지막으로 무시된 라인을 식별합니다.
- **예기치 않은 파일** - Check Point에 대해 잘못된 파일이 감지되었습니다. 예를 들어 Mac OS를 사용하여 압축하면 Mac 시스템 파일이 생성됩니다. Mac 파일을 제거합니다.
- **(r75-r77.30만 해당) Incorrectly named files**(잘못 명명된 파일) - 보안 정책 및 NAT 정책 파일의 이름이 Check Point에 대해 올바르게 지정되지 않은 경우입니다. ACL 및 NAT 파일의 이름을 올바르게 변경합니다.
- **누락된 파일** - Check Point config.zip 파일에서 일부 파일이 누락되었습니다. 필요한 파일을 추가합니다.



참고 r77의 경우 누락된 컨피그레이션 파일을 수동으로 추출합니다. 자세한 내용은 [Check Point r77 컨피그레이션 파일 내보내기](#)를 참조하십시오.

r80-r82의 경우 Live Connect를 사용하여 Secure Firewall 마이그레이션 툴에 대한 올바른 구성 파일을 추출합니다. 자세한 내용은 [Check Point r80-r82 구성 파일 내보내기](#)를 참조하십시오.

Check Point 문제 해결 예: 개체 그룹의 멤버를 찾을 수 없음(r75-r77.30만 해당)

이 예에서는 요소의 컨피그레이션 오류로 인해 Checkpoint 컨피그레이션 파일 업로드 및 구문 분석이 실패했습니다.

프로시저

단계 1 오류 메시지를 검토하여 문제를 식별합니다.

이 실패로 인해 다음 오류 메시지가 생성됩니다.

Location	오류 메시지
Secure Firewall 마이그레이션 툴 메시지	Check Point 컨피그레이션 파일이 구문 분석되어 오류가 발생했습니다. 구문 분석 오류에 대해서는 마이그레이션 전 보고서 오류 섹션을 참조하고, 푸시 단계 중에 발생하는 푸시 오류에 대해서는 마이그레이션 후 보고서 를 참조하십시오.
로그 파일	[ERROR objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;" [INFO objectGroupRules] > "Parsing object-group service:[services_gvxs06]" [INFO objectGroupRules] > "Parsing object-group service:[services_iphigenia]" [INFO objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

단계 2 Check Point services.xml 파일을 엽니다.

단계 3 이름이 services_gvxs06인 개체 그룹을 검색합니다.

단계 4 스마트 대시보드를 사용 중인 개체 그룹에 대해 누락된 멤버를 생성합니다.

단계 5 컨피그레이션 파일을 다시 내보냅니다. 자세한 내용은 [Check Point 컨피그레이션 파일 내보내기](#)를 참조하십시오.

단계 6 오류가 더 이상 없으면 새 Check Point 컨피그레이션 zip 파일을 Secure Firewall 마이그레이션 툴에 업로드하고 마이그레이션을 계속합니다.

Live Connect의 Check Point(r80-r82) 문제 해결 예

예 1: Check Point Security Manager에 대한 세부 정보를 요청합니다.

이 예에서 Secure Firewall 마이그레이션 툴은 Check Point Security Manager에 대한 세부 정보를 요청합니다.

오류 메시지를 검토하여 문제를 식별합니다. 이 실패로 인해 다음 오류 메시지가 생성됩니다.

Location	오류 메시지
Secure Firewall 마이그레이션 툴 메시지	Check Point Security Manager에 대한 세부 정보를 제공하기 위한 요청 화면.
로그 파일	[오류 connect_cp] > "권한 부족, 시간 초과 문제 등으로 인해 Extracted-objects.json 파일을 추출할 수 없습니다. 자세한 정보는 Secure Firewall 마이그레이션 툴 UG를 참조하십시오." 127.0.0.1 - - [20/Jul/2020 17:20:43] "POST /api/CP/connect HTTP/1.1" 500 -

잘못된 자격증명입니다. 자격 증명을 사전 스테이징하려면 다음 단계를 수행합니다. 사용되는 자격 증명에는 Check Point Security Manager용 Check Point Gaia에 /bin/bash 셸 프로파일이 있어야 합니다. 일반 구축을 위해 슈퍼 사용자 권한이 있는 Check Point Security Manager용 Check Point 스마트 콘솔 애플리케이션에서 동일한 자격 증명에 스테이징되어야 합니다. 멀티 도메인 구축을 사용하는 경우 권한은 슈퍼 사용자여야 합니다. 자세한 내용은 [Live Connect를 사용한 컨피그레이션 추출을 위한 Check Point\(r80-r82\) 디바이스 사전 스테이징](#)을 참조하십시오.

예 2: 잘못된 파일 형식

이 예에서는 잘못된 파일 형식으로 인해 Secure Firewall 마이그레이션 툴 마이그레이션이 차단되었습니다.

오류 메시지를 검토하여 문제를 식별합니다. 이 실패로 인해 다음 오류 메시지가 생성됩니다.

Location	오류 메시지
Secure Firewall 마이그레이션 툴 메시지	차단됨
로그 파일	[오류 cp_device_connection] > "잘못된 파일 형식" 2020-07-20 17:10:57,347 [오류 connect_cp] > ".tar 파일을 다운로드할 수 없습니다." 127.0.0.1 - - [20/Jul/2020 17:10:57] "GET /api/CP/generate_tar_file?package=Standard HTTP/1.1" 500 -

잘못된 자격증명입니다. 자격 증명을 사전 스테이징하려면 다음 단계를 수행합니다. 사용되는 자격 증명에는 Check Point Security Manager용 Check Point Gaia에 `/bin/bash` 셸 프로파일이 있어야 합니다. 슈퍼 사용자 권한이 있는 Check Point Security Manager용 Check Point 스마트 콘솔 애플리케이션에서 동일한 자격 증명이 스테이징되어야 합니다. 멀티 도메인 구축을 사용하는 경우 슈퍼 사용자 권한을 부여해야 합니다. 자세한 내용은 [Live Connect를 사용한 컨피그레이션 추출을 위한 Check Point\(r80-r82\) 디바이스 사전 스테이징](#)을 참고하십시오.

예 3: Threat Defense에서 차단된 VSX 기능이 지원되지 않음

이 예에서는 Threat Defense에서 차단된 VSX 기능으로 인해 Secure Firewall 마이그레이션 툴 마이그레이션이 실패합니다.

오류 메시지를 검토하여 문제를 식별합니다. 이 실패로 인해 다음 오류 메시지가 생성됩니다.

Location	오류 메시지
Secure Firewall 마이그레이션 툴 메시지	FTD에서 차단된 VSX 기능이 지원되지 않습니다.
로그 파일	[오류 config_upload] > "VSX 기능이 FTD에서 지원되지 않음" 역추적(가장 최근 호출)

문제 설명 - 이 오류는 Check Point r80.40부터 `fw vsx stat` 명령이 더 이상 사용되지 않을 때 발생합니다.

이 문제를 해결하려면 다음 단계를 수행합니다.

1. `config.zip` 파일의 압축을 풉니다.
2. `networking.txt` 파일을 엽니다.

다음은 샘플 출력의 예입니다.

```
firewall> fw vsx stat
Deprecated command, Please see sk144112 for alternative
Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
```

다음과 같이 수동으로 교체합니다.

```
firewall> fw vsx stat
VSX is not supported on this platform
```

3. 모든 파일을 선택하고 .zip 확장자로 압축합니다.

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.