



Cisco Secure Firewall 마이그레이션 툴을 사용하여 Cisco Secure Firewall ASA를 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)

© 2022–2026 Cisco Systems, Inc. 모든 권리 보유.



목 차

장 1

Secure Firewall 마이그레이션 툴 시작하기 1

가이드 정보 1

Secure Firewall 마이그레이션 툴 정보 1

Secure Firewall 마이그레이션 툴 최신 기능 4

Secure Firewall 마이그레이션 툴 라이선싱 29

Secure Firewall 마이그레이션 툴의 플랫폼 요구 사항 29

Threat Defense 디바이스의 요구 사항 및 사전 요건 29

구성 지원 30

지침 및 제한 사항 35

마이그레이션에 지원되는 플랫폼 40

마이그레이션에 지원되는 대상 Management Center 43

마이그레이션에 지원되는 소프트웨어 버전 45

관련 설명서 46

장 2

ASA를 Threat Defense로 마이그레이션 워크플로우 49

엔드 투 엔드 절차 49

마이그레이션 사전 요건 51

Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드 51

구성 파일 가져오기 52

컨피그레이션 파일 내보내기 53

ASA 에서 PKI 인증서 내보내기 및 Management Center로 가져오기 53

AnyConnect 패키지 및 프로파일 검색 54

마이그레이션 실행 55

Secure Firewall 마이그레이션 툴 실행 55

Secure Firewall 마이그레이션 툴에서 데모 모드 사용	58
ASA 구성 파일 업로드	58
Secure Firewall 마이그레이션 툴에서 ASA에 연결	59
ASA 보안 컨텍스트 선택	60
Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정	62
인라인 그룹화	71
마이그레이션 전 보고서 검토	72
ASA 구성과 Firewall Threat Defense 인터페이스 매핑	73
ASA 인터페이스를 보안 영역 및 VRF에 매핑	75
최적화, 구성 검토 및 검증	77
ACL 최적화 보고	93
마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시	94
마이그레이션 후 보고서 검토 및 마이그레이션 완료	96
Secure Firewall 마이그레이션 툴 제거	100
샘플 마이그레이션: ASA 를 Threat Defense 2100으로	101
유지 보수 기간 작업별	101
유지 보수 기간 작업	103

장 3	Cisco Success Network - 텔레메트리 데이터	105
	Cisco Success Network - 텔레메트리 데이터	105

장 4	마이그레이션 문제 해결	113
	Secure Firewall 마이그레이션 툴 문제 해결	113
	문제 해결에 사용되는 로그 및 기타 파일	114
	ASA 파일 업로드 실패 문제 해결	114
	ASA에 대한 문제 해결 예: 개체 그룹의 멤버를 찾을 수 없음	114
	ASA에 대한 문제 해결 예: 목록 인덱스 범위를 벗어남	115



1 장

Secure Firewall 마이그레이션 툴 시작하기

- 가이드 정보, 1 페이지
- Secure Firewall 마이그레이션 툴 정보, 1 페이지
- Secure Firewall 마이그레이션 툴 최신 기능, 4 페이지
- Secure Firewall 마이그레이션 툴 라이선싱, 29 페이지
- Secure Firewall 마이그레이션 툴의 플랫폼 요구 사항, 29 페이지
- Threat Defense 디바이스의 요구 사항 및 사전 요건, 29 페이지
- 구성 지원, 30 페이지
- 지침 및 제한 사항, 35 페이지
- 마이그레이션에 지원되는 플랫폼, 40 페이지
- 마이그레이션에 지원되는 대상 Management Center, 43 페이지
- 마이그레이션에 지원되는 소프트웨어 버전, 45 페이지
- 관련 설명서, 46 페이지

가이드 정보

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

Secure Firewall 마이그레이션 툴 정보

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

Secure Firewall 마이그레이션 툴은 지원되는 Cisco Secure Firewall ASA 구성을 지원되는 Secure Firewall Threat Defense 플랫폼으로 전환합니다. Secure Firewall 마이그레이션 툴을 사용하면 지원되는 ASA 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.

일반적으로 사용되는 ASA 기능 및 그에 상응하는 Threat Defense 기능에 대한 자세한 내용은 [Cisco Secure Firewall ASA-Threat Defense 기능 매핑](#) 가이드를 참고하십시오.

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

- Cisco ASA(Adaptive Security Appliance) 컨피그레이션 항목 중 완전히 마이그레이션되는 항목, 부분적으로 마이그레이션되는 항목, 마이그레이션이 지원되지 않는 항목, 마이그레이션에서 무시되는 항목
- Secure Firewall 마이그레이션 툴이 인식할 수 없는 CLI를 나열하는 오류가 있는 구성 라인. 이로 인해 마이그레이션이 차단됩니다.

구문 분석 오류가 있는 경우 문제를 해결하고, 새 구성을 다시 업로드하고, 대상 디바이스에 연결하고, 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, ASA 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 ASA 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.

버전	지원 기능
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 ASA를 Cisco Secure Firewall Threat Defense로 마이그레이션</i> 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 ASA를 Cisco Secure Firewall Threat Defense로 마이그레이션</i> 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 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션하기</i> 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. 구문 분석된 요약의 Routes(경로) 타일에는 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 툴에서는 이제 대상 Management Center 및 Threat Defense 버전이 7.1 이상인 경우 사이트 간 VPN 필터 구성 및 이러한 구성과 관련된 확장 액세스 목록 개체의 마이그레이션을 지원합니다. 이전에는 사이트 간 VPN 필터 구성이 마이그레이션되지 않으며, 마이그레이션 후 수동으로 구성해야 했습니다. - 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. Secure Firewall 마이그레이션 툴은 이제 이름과 구성을 기반으로 모든 개체 및 개체 그룹을 분석하고 동일한 이름 및 구성을 가진 개체를 재사용합니다. 이전에는 이름 및 구성을 기준으로 네트워크 개체 및 네트워크 개체 그룹만 분석되었습니다. 원격 액세스 VPN의 XML 프로파일은 여전히 이름을 사용해서만 검증됩니다.

버전	지원 기능
4.0	Secure Firewall 마이그레이션 툴 4.0은 다음을 지원합니다. • 대상 Management Center 및 Threat Defense 버전이 7.3 이상인 경우 ASA에서 PBR(Policy Based Routing) 마이그레이션. 참고 PBR 마이그레이션의 경우, 마이그레이션을 진행하기 전에 기존 Flex 구성을 Management Center에서 제거해야 합니다. • 대상 Management Center가 7.3 이상인 경우 ASA에서 원격 액세스 VPN 사용자 지정 속성 및 VPN 로드 밸런싱 마이그레이션. 방화벽을 사용하거나 사용하지 않고 원격 액세스 VPN 마이그레이션을 수행할 수 있습니다. 그러나 방화벽을 사용하여 마이그레이션을 수행하도록 선택한 경우 Threat Defense 버전은 7.0 이상이어야 합니다. 참고 대상 방화벽을 사용하여 원격 액세스 VPN을 마이그레이션하려면 대상 방화벽을 선택하고 대상 방화벽에 다음 라이선스 중 하나를 추가해야 합니다. • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN만 • 대상 Management Center가 7.1 이상이고 Threat Defense 버전이 6.5 이상인 경우 ASA에서 ECMP(Equal Cost Multi-Path) 경로 마이그레이션.
3.0.2	Secure Firewall 마이그레이션 툴 3.0.2에는 ASA에서 Firewall Management Center 버전 7.2 이상으로 원격 액세스 VPN 구성을 마이그레이션하기 위한 버그 수정이 포함되어 있습니다.
3.0.1	Secure Firewall 마이그레이션 툴 3.0.1은 다음을 지원합니다. • 대상 Management Center가 버전 7.2 이상이고 Threat Defense 버전이 7.0 이상인 경우 ASA에서 EIGRP(Enhanced Interior Gateway Routing Protocol) 마이그레이션. 참고 Threat Defense 디바이스 없이 FirePOWER Services를 포함한 ASA 및 ASA에서 EIGRP를 마이그레이션할 수 없습니다. • Cisco Secure Firewall 3100 Series는 ASA에서의 마이그레이션을 위한 소스 또는 대상 디바이스로 지원됩니다.

버전	지원 기능
3.0	Secure Firewall 마이그레이션 툴 3.0은 다음을 지원합니다. • 대상 Management Center가 7.2 이상인 경우 ASA 의 원격 액세스 VPN 마이그레이션. Secure Firewall Threat Defense를 사용하거나 사용하지 않고 RA VPN 마이그레이션을 수행할 수 있습니다. Threat Defense를 사용하여 마이그레이션을 선택한 경우 Threat Defense 버전은 7.0 이상이어야 합니다. • ASA에서 사이트 간 VPN 사전 공유 키 자동화. • 마이그레이션 전 활동의 일부로 다음을 수행해야 합니다. • ASA 트러스트 포인트는 PKI 개체로 Management Center에 수동으로 마이그레이션해야 합니다. • AnyConnect 패키지, Hostscan 파일(Dap.xml, Data.xml, Hostscan 패키지), 외부 브라우저 패키지 및 AnyConnect 프로파일을 소스 ASA에서 검색해야 합니다. • AnyConnect 패키지를 Management Center에 업로드해야 합니다. • AnyConnect 프로파일을 Management Center에 직접 업로드하거나 Secure Firewall 마이그레이션 툴에서 업로드할 수 있습니다. • Live Connect ASA에서 프로파일을 검색할 수 있도록 하려면 ASA에서 ssh scopy enable 명령을 활성화해야 합니다. • 대상 Management Center가 7.2 이상인 경우 ASA에서 클라우드 제공 Firewall Management Center로 마이그레이션.
2.5.2	Secure Firewall 마이그레이션 툴 2.5.2는 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 ASA 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
2.5.1	Secure Firewall 마이그레이션 툴 2.5.1은 대상 Firewall Management Center가 7.1 이상인 경우 BGP(Border Gateway Protocol) 및 유동 경로 개체 마이그레이션을 지원합니다.
2.5	Secure Firewall 마이그레이션 툴 2.5는 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 구성을 완전히 새도우합니다. 참고 최적화는 ACP 규칙 작업에 대해서만 소스 ASA에 사용할 수 있습니다. 대상 Firewall Management Center 버전이 7.1 이상인 경우 불연속 네트워크 마스크(와일드카드 마스크) 개체를 지원합니다.
2.4	다음 ASA VPN 컨피그레이션을 Firewall Threat Defense로 마이그레이션합니다. - ASA의 암호화 맵(정적/동적) 기반 VPN - 경로 기반(VTI) 기반 ASA VPN - ASA의 인증서 기반 VPN 마이그레이션 참고 - ASA 트러스트 포인트 또는 인증서는 수동으로 마이그레이션되며 마이그레이션 전 활동의 일부입니다. - ASA 트러스트 포인트는 Firewall Management Center PKI 개체로 마이그레이션해야 합니다. PKI 개체는 인증서 기반 VPN 토폴로지를 생성하는 동안 Secure Firewall 마이그레이션 툴에서 사용됩니다.

버전	지원 기능
2.3.5	Secure Firewall 마이그레이션 툴은 대상 Firewall Management Center 및 Firewall Threat Defense가 6.7 이상인 경우 VTI(Virtual Tunnel Interface) 구성의 Firewall Threat Defense로의 마이그레이션을 지원합니다. • VTI 인터페이스 및 관련 정적 경로 • Firewall Management Center 및 Firewall Threat Defense로의 경로 기반(VTI) 사전 공유 키 인증 유형 VPN 구성. • 라우팅된 보안 영역을 생성하고 여기에 VTI 인터페이스를 추가한 다음, VTI 터널을 통해 해독된 트래픽 제어를 위한 액세스 제어 규칙을 정의합니다.
2.3.4	Secure Firewall 마이그레이션 툴을 사용하여 다음과 같은 ASA VPN 구성 요소를 Firewall Threat Defense로 마이그레이션할 수 있습니다. • 정책 기반(암호화 맵) 사전 공유 키 인증 유형 VPN 구성의 Firewall Management Center로의 마이그레이션을 지원합니다. • VPN 개체 - VPN 개체(IKEv1/IKEv2 정책, IKEv1/IKEv2 IPsec-Proposal)를 생성하고 VPN 개체를 특정 사이트 간 VPN 토폴로지에 매핑하며 개체를 Firewall Management Center로 마이그레이션합니다. Review and Validate Configuration(구성 검토 및 검증) 페이지의 규칙에 따라 VPN 개체를 검증합니다. • 사이트 간 VPN 토폴로지 - 소스 ASA 구성의 암호화 맵 관련 구성이 각 VPN 개체와 함께 마이그레이션됩니다. 정책 기반(암호화 맵) VPN 토폴로지는 Firewall Management Center 버전 6.6 이상에서 지원됩니다. 참고 이 릴리스에서 Secure Firewall 마이그레이션 툴은 정적 암호화 맵의 마이그레이션만 지원합니다. 지원되는 모든 ASA 암호화 맵 VPN은 Firewall Management Center Point-to-Point 토폴로지로 마이그레이션됩니다.

버전	지원 기능
1.3	

버전	지원 기능
	- Secure Firewall 마이그레이션 툴을 사용하여 ASA에 구성된 관리자 자격 증명 및 Enable Password(활성화 비밀번호)를 통해 ASA에 연결할 수 있습니다. ASA에 Enable Password(활성화 비밀번호)가 구성되지 않은 경우 Secure Firewall 마이그레이션 툴에서 필드를 비워 둘 수 있습니다. - app_config 파일에서 Bulk Push(일괄 푸시)에 대한 배치 크기 제한을 다음과 같이 구성할 수 있습니다. - 개체의 경우 배치 크기가 500을 초과할 수 없습니다. Secure Firewall 마이그레이션 툴은 값을 50으로 재설정하고 일괄 푸시를 진행합니다. - ACL, 경로 및 NAT의 경우 배치 크기가 각각 1000을 초과할 수 없습니다. Secure Firewall 마이그레이션 툴은 값을 1000으로 재설정하고 일괄 푸시를 진행합니다. - Secure Firewall 마이그레이션 툴을 사용하여 CSM 또는 ASDM 관리 구성을 구문 분석할 수 있습니다. 인라인 그룹화 또는 ASDM 관리 컨피그레이션을 지우도록 선택하는 경우 미리 정의된 개체가 실제 개체 또는 멤버 이름으로 대체됩니다. CSM 또는 ASDM 관리 컨피그레이션을 지우지 않으면 마이그레이션 시 미리 정의된 개체 이름이 유지됩니다. - 마이그레이션 실패 시 고객 지원을 통해 로그 파일, dB 및 컨피그레이션 파일을 다운로드하는 기능을 제공합니다. 이메일을 통해 기술 팀에 지원 케이스를 제출할 수도 있습니다. - 개체, 인터페이스, ACL, NAT 및 경로에서 IPv6 컨피그레이션의 마이그레이션을 지원합니다. - Secure Firewall 마이그레이션 툴을 사용하여 Firewall Threat Defense 개체 유형(물리적 인터페이스, 포트 채널 및 하위 인터페이스)의 물리적 인터페이스에 ASA 인터페이스 이름을 매핑할 수 있습니다. 예를 들어 ASA의 포트 채널을 Firewall Management Center의 물리적 인터페이스에 매핑할 수 있습니다. - Secure Firewall 마이그레이션 툴이 선택한 NAT 규칙 및 경로 인터페이스의 마이그레이션을 건너뛰도록 지원합니다. 이전 버전의 Secure Firewall 마이그레이션 툴에서는 액세스 제어 규칙에 대해서만 이 옵션을 제공했습니다. - 구문 분석된 액세스 제어, NAT, 네트워크 개체, 포트 개체, 인터페이스 및 경로 컨피그레이션 항목을 Optimize, Review and Validate Configuration(컨피그레이션 최적화, 검토 및 검증) 화면에서 Excel 또는 CSV 형식으로 다운로드할 수 있습니다.

버전	지원 기능
	참고 CSV 파일은 가져올 수 없습니다.
1.2	• Firewall Management Center 6.3으로의 마이그레이션 지원 • IPv4 FQDN 개체 및 그룹의 마이그레이션을 지원합니다. • 멀티 컨텍스트 ASA에 대한 수동 업로드 방법에서 show tech-support 명령을 지원합니다. • Firewall Management Center에 등록된 컨테이너 유형 Firewall Threat Defense(MI)로의 마이그레이션을 지원합니다. • 액세스 제어 테이블의 마이그레이션된 액세스 제어 규칙에 대한 규칙 작업(허용, 신외, 모니터링, 차단 또는 차단 후 재설정) 매핑을 지원합니다. • Secure Firewall 마이그레이션 툴의 버전 확인을 통해 최신 버전의 Secure Firewall 마이그레이션 툴을 사용하고 있는지 확인합니다.
1.1	• 개체, NAT, 정적 경로에 대한 일괄 푸시 기능은 구성을 Firewall Management Center에 푸시하는 데 걸리는 시간을 크게 줄입니다. • 프로덕션 ASA에서 컨피그레이션 추출 • 선택적 기능 마이그레이션(공유 정책 및 디바이스별 정책) • 규칙 최적화 • 마이그레이션 중인 ASA 액세스 제어 규칙을 Firewall Management Center에서 구성된 침입 방지 시스템 및 파일 정책 목록에 매핑합니다. • 정책에서 참조되는 개체만 마이그레이션합니다. 이렇게 하면 마이그레이션 시간이 최적화되고 컨피그레이션 중에 사용되지 않는 개체가 제거됩니다. • 멀티 컨텍스트 모드에서 실행 중인 ASA의 데이터 컨텍스트 중 하나에서 running-config 또는 sh run에 대한 마이그레이션을 지원합니다. • macOS 10.13 이상 버전에서 지원 • 마이그레이션된 액세스 제어 규칙에 대한 기록 작업(활성화 또는 비활성화, 시작 또는 종료 시 기록) 수정을 지원합니다. • Firewall Management Center의 도메인 내에 구성된 Firewall Threat Defense 디바이스로 마이그레이션합니다. • 개체 이름에 대한 일괄 수정 기능 • Cisco Success Network를 통한 텔레메트리 지원

버전	지원 기능
1.0	- 구문 분석 및 푸시 작업을 포함한 마이그레이션 전체에 걸친 검증 - 개체 재사용 기능 - 개체 충돌 해결 - 인터페이스 매핑 - 인터페이스 개체 자동 생성 또는 재사용(보안 영역 또는 인터페이스 그룹 매핑 시 ASA 이름) - ACL의 일괄 마이그레이션 지원

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 ASA 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 Threat Defense 디바이스에서 최소한 와 같은 수의 물리적 데이터 및 포트 채널 인터페이스('관리 전용' 및 하위 인터페이스 제외)를 사용해야 합니다. 그렇지 않은 경우 대상 Threat Defense 디바이스에 필요한 인터페이스 유형을 추가해야 합니다. 하위 인터페이스는 물리적 또는 포트 채널 매핑을 기반으로 Secure Firewall 마이그레이션 툴에서 생성됩니다.
 - 대상 Threat Defense 디바이스가 컨테이너 인스턴스인 경우 ASA와 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.

구성 지원

지원되는 구성

Secure Firewall 마이그레이션 툴은 다음 구성을 완전히 마이그레이션할 수 있습니다.

- 네트워크 개체 및 그룹
- 서비스 개체(소스 및 대상에 대해 구성된 서비스 개체 제외)



참고

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

- 서비스 개체 그룹(중첩된 서비스 개체 그룹 제외)



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

- IPv4 및 IPv6 FQDN 개체 및 그룹
- IPv6 변환 지원(인터페이스, 정적 경로, 개체, ACL 및 NAT)
- 인바운드 방향 및 전역 ACL의 인터페이스에 적용되는 액세스 규칙
- 자동 NAT, 수동 NAT 및 개체 NAT(조건부)
- 정적 경로, ECMP 경로 및 PBR
- 서버, 릴레이 및 DDNS를 포함한 DHCP 구성
- SNMP
- 물리적 인터페이스
- 인터페이스의 보조 VLAN은 Firewall Threat Defense에 마이그레이션되지 않습니다.
- 하위 인터페이스(하위 인터페이스 ID는 마이그레이션 시 항상 VLAN ID와 동일한 숫자로 설정됨)
- 포트 채널
- Virtual tunnel interface(VTI)
- 동적 VTI 및 IPv6
- 브리지 그룹(투명 모드만)
- IP SLA 모니터링

Secure Firewall 마이그레이션 툴에서 IP SLA 개체를 생성하고, 개체를 특정 정적 경로와 매핑하고, 개체를 Firewall Management Center로 마이그레이션합니다.

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



참고 IP SLA 모니터는 비 Firewall Threat Defense 플로우에 대해 지원되지 않습니다.

- 개체 그룹 검색

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



참고

- Firewall Management Center 또는 Firewall Threat Defense 6.6 이전 버전에서는 개체 그룹 검색을 사용할 수 없습니다.
- 개체 그룹 검색은 비 Firewall Threat Defense 플로우에 대해 지원되지 않으므로 비활성화됩니다.

- 보안 그룹 태그 기반 개체

SGT(보안 그룹 태그) 개체는 정책 기반 액세스 제어 사용을 통해 확장 가능한 유동 네트워크 보안을 활성화합니다. Secure Firewall 마이그레이션 툴이 SGT 기반 개체를 탐지하면 **Review and Validate Configuration**(구성 검토 및 검증) 페이지의 규칙에 따라 개체를 확인합니다.

SGT 개체 구성을 마이그레이션하려면 관리 센터 및 위협 방어 버전이 7.0 이상인지 확인하십시오.

- 시간 기반 개체

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

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



참고

- 소스에서 대상 FTD로 표준 시간대 컨피그레이션을 수동으로 마이그레이션해야 합니다.
- 시간 기반 개체는 비 Firewall Threat Defense 플로우에 대해 지원되지 않으므로 비활성화됩니다.
- 시간 기반 개체는 Firewall Management Center 6.6 이상 버전에서 지원됩니다.

- 사이트 간 VPN 터널

- 사이트 간 VPN - Secure Firewall 마이그레이션 툴이 소스에서 암호화 맵 구성을 탐지하면 Secure Firewall 마이그레이션 툴은 암호화 맵을 Point-to-Point 토폴로지로 Firewall Management Center VPN에 마이그레이션합니다.

- ASA의 암호화 맵(정적/동적) 기반 VPN
- 경로 기반(VTI) 기반 ASA VPN
- ASA의 인증서 기반 VPN 마이그레이션
- Firewall Management Center로의 ASA 트러스트 포인트 또는 인증서 마이그레이션은 수동으로 수행해야 하며, 마이그레이션 전 활동의 일부입니다.
- 유동 경로 개체, BGP 및 EIGRP
 - Policy-List
 - Prefix-List
 - 커뮤니티 목록
 - AS(Autonomous System)-경로
- 원격 액세스 VPN
 - SSL 및 IKEv2 프로토콜
 - 인증 방법 - AAA 전용, 클라이언트 인증서 전용, SAML, AAA, 클라이언트 인증서
 - AAA - Radius, 로컬, LDAP 및 AD
 - 연결 프로파일, 그룹 정책, Dynamic Access Policy, LDAP 속성 맵, 인증서 맵
 - 표준 및 확장 ACL
 - RA VPN 사용자 지정 속성 및 VPN 로드 밸런싱
 - 마이그레이션 전 활동의 일부로 다음을 수행합니다.
 - ASA 트러스트 포인트를 Firewall Management Center에 PKI 개체로 수동 마이그레이션합니다.
 - 소스 ASA에서 AnyConnect 패키지, Hostscan 파일(Dap.xml, Data.xml, Hostscan 패키지), 외부 브라우저 패키지 및 AnyConnect 프로파일을 검색합니다.
 - 모든 AnyConnect 패키지를 Firewall Management Center에 업로드합니다.
 - AnyConnect 프로파일을 Firewall Management Center에 직접 업로드하거나 Secure Firewall 마이그레이션 툴에서 업로드합니다.
 - Live Connect ASA에서 프로파일을 검색할 수 있도록 하려면 ASA에서 **ssh scopy enable** 명령을 활성화합니다.
- WebVPN
 - 그룹 보안 정책 SSL 클라이언트리스 VPN 터널 프로토콜
 - SAML(Security Assertion Markup Language)을 인증 방법으로 사용하는 그룹 정책 관련 터널 그룹

- SSL(Domain Name System) 기반 애플리케이션 URL이 포함된 터널 그룹



참고 앞서 언급한 기준이 충족되면 SAML 설정 및 애플리케이션 URL이 마이그레이션됩니다.

부분적으로 지원되는 구성

Secure Firewall 마이그레이션 툴은 다음 방화벽 구성의 마이그레이션을 부분적으로 지원합니다. 이러한 구성 중 일부에는 고급 옵션을 포함하며 고급 옵션 없이 마이그레이션되는 규칙이 있습니다. Firewall Management Center에서 이러한 고급 옵션을 지원하는 경우 마이그레이션이 완료된 후 수동으로 구성할 수 있습니다.

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

지원되지 않는 구성

Secure Firewall 마이그레이션 툴은 다음 방화벽 구성의 마이그레이션을 지원하지 않습니다. Firewall Management Center에서 이러한 구성을 지원하는 경우 마이그레이션이 완료된 후 수동으로 구성을 구성할 수 있습니다.

- 사용자 기반 액세스 제어 정책 규칙
- 블록 할당 옵션으로 구성된 NAT 규칙
- 터널링 프로토콜 기반 액세스 제어 정책 규칙



참고 Secure Firewall 마이그레이션 툴 및 Firewall Management Center 6.5에서 사전 필터를 지원합니다.

- SCTP로 구성된 NAT 규칙
- 호스트 '0.0.0.0'으로 구성된 NAT 규칙
- SLA 추적으로 DHCP 또는 PPPoE를 통해 얻은 기본 경로
- SLA 모니터 스케줄
- 전송 모드 IPsec transform-set

- Firewall Management Center로 ASA 트러스트 포인트 마이그레이션
- BGP용 투명 방화벽 모드
- ASA WebVPN-ZTA(Zero Trust 애플리케이션) 정책 마이그레이션에서 다음은 지원되지 않습니다.
 - WebVPN 즐겨찾기 가져오기
 - 로컬, RADIUS 및 LDAP 인증 방법
- 액세스 목록 비교

지침 및 제한 사항

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

Secure Firewall 마이그레이션 툴은 지원되지 않는 개체 및 규칙을 다음과 같이 처리합니다.

- 지원되지 않는 개체 및 NAT 규칙은 마이그레이션되지 않습니다.
- 지원되지 않는 ACL 규칙은 비활성화된 규칙으로 Firewall Management Center에 마이그레이션됩니다.
- 아웃바운드 ACL은 지원되지 않으며 Firewall Management Center로 마이그레이션되지 않습니다. 소스 방화벽에 아웃바운드 ACL이 있는 경우 **Pre-Migration Report**(마이그레이션 전 보고서)의 **ignored**(무시) 섹션에 보고됩니다.
- 지원되는 모든 암호화 맵 VPN은 Firewall Management Center Point-to-Point 토폴로지로 마이그레이션됩니다.
- 지원되지 않거나 불완전한 정적 암호화 맵 VPN 토폴로지는 마이그레이션되지 않습니다.
- ASA 멀티컨텍스트에서 단일 인스턴스 Threat Defense 마이그레이션에서 ECMP(Equal-Cost Multipath) 라우팅 구성은 해당 VRF(가상 라우팅 및 포워딩) 구성으로 마이그레이션됩니다.
 - 동일한 이름을 가진 두 개의 서로 다른 보안 컨텍스트에 있는 인터페이스는 밑줄 표시와 컨텍스트 이름이 추가되어 이름이 변경됩니다.
 - 동일한 이름을 가진 두 개의 서로 다른 보안 컨텍스트에 있는 보안 영역은 밑줄 표시와 컨텍스트 이름이 추가되어 이름이 변경됩니다.
 - ECMP 라우팅 구성이 VPN 구성과 함께 제공되는 경우, 전역 라우터(전역 VRF)로 마이그레이션됩니다.

구성 제한 사항

소스 구성을 마이그레이션하는 경우 다음과 같은 제한 사항이 있습니다.

- Secure Firewall 마이그레이션 툴은 에서 개별 보안 컨텍스트를 별도 Firewall Threat Defense 디바이스로 마이그레이션할 수 있도록 지원합니다.
- 시스템 컨피그레이션은 마이그레이션되지 않습니다.
- Secure Firewall 마이그레이션 툴은 50개가 넘는 인터페이스에 적용되는 단일 ACL 정책의 마이그레이션을 지원하지 않습니다. 50개 이상의 인터페이스에 적용된 ACL 정책은 수동으로 마이그레이션해야 합니다.
- 일부 구성(예: 유동 라우팅을 Firewall Threat Defense로 마이그레이션)은 마이그레이션할 수 없습니다. 이러한 컨피그레이션은 수동으로 마이그레이션해야 합니다.
- BVI(Bridge Virtual Interface), 이중화 인터페이스 또는 터널링 인터페이스를 사용하여 라우팅 모드로 디바이스를 마이그레이션할 수 없습니다. 그러나 BVI를 사용하여 투명 모드로 디바이스를 마이그레이션할 수는 있습니다.
- 중첩된 서비스 개체 그룹 또는 포트 그룹은 Firewall Management Center에서 지원되지 않습니다. 변환 과정에서 Secure Firewall 마이그레이션 툴은 참조된 중첩 개체 그룹 또는 포트 그룹의 콘텐츠를 확장합니다.
- Secure Firewall 마이그레이션 툴은 한 라인에 있는 소스 및 대상 포트를 포함한 확장 서비스 개체 또는 그룹을 여러 라인에 걸친 서로 다른 개체로 분할합니다. 이러한 액세스 제어 규칙에 대한 참조는 정확히 동일한 의미의 Firewall Management Center 규칙으로 변환됩니다.
- 소스 구성에 특정 터널링 프로토콜(예: GRE, IP-in-IP 및 IPv6-in-IP)을 참조하지 않는 액세스 제어 규칙이 있지만 이러한 규칙이 암호화되지 않은 터널 트래픽과 일치하는 경우 Firewall Threat Defense로 마이그레이션 시 해당 규칙이 에서와 동일한 방식으로 동작하지 않습니다. Firewall Threat Defense에서 사전 필터 정책에 이에 대한 특정 터널 규칙을 생성하는 것이 좋습니다.
- 지원되는 암호화 맵은 Point-to-Point 토폴로지로 마이그레이션됩니다.
- Firewall Management Center에 동일한 이름의 AS 경로 개체가 표시되면 다음 오류 메시지와 함께 마이그레이션이 중지됩니다.
"충돌하는 AS 경로 개체 이름이 Firewall Management Center에서 탐지되었습니다. 계속 진행하려면 Firewall Management Center의 충돌을 해결하십시오."
- OSPF 및 RIP(Routing Information Protocol)에서 EIGRP로의 재배포는 지원되지 않습니다.
- PBR의 경우 ASA 구성에는 경로 맵이 있는 반면 Management Center에는 경로 맵을 사용하지 않습니다. Secure Firewall 마이그레이션 툴은 인터페이스에 적용된 경로 맵 내부의 구성을 마이그레이션합니다.
- 시퀀스 번호가 여러 개인 경로 맵의 경우 첫 번째 시퀀스 번호만 마이그레이션됩니다. 다른 모든 시퀀스 번호는 무시되고 마이그레이션 전 보고서에 표시됩니다.

RA VPN 마이그레이션에 대한 제한 사항

원격 액세스 VPN 마이그레이션은 다음과 같은 제한 사항과 함께 지원됩니다.

- SSL 설정 마이그레이션은 API 제한으로 인해 지원되지 않습니다.
- LDAP 서버가 암호화 유형이 "none(없음)"인 상태로 마이그레이션됩니다.
- 정책이 전체 Firewall Management Center에 적용되므로 DfltGrpPolicy는 마이그레이션되지 않습니다. Firewall Management Center에서 직접 필요한 변경을 수행할 수 있습니다.
- Radius 서버의 경우 유동 권한 부여가 활성화되면 AAA 서버 연결은 유동 라우팅이 아닌 인터페이스를 통해 이루어져야 합니다. 인터페이스 없이 유동 권한 부여가 활성화된 AAA 서버에서 ASA 구성이 발견되면 Secure Firewall 마이그레이션 툴은 유동 권한 부여를 무시합니다. Management Center에서 인터페이스를 선택한 후 유동 권한 부여를 수동으로 활성화해야 합니다.
- ASA 구성은 터널 그룹에서 주소 풀을 호출하는 동안 인터페이스를 가질 수 있습니다. 하지만 Management Center에서 동일하게 지원되지는 않습니다. ASA 구성에서 인터페이스가 탐지되면 Secure Secure Firewall 마이그레이션 툴에서 무시되며 주소 풀은 인터페이스 없이 마이그레이션됩니다.
- ASA 구성에는 터널 그룹 아래에 dhcp-server에 대한 키워드 **link-selection/subnet-selection**를 가질 수 있습니다. 하지만 Management Center에서 동일하게 지원되지는 않습니다. 이러한 키워드를 사용하여 dhcp 서버가 ASA에서 탐지되면 Secure Firewall 마이그레이션 툴에서 이를 무시하고 dhcp-server가 키워드 없이 푸시됩니다.
- ASA 구성은 터널 그룹 아래의 인증 서버 그룹, 보조 인증 서버 그룹, 권한 부여 서버 그룹을 호출하는 동안 인터페이스를 가질 수 있습니다. 하지만 Management Center에서 동일하게 지원되지는 않습니다. ASA 구성에서 인터페이스가 탐지되면 Secure Secure Firewall 마이그레이션 툴에서 무시되며 명령은 인터페이스 없이 푸시됩니다.
- ASA 구성은 리디렉션 ACL을 Radius 서버에 매핑하지 않습니다. 따라서 Secure Firewall 마이그레이션 툴에서 검색할 수 있는 방법이 없습니다. 재전송 ACL이 ASA에서 사용되는 경우, 비워지며 Management Center에서 수동으로 추가하고 매핑해야 합니다.
- ASA에서는 vpn-addr-assign 로컬 재사용 지연에 대해 0~720 범위의 값을 지원합니다. 그러나 Management Center는 0~480의 값을 지원합니다. ASA 구성에서 480보다 큰 값이 발견되는 경우, Management Center에서 지원되는 최대값인 480으로 설정됩니다.
- 연결 프로파일에 대한 IPv4 풀 및 DHCP 사용SecondaryUsernameforSession 설정 구성은 API 문제로 인해 지원되지 않습니다.
- 우회 액세스 제어 sysopt permit-vpn 옵션은 RA VPN 정책에서 활성화되지 않습니다. 그러나 필요한 경우 Management Center에서 활성화할 수 있습니다.
- 프로파일이 Secure Firewall 마이그레이션 툴에서 Management Center로 업로드된 경우에만 AnyConnect 클라이언트 모듈 및 프로파일 값을 그룹 정책에 따라 업데이트할 수 있습니다.
- Management Center에서 직접 인증서를 매핑해야 합니다.
- IKEv2 매개변수는 기본적으로 마이그레이션되지 않습니다. Management Center를 통해 추가해야 합니다.

ASA 마이그레이션 지침

ACL 로그 옵션의 마이그레이션은 Firewall Threat Defense의 모범 사례를 따릅니다. 규칙에 대한 로그 옵션은 소스 ASA 컨피그레이션에 따라 활성화되거나 비활성화됩니다. **deny(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

와 Firewall Threat Defense는 개체에 대한 구성 지침이 서로 다릅니다. 예를 들어 예서는 한 개체의 이름이 소문자, 다른 개체의 이름이 대문자로 되어 있다면 하나 이상의 개체가 동일한 이름을 가질 수 있지만, Firewall Threat Defense에서는 대소문자에 관계없이 각 개체가 고유한 이름을 가져야 합니다. 이러한 차이를 수용하기 위해 Secure Firewall 마이그레이션 툴은 모든 개체를 분석하고 다음 방법 중 하나로 마이그레이션을 처리합니다.

- 각 개체에 고유한 이름과 구성이 있음 - Secure Firewall 마이그레이션 툴은 변경 없이 개체를 마이그레이션합니다.
- 개체의 이름에 Firewall Management Center에서 지원하지 않는 특수 문자가 하나 이상 포함되어 있음 - Secure Firewall 마이그레이션 툴은 개체 이름의 특수 문자 이름을 "_" 문자로 변경하여 Management Center 개체 명명 기준을 충족합니다.
- 개체에 Firewall Management Center의 기존 개체와 동일한 이름과 구성이 있음 - Secure Firewall 마이그레이션 툴은 Secure Firewall Threat Defense 구성에 해당 Secure Firewall Management Center 개체를 재사용하고 개체를 마이그레이션하지 않습니다.
- 의 기존 개체와 이름이 같지만 구성이 다른 Secure Firewall Management Center 개체가 있음 - Secure Firewall 마이그레이션 툴에서 개체 충돌이 보고되며 마이그레이션을 위해 개체 이름에 고유한 접미사를 추가하여 충돌을 해결할 수 있도록 합니다.
- 여러 개체가 대소문자가 다르지만 이름이 같음 - Secure Firewall 마이그레이션 툴이 Secure Firewall Threat Defense 개체 명명 기준에 맞게 이름을 바꿉니다.



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



참고 Secure Firewall 마이그레이션 툴은 대상 Firewall Management Center가 7.1 이상인 경우 불연속 네트워크 마스크(와일드카드 마스크) 개체 마이그레이션을 지원합니다.

ASA example:
object network wildcard2
subnet 2.0.0.2 255.0.0.255

ASA WebVPN에서 ZTA로의 마이그레이션에 대한 지침 및 제한 사항

ASA WebVPN에서 ZTA로의 마이그레이션을 시도하기 전에 다음 사항을 자세히 읽어보십시오.

- Management Center 및 Threat Defense 디바이스는 버전 7.4 이상에서 실행 중이어야 합니다.
- 대상 Threat Defense 디바이스는 Snort3을 탐지 엔진으로 사용 중이어야 합니다.
- ASA 트러스트 포인트 인증서(IdP 및 사전 인증)는 마이그레이션 전에 대상 Management Center에 수동으로 업로드해야 합니다.
- 마이그레이션 전에 애플리케이션 SSL 인증서와 개인 키를 대상 Management Center에 업로드해야 합니다.
- 로컬, RADIUS 및 LDAP 인증 방법은 지원되지 않습니다.
- Threat Defense 디바이스에는 하나의 ZTA 정책만 할당할 수 있습니다.

Firewall Threat Defense 디바이스 관련 지침 및 제한 사항

ASA 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 ASA 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 ASA 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 ASA 컨피그레이션에 다음 인터페이스 및 포트 채널이 할당된 경우 마이그레이션 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.

- Secure Firewall 마이그레이션 툴은 ASA 구성을 기반으로 하는 Firewall Threat Defense 디바이스의 네이티브 인스턴스에서 하위 인터페이스 및 브리지 그룹 가상 인터페이스(투명 모드)를 생성할 수 있습니다. 마이그레이션을 시작하기 전에 대상 Firewall Threat Defense 디바이스에서 인터페이스 및 포트 채널 인터페이스를 수동으로 생성합니다. 예를 들어 ASA 컨피그레이션에 다음 인터페이스 및 포트 채널이 할당된 경우 마이그레이션 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 ASA 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 ASA 디바이스를 독립형 Firewall Threat Defense 디바이스로 마이그레이션하는 것만 지원합니다.

지원되는 소스 **ASA** 플랫폼

Secure Firewall 마이그레이션 툴을 사용하여 다음과 같은 단일 또는 멀티 컨텍스트 ASA 플랫폼에서 컨피그레이션을 마이그레이션할 수 있습니다.

- ASA5510
- ASA 5520
- ASA 5540

- ASA 5550
- ASA 5580
- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA가 포함된 ASA 5585-X 전용(Secure Firewall 마이그레이션 툴은 ASA FirePOWER 모듈에서 구성을 마이그레이션하지 않음)
- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- 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 ASA 가상

지원되는 대상 **Firewall Threat Defense** 플랫폼

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

- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- 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 (ASA 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](#), [45 페이지](#)에 설명된 대로 마이그레이션에 지원되는 Management Center 소프트웨어 버전.
- 다음에 설명된 대로 ASA 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 Control는 보안 디바이스 커넥터(SDC)를 통해 클라우드 제공 Firewall Management Center에 연결합니다. 클라우드 제공 Firewall Management Center에 대한 자세한 내용은 [클라우드 제공 Firewall Management Center를 사용하여 Cisco Secure Firewall Threat Defense 디바이스 관리](#)를 참조하십시오.

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, ASA 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 **ASA** 버전

Secure Firewall 마이그레이션 툴은 ASA 소프트웨어 버전 8.4 이상을 실행하는 디바이스에서 마이그레이션을 지원합니다.

소스 **ASA** 컨피그레이션에 지원되는 **Firewall Management Center** 버전

ASA의 경우 Secure Firewall 마이그레이션 툴은 6.2.3 또는 6.2.3 이상 버전을 실행하는 Firewall Management Center에서 관리되는 Firewall Threat Defense 디바이스로의 마이그레이션을 지원합니다.



참고 일부 기능은 Firewall Management Center 및 Firewall Threat Defense의 최신 버전에서만 지원됩니다.



참고 마이그레이션 시간을 최적화하기 위해 Firewall Management Center를 software.cisco.com/downloads에서 제공하는 권장 릴리스 버전으로 업그레이드하는 것이 좋습니다.

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.

관련 설명서

이 섹션에는 ASA-Firewall Threat Defense 마이그레이션 관련 문서가 요약되어 있습니다.

- [Cisco Secure Firewall ASA-Threat Defense 기능 매핑](#) - 자주 사용되는 ASA 기능과 이에 상응하는 위협 방어 기능을 나열합니다. 각 ASA 기능의 경우, 동등한 위협 방어 기능은 UI 경로가 있어 Secure Firewall Management Center 또는 클라우드 제공 Firewall Management Center에서 구성할 수 있는 목록을 나열합니다.
- [ASA에서 Firepower Threat Defense로 인증서 마이그레이션](#) - Cisco ASA에서 Secure Firewall Threat Defense 디바이스로 ID 및 CA(Certificate Authority) 인증서를 마이그레이션하는 절차를 설명합니다.
- [인증서와 함께 IKEv1을 사용하여 ASA를 Firepower Threat Defense Site-to-Site VPN으로 마이그레이션](#) - 인증서(rsa-sig)를 인증 방법으로 사용하여 기존 Cisco ASA로부터 Firewall Management Center에서 관리되는 Firewall Threat Defense로 사이트 대 사이트 IKEv1 VPN 터널을 마이그레이션하는 절차를 설명합니다.
- [인증서와 함께 IKEv2를 사용하여 ASA를 Firepower Threat Defense Site-to-Site VPN으로 마이그레이션](#) - 인증서(rsa-sig)를 인증 방법으로 사용하여 기존 ASA로부터 Firewall Management Center에서 관리하는 Firewall Threat Defense로 사이트 대 사이트 IKEv2 VPN 터널을 마이그레이션하는 절차를 설명합니다.
- [ASA를 FTD의 Firepower Threat Defense 유동 암호화 맵 기반 사이트 대 사이트 터널로 마이그레이션](#) - 사전 공유 키와 인증서를 인증 방법으로 사용하여 기존 ASA에서 Firewall Threat Defense(Firewall Management Center를 통해 관리)로 유동 암호화 맵 기반 사이트 대 사이트 VPN 터널(IKEv1 또는 IKEv1 사용)을 마이그레이션하는 절차를 설명합니다.
- [사전 공유 키 인증과 함께 IKEv1을 사용하여 ASA를 Firepower Threat Defense Site-to-Site VPN으로 마이그레이션](#) - PSK(Pre-Shared Key)를 인증 방법으로 사용하여 기존 ASA로부터 Firewall Management Center에서 관리하는 Firewall Threat Defense로 사이트 대 사이트 IKEv1 VPN 터널을 마이그레이션하는 절차를 설명합니다.
- [사전 공유 키 인증과 함께 IKEv2를 사용하여 ASA를 Firepower Threat Defense Site-to-Site VPN으로 마이그레이션](#) - PSK(Pre-Shared Key)를 인증 방법으로 사용하여 기존 ASA로부터 Firewall Management Center에서 관리하는 Firewall Threat Defense로 사이트 대 사이트 IKEv2 VPN 터널을 마이그레이션하는 절차를 설명합니다.
- [ASA를 Firepower Threat Defense 플랫폼 설정으로 마이그레이션](#) - ASA의 플랫폼 설정 컨피그레이션을 Firewall Threat Defense 디바이스로 마이그레이션하는 단계를 설명합니다.

- [Cisco ASA FirePOWER 모듈 빠른 시작 가이드](#)—ASA FirePOWER 모듈이 ASA에서 작동하는 방식을 설명합니다.



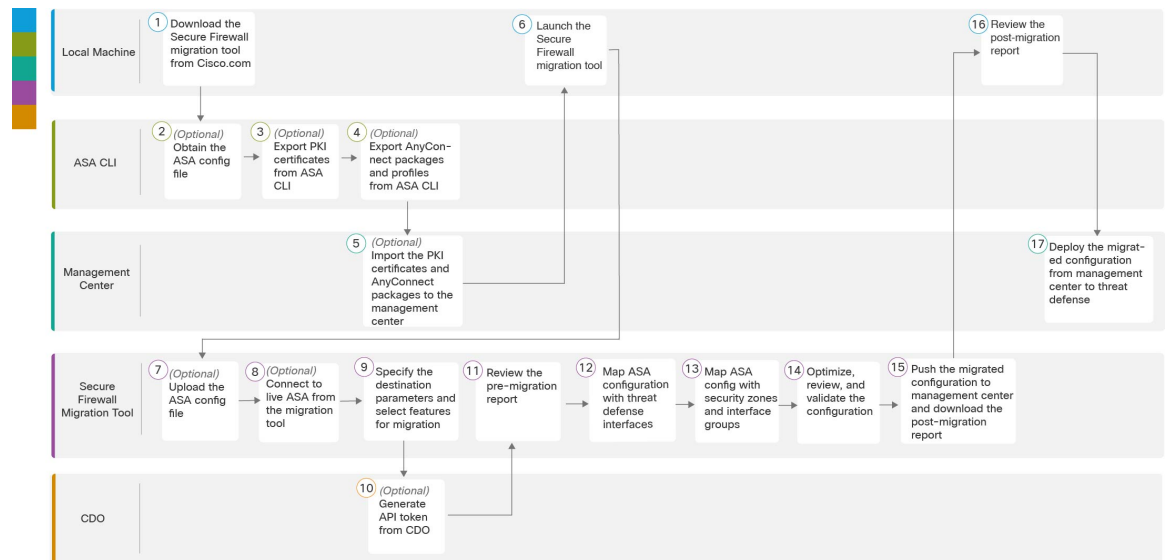
2 장

ASA를 Threat Defense로 마이그레이션 워크플로우

- 엔드 투 엔드 절차, 49 페이지
- 마이그레이션 사전 요건, 51 페이지
- 마이그레이션 실행, 55 페이지
- Secure Firewall 마이그레이션 툴 제거, 100 페이지
- 샘플 마이그레이션: ASA 를 Threat Defense 2100으로 , 101 페이지

엔드 투 엔드 절차

다음 순서도는 Secure Firewall 마이그레이션 툴을 사용하여 ASA를 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 다운로드 를 참고하십시오.
②	ASA CLI	(선택 사항) ASA 구성 파일 가져오기: ASA CLI에서 ASA 구성 파일을 가져오려면 ASA 구성 파일 가져오기 를 참고하십시오. Secure Firewall 마이그레이션 툴에서 ASA를 연결하려는 경우 3단계로 건너뛵니다.
③	ASA CLI	(선택 사항) ASA CLI에서 PKI 인증서 내보내기: 이 단계는 사이트 대 사이트 VPN, RA VPN 또는 WebVPN 구성을 ASA에서 Threat Defense로 마이그레이션하려는 경우에만 필요합니다. ASA CLI에서 PKI 인증서를 내보내려면 Firewall Management Center에서 PKI 인증서 내보내기 및 Firewall Management Center로 가져오기 , 1단계를 참고하십시오. 사이트 간 VPN, RA VPN 또는 WebVPN을 마이그레이션할 계획이 없는 경우 7단계로 건너뛵니다.
④	ASA CLI	(선택 사항) ASA CLI에서 AnyConnect 패키지 및 프로파일 내보내기: 이 단계는 RA VPN 기능을 ASA에서 Threat Defense로 마이그레이션하려는 경우에만 필요합니다. ASA CLI에서 AnyConnect 패키지 및 프로파일을 내보내려면 AnyConnect 패키지 및 프로파일 검색 , 1단계를 참고하십시오. 사이트 간 VPN 및 RA VPN을 마이그레이션할 계획이 없는 경우 7단계로 건너뛵니다.
⑤	Management Center	(선택 사항) PKI 인증서 및 AnyConnect 패키지를 Management Center로 가져오기: PKI 인증서를 Management Center로 가져오려면 Firewall Management Center에서 PKI 인증서 내보내기 및 Firewall Management Center로 가져오기 , 2단계 및 AnyConnect 패키지 및 프로파일 검색 , 2단계를 참고하십시오.
⑥	로컬 컴퓨터	로컬 컴퓨터에서 Secure Firewall 마이그레이션 툴을 실행합니다(Secure Firewall 마이그레이션 툴 실행 참조).
⑦	Secure Firewall 마이그레이션 툴	(선택 사항) ASA CLI에서 가져온 ASA 구성 파일을 업로드합니다. ASA 구성 파일 업로드 를 참고하십시오. 라이브 ASA에 연결하려는 경우 8단계로 건너뛵니다.
⑧	Secure Firewall 마이그레이션 툴	Secure Firewall 마이그레이션 툴에서 라이브 ASA에 직접 연결할 수 있습니다. 자세한 내용은 Secure Firewall 마이그레이션 툴에서 ASA에 연결 을 참고하십시오.
⑨	Secure Firewall 마이그레이션 툴	이 단계에서 마이그레이션의 대상 매개변수를 지정할 수 있습니다. 자세한 단계는 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정 을 참고하십시오.

	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 ASA 구성을 Threat Defense 인터페이스와 매핑할 수 있습니다. 자세한 단계는 Secure Firewall Device Manager Threat Defense 인터페이스와 ASA 구성 매핑 을 참고하십시오.
⑬	Secure Firewall 마이그레이션 툴	ASA 구성이 올바르게 마이그레이션되도록 하려면 ASA 인터페이스를 적절한 위협 방어 인터페이스 개체, 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 단계는 ASA 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

ASA 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 건너뛰니다.

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

[ASA 컨피그레이션 파일 가져오기](#)

구성 파일 가져오기

다음 방법 중 하나를 사용하여 컨피그레이션 파일을 가져올 수 있습니다.

- [컨피그레이션 파일 내보내기, 53 페이지](#)
- [Secure Firewall 마이그레이션 툴에서 ASA에 연결, 59 페이지](#)

컨피그레이션 파일 내보내기

이 작업은 컨피그레이션 파일을 수동으로 업로드하려는 경우에만 필요합니다. Secure Firewall 마이그레이션 툴에서 에 연결하려면 [Secure Firewall 마이그레이션 툴에서 ASA에 연결, 59 페이지](#)로 건너뛵니다.



참고 파일을 내보낸 후에는 직접 코딩하거나 컨피그레이션을 변경하지 마십시오. 이러한 변경 사항은 마이그레이션되지 않으며 마이그레이션에 오류를 일으키거나 실패를 초래합니다. 예를 들어 터미널에서 구성 파일을 열고 저장하면 Secure Firewall 마이그레이션 툴에서 구문 분석할 수 없는 공백 또는 빈 라인이 추가될 수 있습니다.

내보낸 구성 파일에 **--More--** 키워드가 텍스트로 포함되어 있지 않은지 확인하십시오. 이 키워드로 인해 마이그레이션이 실패할 수 있습니다.

프로시저

단계 1 마이그레이션하는 ASA 디바이스 또는 컨텍스트에 대해 **show running-config** 명령을 사용하고 여기에서 컨피그레이션을 복사합니다. **실행 중인 컨피그레이션 보기**를 참고하십시오.

또는 마이그레이션하려는 ASA 디바이스 또는 컨텍스트에 대해 ASDM(Adaptive Security Device Manager)을 사용하고 **File(파일) > Show Running Configuration in New Windows(실행 중인 컨피그레이션 표시)**를 선택하여 컨피그레이션 파일을 가져옵니다.



참고 멀티 컨텍스트의 경우 **show tech-support** 명령을 사용하여 모든 컨텍스트에 대한 컨피그레이션을 단일 파일로 가져올 수 있습니다.

단계 2 컨피그레이션을 .cfg 또는 .txt로 저장합니다.

다른 확장명을 갖는 경우 Secure Firewall 마이그레이션 툴에 구성을 업로드할 수 없습니다.

단계 3 Secure Firewall 마이그레이션 툴을 다운로드한 컴퓨터로 구성 파일을 전송합니다.

ASA 에서 PKI 인증서 내보내기 및 Management Center로 가져오기

시작하기 전에

Secure Firewall 마이그레이션 툴은 Management Center로의 인증서 기반 VPN 마이그레이션을 지원합니다.

ASA에서는 구성에 인증서를 저장하기 위해 트러스트 포인트 모델을 사용합니다. 트러스트 포인트는 인증서가 저장되는 컨테이너입니다. ASA 트러스트 포인트는 최대 2개의 인증서를 저장할 수 있습니다.

ASA 구성 파일의 ASA 트러스트 포인트 또는 인증서에 해시 값이 포함되어 있습니다. 따라서 Management Center로 직접 가져올 수 없습니다.

대상 Management Center에서 마이그레이션 전 활동의 일부로 ASA 트러스트 포인트 또는 VPN 인증서를 PKI 개체로 수동으로 마이그레이션합니다.

프로시저

단계 1 다음 명령을 사용하여 CLI를 통해 키가 있는 소스 ASA 구성에서 PKCS12 파일로 PKI 인증서를 내보냅니다.

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

단계 2 PKI 인증서를 Management Center(Object Management(개체 관리) PKI Objects(PKI 개체))로 가져옵니다.

자세한 내용은 [Firepower Management Center 구성 가이드](#)를 참조하십시오.

수동으로 생성한 PKI 개체는 이제 **Optimize, Review and Validate**(최적화, 검토 및 검증) 페이지의 **Remote Access VPN**(원격 액세스 VPN)의 **Trustpoint**(트러스트 포인트) 섹션에 있는 Secure Firewall 마이그레이션 툴에서 사용할 수 있습니다.

AnyConnect 패키지 및 프로파일 검색

AnyConnect 프로파일은 선택 사항이며, Management Center 또는 Secure Firewall 마이그레이션 툴을 통해 업로드할 수 있습니다.

시작하기 전에

- Management Center의 원격 액세스 VPN에는 하나 이상의 AnyConnect 패키지가 필요합니다.
- 구성이 Hostscan 및 외부 브라우저 패키지로 구성된 경우 이러한 패키지를 업로드해야 합니다.
- 모든 패키지는 마이그레이션 전 활동의 일부로 Management Center에 추가해야 합니다.
- Dap.xml 및 Data.xml은 Secure Firewall 마이그레이션 툴을 통해 추가해야 합니다.

프로시저

단계 1 다음 명령을 사용하여 소스 ASA에서 필요한 패키지를 FTP 또는 TFTP 서버로 복사합니다.

```
Copy <source file location:/source file name> <destination>
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Example
of copying Anyconnect Package.
ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Example
of copying External Browser Package.
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example of copying
Hostscan Package.
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect
Profile.
```

단계 2 다운로드한 패키지를 Management Center(Object Management(개체 관리) >) > VPN > AnyConnect File(AnyConnect 파일)로 가져옵니다.

1. Dap.xml 및 Data.xml을 **Review and Validate**(검토 및 검증) > **Remote Access VPN**(원격 액세스 VPN) > **AnyConnect File**(AnyConnect 파일) 섹션을 통해 Secure Firewall 마이그레이션 툴에서 Management Center로 업로드해야 합니다.
2. AnyConnect 프로파일은 Management Center에 직접 업로드하거나 **Review and Validate**(검토 및 검증) > **Remote Access VPN**(원격 액세스 VPN) > **AnyConnect File**(AnyConnect 파일)의 Secure Firewall 마이그레이션 툴을 통해 업로드할 수 있습니다.

수동으로 업로드한 파일을 이제 Secure Firewall 마이그레이션 툴에서 사용할 수 있습니다.

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, [ASA 구성 파일 업로드](#), [58 페이지](#)로 건너뛵니다.



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](#), [43 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.

- 컨피그레이션을 컴퓨터로 내보낸 경우 **Upload the Configuration File**(컨피그레이션 파일 업로드)를 진행합니다.

- Secure Firewall 마이그레이션 툴을 사용하여 예서 정보를 추출하려면 [Secure Firewall 마이그레이션 툴에서 ASA에 연결, 59 페이지](#)로 진행합니다.

Secure Firewall 마이그레이션 툴에서 데모 모드 사용

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

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



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

또한 실제 마이그레이션 워크플로우에서와 마찬가지로 마이그레이션 전 보고서를 다운로드하여 확인하고, 인터페이스를 매핑하고, 보안 영역을 매핑하고, 인터페이스 그룹을 매핑하는 등 모든 작업을 수행할 수 있습니다. 그러나 구성 검증까지만 데모 마이그레이션을 수행할 수 있습니다. 선택한 데모 대상 디바이스는 데모 모드이므로 구성을 푸시할 수 없습니다. 검증 상태 및 요약을 확인하고 **Exit Demo Mode**(데모 모드 종료)를 클릭하여 **Select Source Configuration**(소스 구성 선택) 페이지로 다시 이동하여 실제 마이그레이션을 시작할 수 있습니다.



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

ASA 구성 파일 업로드

시작하기 전에

소스 ASA 디바이스에서 구성 파일을 .cfg 또는 .txt로 내보냅니다.



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

프로시저

단계 1 **Extract(추출) ASA Information(정보)** 페이지의 **Manual Upload(수동 업로드)** 섹션에서 **Upload(업로드)**를 클릭하여 ASA 구성 파일을 업로드합니다.

단계 2 구성 파일이 있는 위치로 이동하여 **Open(열기)**을 클릭합니다.

Secure Firewall 마이그레이션 툴이 컨피그레이션 파일을 업로드합니다. 대규모 컨피그레이션 파일의 경우 이 단계는 시간이 더 오래 걸립니다. 콘솔에서는 구문 분석 중인 ASA 구성 라인을 포함하여 진행 상황의 라인별 로그 보기를 제공합니다. 콘솔이 표시되지 않는 경우 Secure Firewall 마이그레이션 툴 뒤의 별도 창에서 콘솔을 찾을 수 있습니다.

Context Selection(컨텍스트 선택) 섹션에는 업로드된 구성이 멀티 컨텍스트 ASA에 해당하는지 여부가 나와 있습니다.

단계 3 **Context Selection(컨텍스트 선택)** 섹션을 검토하고 마이그레이션할 컨텍스트를 선택합니다.

다음에 수행할 작업

[Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 62 페이지](#)

Secure Firewall 마이그레이션 툴에서 ASA에 연결

Secure Firewall 마이그레이션 툴은 마이그레이션할 ASA 디바이스에 연결하여 필요한 구성 정보를 추출할 수 있습니다.

시작하기 전에

- Secure Firewall 마이그레이션 툴을 다운로드하여 실행합니다.
- 단일 컨텍스트 ASA의 경우 관리 IP 주소, 관리자 자격 증명 및 활성화 비밀번호를 가져옵니다.
- 멀티 컨텍스트 모드 ASA의 경우 관리자 컨텍스트의 IP 주소, 관리자 자격 증명 및 활성화 비밀번호를 가져옵니다.



참고 ASA에 **Enable Password(활성화 비밀번호)**가 구성되지 않은 경우 Secure Firewall 마이그레이션 툴에서 필드를 비워 둘 수 있습니다.

프로시저

단계 1 **Extract ASA Information(ASA 정보 추출)** 화면의 **Connect to ASA(ASA에 연결)** 섹션에서 **Connect(연결)**를 클릭하여 마이그레이션할 ASA 디바이스에 연결합니다.

단계 2 **ASA Login(ASA 로그인)** 화면에서 다음 정보를 입력합니다.

1. **ASA IP Address/Hostname(ASA IP 주소/호스트 이름)** 필드에 관리 IP 주소 또는 호스트 이름(단일 컨텍스트 ASA의 경우) 또는 관리자 컨텍스트 IP 주소 또는 호스트 이름(멀티 컨텍스트 ASA의 경우)을 입력합니다.
2. **Username(사용자 이름), Password(비밀번호) 및 Enable Password(활성화 비밀번호)** 필드에 해당 관리자 로그인 자격 증명을 입력합니다.



참고 ASA에 **Enable Password(활성화 비밀번호)**가 구성되지 않은 경우 Secure Firewall 마이그레이션 툴에서 필드를 비워 둘 수 있습니다.

3. **Login(로그인)**을 클릭합니다.

Secure Firewall 마이그레이션 툴이 ASA에 연결되면 ASA에 성공적으로 연결되었다는 메시지가 표시됩니다.

멀티 컨텍스트 ASA의 경우 Secure Firewall 마이그레이션 툴이 컨텍스트를 식별하고 나열합니다.

단계 3 **Context(컨텍스트)** 드롭다운 목록에서 마이그레이션할 ASA 컨텍스트를 선택합니다.

단계 4 (선택 사항) **Collect Hitcounts(적중 횟수 수집)**를 선택합니다.

이 옵션을 선택하면 Firepower 마이그레이션 툴에서 ASA 규칙이 사용된 횟수와 ASA 업타임 또는 최종 ASA 재시작 이후 마지막으로 규칙이 사용된 시간을 계산하여 이 정보를 **Review and Validate(검토 및 검증)** 페이지에 표시합니다. 이를 통해 마이그레이션 전에 규칙의 효율성과 관련성을 평가할 수 있습니다.

단계 5 **Start Extraction(추출 시작)**을 클릭합니다.

Secure Firewall 마이그레이션 툴이 ASA에 연결되고 구성 정보 추출을 시작합니다. 추출이 성공적으로 완료되면 업로드된 컨피그레이션이 단일 컨텍스트 ASA와 멀티 컨텍스트 ASA 중 어느 것에 해당하는지가 **Context Selection(컨텍스트 선택)** 섹션에 표시됩니다.

ASA 보안 컨텍스트 선택

시작하기 전에

단일 ASA 디바이스를 다중 가상 장치로 분할할 수 있으며 이러한 파티션을 보안 컨텍스트라고 합니다. 각 보안 상황은 각자 보안 정책, 인터페이스, 관리자가 있는 독립적인 디바이스의 역할을 합니다. 다중 컨텍스트는 실제로는 단 하나의 디바이스만 있음에도 불구하고, 마치 여러 대의 독립형 디바이스가 있는 것과 비슷합니다. 보안 컨텍스트에 대해 자세히 알아보려면 *Cisco ASA* 시리즈 일반 운영 CLI 컨피그레이션 가이드의 **보안 컨텍스트의 일반적인 용도**를 참조하십시오.

이 작업 절차는 Cisco Secure Firewall ASA에서 둘 이상의 보안 컨텍스트를 구성한 경우에 적용됩니다. ASA 구성을 업로드할 때 Secure Firewall 마이그레이션 툴은 디바이스에서 보안 상황을 탐지하고, 컨

텍스트에 관련된 모든 구성 정보를 구문 분석하여 **Context Selection**(컨텍스트 선택) 페이지에 표시합니다.

프로시저

단계 1 ASA 구성 파일을 업로드합니다. 구성 파일에 컨텍스트가 포함된 경우 마이그레이션 툴은 모든 보안 컨텍스트의 이름을 표시합니다.

그림 1: **Cisco ASA(8.4+)** 정보창 추출

Extract Cisco ASA (8.4+) Information ⓘ Source: Cisco ASA (8.4+)

Extraction Methods >

Context Selection ▾

Choose (One from below)

☐ Context Migration (One at a time) ☒ Merge Multi-Context to Single Instance

Note - Choose at least two contexts of the same type (routed or transparent) for merging.

☐ Select All 13 Contexts - Routed ☐ Select All 0 Contexts - Transparent

Context Selection	Context Name & Type	#Config Lines	#ACLs	#Objects	#NATs	#Routes	#Interfaces	#VPN
☐	fw103-vc002 (R)	14196	4150	1989	16	38	31	0
☐	fw103-vc004 (R)	9444	2402	1319	0	62	37	0
☐	fw103-vc007 (R)	5083	1519	627	44	231	12	0

Back Next

단계 2 (선택 사항) 컨텍스트 중 하나에서 구성을 마이그레이션하려면 **Context Migration (One at a time)**(컨텍스트 마이그레이션(한 번에 하나씩)) 라디오 버튼을 클릭하고 컨텍스트를 선택하여 마이그레이션을 계속 진행합니다.

단계 3 (선택 사항) 여러 컨텍스트의 설정을 단일 인스턴스로 병합하고 마이그레이션하려면 다음을 수행합니다.



참고 여러 컨텍스트 병합을 시도하기 전에 다음 사전 요건을 읽어보십시오.

- ASA에 포트 채널이 구성되어 있는 경우 대상 Firewall Threat Defense 디바이스에서도 포트 채널이 구성되어 있는지 확인합니다.
- 두 인터페이스의 VLAN ID 및 하위 인터페이스 ID가 동일한 경우 마이그레이션 툴은 새 인터페이스에 새 VLAN 및 하위 인터페이스 ID를 자동으로 추가합니다. 이러한 ID에 대한 정보는 마이그레이션 전 보고서의 일부입니다. 마이그레이션 툴로 생성한 새 인터페이스를 해당 디바이스의 트렁크 포트 개체로 구성해야 합니다. 이는 Firewall Threat Defense 디바이스가 동일한 VLAN 및 하위 인터페이스 ID를 가진 두 개의 인터페이스를 허용하지 않기 때문입니다.
- AS 경로 개체는 마이그레이션되는 모든 컨텍스트에서 고유해야 합니다. 중복은 마이그레이션되지 않습니다.

- a) **Merge Multi-Context to Single Instance**(멀티 컨텍스트를 단일 인스턴스로 병합) 라디오 버튼을 클릭합니다. 멀티컨텍스트 병합을 선택하는 경우 설정 라인 수, ACL, 개체, 정적 경로를 포함한 경로, PBR 및 ECMP, 인터페이스 등의 컨텍스트 정보를 볼 수 있습니다.
- b) 모든 라우팅 모드 방화벽 컨텍스트를 병합하려면 **Select All Context - Routed**(모든 컨텍스트 선택 - 라우팅) 체크 박스를 선택하고 모든 투명 모드 방화벽 컨텍스트를 병합하려면 **Select All Context - Transparent**(모든 컨텍스트 선택 - 투명) 체크 박스를 선택합니다.



참고 여러 컨텍스트를 병합할 때 병합하기 위해 선택한 둘 이상의 컨텍스트에 VPN이 구성된 경우 마이그레이션 툴은 VPN 구성을 사용하여 컨텍스트 중 하나를 선택하라는 프롬프트를 표시합니다. 선택한 컨텍스트의 VPN 설정만 마이그레이션되고 다른 컨텍스트의 VPN 설정은 무시됩니다. 그러나 개체, 확장 ACL, NAT 규칙 및 선택되지 않은 컨텍스트에서 참조되지 않은 VPN 개체와 같은 다른 모든 구성은 계속 마이그레이션됩니다.

단계 4 Start Parsing(구문 분석 시작)을 클릭합니다. 컨텍스트를 선택하고 구문 분석을 시작하면 마이그레이션 툴은 모든 컨텍스트의 구성을 병합하고 구문 분석하며 **Parsed Summary**(구문 분석 요약)를 표시합니다. 병합 컨텍스트 마이그레이션을 수행하는 경우, 마이그레이션하도록 선택한 컨텍스트의 수는 구문 분석된 요약에 있는 VRF의 수와 동일합니다. 그러나 VPN 구성이 있는 컨텍스트가 있는 경우 VPN 구성이 있는 VRF는 글로벌 라우터에 직접 푸시되므로 구문 분석된 요약은 하나의 VRF를 덜 표시합니다.



참고 **Start Parsing**(구문 분석 시작)을 클릭한 상태에서 다른 컨텍스트를 선택하려는 경우, 이전으로 돌아가 다른 컨텍스트를 선택할 수 없습니다. **Back**(뒤로)을 클릭하고 구성 파일 업로드부터 시작하여 이번에는 다른 컨텍스트를 선택할 수 있습니다.

단계 5 업로드된 구성 파일에서 Secure Firewall 마이그레이션 툴이 감지하고 구문 분석한 요소에 대한 요약을 검토합니다.

단계 6 Next(다음)를 클릭하여 대상 매개변수를 선택합니다.

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.
- **관리 액세스를 위한 사용자 어카운트**에 설명된 대로 Firewall Management Center에서 REST API에 액세스할 수 있는 충분한 권한이 있는 Secure Firewall 마이그레이션 툴 전용 사용자를 생성합니다.
- (선택 사항) 인터페이스 및 경로와 같은 디바이스별 구성을 마이그레이션하려면 대상을 추가합니다. Firewall Threat Defense인 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 2단계로 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.

- Security Cloud Control에 로그인합니다.
- 오른쪽 상단에서 **Preferences**(환경 설정) > **General Preferences**(일반 환경설정)로 이동하여 **My Tokens**(내 토큰) 섹션의 API 토큰을 복사합니다.

- 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.

Choose Threat Defense(Threat Defense 선택) 섹션에서 마이그레이션할 Firewall Threat Defense 디바이스를 선택하거나 Firewall Threat Defense 디바이스가 없는 경우 ASA 구성의 공유 정책(액세스 제어 목록, NAT 및 개체)을 Firewall Management Center로 마이그레이션할 수 있습니다.

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

- **Select FTD Device(FTD 디바이스 선택)****Select FTD Device (Includes FTD - Standalone/HA Pair)(FTD 디바이스 선택(FTD - 독립형/HA 쌍 포함))** 드롭다운 목록을 클릭하고 ASA 구성을 마이그레이션할 디바이스를 선택합니다.



참고 이 목록에는 독립형 위협 방어 디바이스와 대상 Firewall Management Center의 고가용성(HA) 쌍의 일부인 디바이스가 모두 포함됩니다.

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 ASA 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. ASA 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.

표 2: ASA 방화벽 기능 및 지원되는 **Firewall Management Center** 또는 **Firewall Threat Defense** 버전

방화벽 기능	지원되는 Management Center 또는 Threat Defense 버전
원격 구축으로	6.7 이상
암호화 맵 사이트 간 VPN	6.6 이상
Virtual Tunnel Interface(VTI) 및 경로 기반 (VTI)	6.7 이상
유동 경로 개체 및 BGP	7.1 이상
원격 액세스 VPN	• Management Center 7.2 이상 • Threat Defense 7.0 이상
EIGRP	• Management Center 7.2 이상 • Threat Defense 7.0 이상
PBR	• Management Center 7.3 이상 • Threat Defense 7.3 이상
ECMP	• Management Center 7.1 이상 • Threat Defense 6.5 이상
WebVPN	• Management Center 7.4 이상 • Threat Defense 7.4 이상
SNMP	• Management Center 7.4 이상 • Threat Defense 7.4 이상
DHCP 릴레이, 서버 및 DDNS	• Management Center 7.4 이상 • Threat Defense 7.4 이상



참고 사이트 간 VPN, VTI 및 경로 기반 (VTI) 인터페이스를 마이그레이션하려면 Firewall Threat Defense를 Firewall Management Center에 구성해야 합니다.

- ASA 5505의 경우, 지원되는 대상 Firewall Threat Defense 플랫폼이 Firewall Management Center 6.5 이상 버전을 실행하는 Firewall 1010인 경우에만 디바이스별 구성(인터페이스 및 경로) 및 공유 정책(NAT, ACL 및 개체)을 마이그레이션할 수 있습니다.



참고

- 대상 Firewall Threat Defense가 FPR-1010이 아니거나 대상 Firewall Management Center가 6.5 이전 버전인 경우, ASA 5505 마이그레이션 지원은 공유 정책에만 적용됩니다. 디바이스 관련 정보는 마이그레이션되지 않습니다.
 - 소스 구성이 ASA 5505이므로 **Select Device**(디바이스 선택) 드롭다운 목록에서 FPR-1010만 선택할 수 있습니다.
 - ASA-SM 마이그레이션 지원은 공유 정책에만 적용됩니다. 디바이스 관련 정보는 마이그레이션되지 않습니다.
-
- 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.
 - 이 옵션은 소스 ASA 디바이스가 HA 쌍에 있는 경우에만 표시됩니다.
Proceed with FTD HA Pair Configuration(FTD HA 쌍 구성 진행) 클릭하여 HA 쌍에 대한 액티브 및 스탠바이 위협 방어 디바이스를 선택합니다. 액티브 디바이스를 선택할 때 FMT가 스탠바이 디바이스 옵션으로 동일한 디바이스를 표시하고 HA 쌍 생성이 성공하려면 대상 Firewall Management Center에 동일한 디바이스가 있는지 확인합니다.



참고

스탠바이 디바이스로 선택할 대상 Firewall Management Center에 동일한 디바이스가 없거나 대기 위협 방어 디바이스를 선택하지 않는 경우 마이그레이션의 추가 단계를 진행할 수 없습니다.

Setup FTD HA Pair(FTD HA 쌍 설정)를 클릭하고 **Configure Target FTDs in High Availability Pair(고가용성 쌍에서 대상 FTD 구성)** 창에서 다음을 구성합니다.

1. **HA Pair Name(HA 쌍 이름)** 필드에 HA 쌍의 이름을 지정합니다.
2. **High Availability Link(고가용성 링크)**에서 페일오버 통신을 수행해야 하는 경우 대역폭이 충분한 **Interface(인터페이스)**를 선택합니다.



참고

Interface(인터페이스) 드롭다운에는 논리적 이름이 없고 보안 영역의 일부가 아닌 인터페이스만 나열됩니다.

3. 인터페이스의 **Logical Name(논리적 이름)**을 지정합니다.
4. 액티브 디바이스 유닛에서 고가용성 링크에 대한 **Primary IP(기본 IP)** 주소를 지정합니다. IP 주소가 사용되지 않는 서브넷에 있는지 확인합니다.
5. 스탠바이 디바이스 유닛에서 고가용성 링크에 대한 **Secondary IP(보조 IP)** 주소를 지정합니다. 보조 IP 주소가 기본 IP 주소와 동일한 서브넷에 있는지 확인합니다.
6. 기본 및 보조 IP 주소에 적용되는 **Subnet Mask(서브넷 마스크)**를 입력합니다.
7. **State Link(상태 링크)**에서 **Same as LAN Failover Link(LAN 페일오버 링크와 동일)** 또는 다른 **Interface(인터페이스)**를 선택합니다. **Same as LAN Failover Link(LAN 페일오버 링크와 동일)**를 선택하면 방금 구성한 페일오버 링크의 데이터가 입력됩니다.
8. **IPsec Encryption(IPsec 암호화)** 아래의 **Enabled(활성화됨)** 체크 박스를 선택하여 페일오버 링크 사이에 암호화를 활성화하고 **Key Generation(키 생성)** 방법을 선택합니다.
9. **Add(추가)**를 클릭하여 HA 쌍 설정을 시작합니다.

HA 쌍 생성이 진행될 때까지 **Notifications Center**(알림 센터) 아이콘은 계속 깜박입니다. 어떤 이유로든 HA 쌍 생성에 실패하는 경우 FMT는 **Blocked**(차단됨) 오류 메시지를 표시하여 알림을 전송합니다. 이 경우 마이그레이션 툴이 HA 쌍 생성을 시도했는데 실패했으므로 Firewall Management Center는 HA 쌍을 생성하지만 성공하지 못합니다.

Firewall Management Center에 로그인하고 수동으로 HA를 중단한 다음 마이그레이션 툴의 오류 메시지에서 **Click here**(여기를 클릭)를 선택하여 HA 쌍 다시 구성을 시작합니다. HA 쌍을 분리하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 대상 Firewall Management Center가 온프레미스 방화벽 Management Center인 경우 [고가용성 쌍 분리](#)
- 대상 Firewall Management Center가 클라우드 제공 Firewall Management Center인 경우 [고가용성 쌍 분리](#)



참고 다른 마이그레이션 단계의 일부로 입력되거나 채워진 값은 HA 설정이 실패하여 다시 구성되는 경우에도 유지됩니다.

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 ASA 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 ASA 구성에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.
- Secure Firewall 마이그레이션 툴은 마이그레이션 중에 다음과 같은 액세스 제어 기능을 지원합니다.
 - 대상 보안 영역 채우기 - 마이그레이션 중에 ACL에 대한 대상 영역의 매핑을 활성화합니다. 경로 조회 논리는 정적 경로와 연결된 경로로 제한되며, PBR과 유동 경로, NAT는 고려되지 않습니다. 인터페이스 네트워크 컨피그레이션은 연결된 경로 정보를 도출하는 데 사용됩니다. 소스 및 대상 네트워크 개체 그룹의 특성에 따라 이 작업으로 인해 규칙이 급증할 수 있습니다.
 - 터널링된 규칙을 사전 필터로 마이그레이션 - ASA 캡슐화된 터널 프로토콜 규칙을 사전 필터 터널 규칙에 매핑하면 다음과 같은 이점이 있습니다.

- 심층 검사 맞춤화 - 캡슐화된 트래픽에 대해 가능하며 단축경로(Fastpath)를 지정하여 성능을 높일 수 있습니다.
- 성능 향상 - 조기에 처리하는 것이 유리한 그 밖의 연결도 단축경로를 지정하거나 차단할 수 있습니다.

Secure Firewall 마이그레이션 툴은 소스 구성에서 캡슐화된 터널 트래픽 규칙을 식별하고 이를 사전 필터 터널 규칙으로 마이그레이션합니다. 사전 필터 정책에서 마이그레이션된 터널 규칙을 확인할 수 있습니다. 사전 필터 정책은 Firewall Management Center에서 마이그레이션된 액세스 제어 정책과 연결됩니다.

사전 필터 터널 규칙으로 마이그레이션되는 프로토콜은 다음과 같습니다.

- GRE(47)
- IPv4 캡슐화(4)
- IPv6 캡슐화(41)
- Teredo 터널링(UDP:3544)



참고 사전 필터 옵션을 선택하지 않으면 모든 터널링된 트래픽 규칙이 지원되지 않는 규칙으로 마이그레이션됩니다.

ASA 구성의 ACL 터널 규칙(GRE 및 IPnIP)은 현재 기본적으로 양방향으로 마이그레이션됩니다. 이제 액세스 제어 상태 옵션에서 대상의 규칙 방향을 양방향 또는 단방향으로 지정할 수 있습니다.

- Secure Firewall 마이그레이션 툴은 VPN 터널 마이그레이션을 위해 다음 인터페이스 및 개체를 지원합니다.
 - 정책 기반(암호화 맵) - 대상 Firewall Management Center 및 Firewall Threat Defense가 버전 6.6 이상인 경우.
 - 경로 기반(VTI) - 대상 Firewall Management Center 및 Firewall Threat Defense가 버전 6.7 이상인 경우.
- Secure Firewall 마이그레이션 툴은 대상 Management Center가 7.2 이상인 경우 원격 액세스 VPN의 마이그레이션을 지원합니다. 원격 액세스 VPN은 Threat Defense 없이도 마이그레이션할 수 있는 공유 정책입니다. Threat Defense를 사용하여 마이그레이션을 선택한 경우 Threat Defense 버전은 7.0 이상이어야 합니다.
- (선택 사항) **Optimization(최적화)** 섹션에서 **Migrate only referenced objects**(참조된 개체만 마이그레이션)를 선택하여 액세스 제어 정책 및 NAT 정책에서 참조되는 개체만 마이그레이션합니다.



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

- (선택 사항) **Optimization(최적화)** 섹션에서 Firewall Threat Defense의 액세스 정책을 기준으로 최적의 메모리 사용률을 위한 **Object group search(개체 그룹 검색)**를 선택합니다.
- (선택 사항) **Inline Grouping(인라인 그룹화)** 섹션에서 Secure Firewall 마이그레이션 툴을 사용하면 CSM 또는 DM으로 시작하는 사전 정의된 네트워크 및 서비스 개체 이름의 액세스 규칙을 지울 수 있습니다. 이 옵션의 선택을 취소하면 마이그레이션 중에 사전 정의된 개체 이름이 유지됩니다. 자세한 내용은 [인라인 그룹화](#)를 참고하십시오.



참고 기본적으로 인라인 그룹화 옵션은 활성화되어 있습니다.

- 소스 ASA 디바이스에서 **SNMP** 및 **DHCP** 서버, 릴레이 및 **DDNS** 구성이 있는 경우 해당 확인란이 기본적으로 선택됩니다. 이러한 설정을 마이그레이션하지 않으려면 수동으로 선택을 취소합니다. DHCP를 선택하면 서버 또는 릴레이 및 **DDNS**를 모두 선택할 수 있습니다.
- SSL 클라이언트리스 VPN 터널 프로토콜 구성이 포함된 그룹 정책과 SAML 인증을 사용하는 그룹 정책이 포함된 터널 그룹이 있는 경우 마이그레이션 툴은 기본적으로 **WebVPN** 확인란을 선택합니다. 이러한 구성을 마이그레이션하지 않으려는 경우에는 이 확인란을 수동으로 선택 취소해야 합니다.

단계 7 **Proceed(진행)**를 클릭합니다.

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

단계 9 Secure Firewall 마이그레이션 툴에서 변환한 요소의 요약 검토합니다.

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

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

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

다음에 수행할 작업

[마이그레이션 전 보고서 검토, 72 페이지](#)

인라인 그룹화

ASDM 및 CSM으로 관리되는 ASA별 개체 그룹화

소스/수신 주소 또는 소스/대상 서비스에 둘 이상의 항목(개체 또는 인라인 값)을 입력할 경우, CSM 또는 ASDM에서는 개체 그룹을 자동으로 생성합니다. 각 ASA 디바이스에 컨피그레이션을 구축하는 동안 CSM 및 ASDM에서 사용되는 이러한 개체 그룹의 명명 규칙은 각각 CSM_INLINE 및 DM_INLINE입니다.



참고 **Tools(툴) > Preferences(기본 설정)**에서 개체 그룹화의 동작을 변경하려면 **Auto-expand network and service objects with specified prefix**(지정된 접두사로 네트워크 및 서비스 개체 자동 확장) 규칙 테이블 기본 설정을 선택합니다.

다음은 ASDM으로 관리되는 ASA에서 **show run** 명령을 사용하여 추출한 컨피그레이션 스니펫입니다.

```
object network host1
  host 10.1.1.100
object network fqdn_obj1
  fqdn abc.cisco.com
object-group network DM_INLINE_NETWORK_1
  network-object 10.21.44.189 255.255.255.255
  network-object 10.21.44.190 255.255.255.255
object-group network DM_INLINE_NETWORK_2
  network-object 10.21.44.191 255.255.255.255
  network-object object host1
  network-object object fqdn_obj1
```

```
access-list CSM_DM_ACL extended permit tcp object-group DM_INLINE_NETWORK_1 object-group
DM_INLINE_NETWORK_2
```

위의 예에서 ASDM UI의 access-list CSM_DM_ACL은 DM_INLINE 그룹을 규칙의 소스 및 대상 네트워크로 표시하지 않으며 대신 DM_INLINE 그룹의 내용을 표시합니다.

인라인 그룹화 - ASDM/CSM

Secure Firewall 마이그레이션 툴의 인라인 그룹화 기능을 사용하면 ASDM 또는 CSM으로 관리되는 ASA 디바이스의 **show running-configuration**을 구문 분석할 수 있습니다. 이 기능은 ASDM 또는 CSM과 동일하게 access-list 규칙의 UI 표현을 유지하는 옵션을 제공합니다. 이 옵션의 선택을 취소하면 마이그레이션된 규칙이 ASA **show running-configuration**에 기록된 대로 DM_INLINE 그룹을 참조합니다.



참고 Secure Firewall 마이그레이션 툴에 입력된 소스 ASA 구성 파일은 여전히 ASA에서 수집되거나 ASA 디바이스에 대한 라이브 연결(SSH)을 통해 수집된 **show run** 또는 **show tech**입니다. Secure Firewall 마이그레이션 툴은 다른 형식의 구성 파일 또는 메서드를 지원하지 않습니다.

다음 그림에서는 인라인 그룹화 옵션을 활성화하거나 비활성화할 때 ACE 또는 RULE의 Source(소스) 및 Destination(대상) Network(네트워크) 필드가 각각 어떻게 변경되는지 보여줍니다.

그림 2: 인라인 그룹화 - ASDM/CSM 활성화 시

		SOURCE				DESTINATION			State	Action
	#	Name	Zone	Network	Port	Zone	Network	Port		
☐	121	CSM_DM_ACL_#1	outside	10.21.44.185, 10.21.44.190	ANY	ANY	10.21.44.191, host1, fqdn_obj1	ANY	✓	Allow

그림 3: 인라인 그룹화 - ASDM/CSM 비활성화 시

		SOURCE				DESTINATION			State	Action
	#	Name	Zone	Network	Port	Zone	Network	Port		
☐	121	CSM_DM_ACL_#1	outside	DM_INLINE_NETWORK_1	ANY	ANY	DM_INLINE_NETWORK_2	ANY	✓	Allow

마이그레이션 전 보고서 검토

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

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



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

프로시저

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



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

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

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

- **Overall Summary**(전체 요약) - ASA 구성 정보를 추출하거나 라이브 ASA 구성에 연결하는 데 사용되는 방법입니다.

라이브 ASA에 연결한다면 ASA에서 감지된 방화벽 모드이며, 멀티 컨텍스트 모드의 경우 마이그레이션을 위해 선택한 컨텍스트입니다.

Firewall Threat Defense 또는 Multicloud Defense로 성공적으로 마이그레이션할 수 있는 지원되는 ASA 구성 요소 및 마이그레이션을 위해 선택한 특정 ASA 기능의 요약입니다.

라이브 ASA에 연결하는 동안에는 요약에 적중 횟수 정보(ASA 규칙이 적용된 횟수 및 타임스탬프 정보)가 포함됩니다.

- **Configuration Lines with Errors(오류가 있는 구성 라인)** - Secure Firewall 마이그레이션 툴이 구문 분석할 수 없으므로, 마이그레이션할 수 없는 ASA 구성 요소에 대한 세부 정보입니다. 계속 진행하기 전에 ASA 구성에서 이러한 오류를 해결하고 새 구성 파일을 내보낸 다음 Secure Firewall 마이그레이션 툴에 새 구성 파일을 업로드합니다.
- **Object and Object Groups Conflict Resolution(개체 및 개체 그룹 충돌 확인)** - 마이그레이션하려는 상황 전체에서 충돌이 발생한 ASA 네트워크 및 서비스 개체와 개체, 서비스, 프로토콜 개체 그룹에 대한 세부 정보입니다. 이러한 개체 충돌에 대한 세부 정보를 보려면 **Link for Conflict Count(충돌 수 링크)**를 클릭합니다. 충돌의 이유를 확인하고 마이그레이션 툴이 충돌을 처리하는 방법도 알 수 있습니다.
- **Ignored Configuration(무시된 구성)** - Firewall Management Center 또는 Secure Firewall 마이그레이션 툴에서 지원되지 않기 때문에 무시되는 ASA 구성 요소의 세부 정보입니다. Secure Firewall 마이그레이션 툴은 이러한 라인을 구문 분석하지 않습니다. 이러한 라인을 검토하고 Firewall Management Center에서 각 기능이 지원되는지 확인한 다음, 지원되지 않는 경우 해당 기능을 수동으로 구성하도록 계획합니다. 모든 무시된 라인을 보려면 무시된 구성 라인에 대한 링크를 클릭합니다.

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

- 단계 3 (선택 사항) **Pre-Migration Report(마이그레이션 전 보고서)**에서 시정 조치를 권장하는 경우, 계속하기 전에 ASA 인터페이스에서 해당 시정 조치를 완료하고 ASA 구성 파일을 다시 내보낸 후 업데이트된 구성 파일을 업로드하십시오.
- 단계 4 ASA 구성 파일이 성공적으로 업로드되고 구문 분석된 후 Secure Firewall 마이그레이션 툴로 돌아가 **Next(다음)**를 클릭하여 마이그레이션을 계속합니다.

다음에 수행할 작업

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

ASA 구성과 Firewall Threat Defense 인터페이스 매핑

Firewall Threat Defense 디바이스에는 ASA 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 ASA의 인터페이스와 Firewall Threat Defense 디바이스를 매핑합니다. 예를 들

어, ASA 인터페이스의 '관리 전용' 인터페이스는 Firewall Threat Defense 디바이스의 '관리 전용' 인터페이스에 자동으로 매핑되며 이를 변경할 수 없습니다.

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

- 대상 Firewall Threat Defense가 네이티브 유형인 경우:
 - Firewall Threat Defense에서 같거나 더 많은 수의 ASA 인터페이스 또는 PC(Port Channel) 데이터 인터페이스(ASA 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 ASA 인터페이스, 물리적 하위 인터페이스, 포트 채널 또는 포트 채널 하위 인터페이스(ASA 구성의 관리 전용 인터페이스 제외)를 사용해야 합니다. 이 수가 더 적은 경우 대상 Firewall Threat Defense에 필요한 인터페이스 유형을 추가합니다. 예를 들어, 대상 Firewall Threat Defense의 물리적 인터페이스 및 물리적 하위 인터페이스 수가 ASA 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 참고하십시오.



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

프로시저

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

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

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

다음에 수행할 작업

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

ASA 인터페이스를 보안 영역 및 VRF에 매핑



참고 ASA 구성에 액세스 목록 및 NAT 규칙이 포함되어 있지 않거나 이러한 정책을 마이그레이션하지 않도록 선택한 경우에는 이 단계를 건너뛰고 [최적화, 구성 검토 및 검증, 77 페이지](#)로 진행할 수 있습니다.

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

- 보안 영역 — 하나의 인터페이스가 하나의 보안 영역에만 속할 수 있습니다.
- 인터페이스 그룹 — 하나의 인터페이스가 여러 인터페이스 그룹에 속할 수 있습니다.
- VRF — 하나의 인터페이스는 하나의 VRF 구성에만 속할 수 있습니다.

Secure Firewall 마이그레이션 툴을 사용하면 보안 영역 인터페이스 그룹 및 VRF이 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, 인터페이스 그룹 및 VRF 구성을 검토합니다.

단계 2 Firewall Management Center에 존재하는, 즉 ASA 구성 파일에서 보안 영역 유형 개체로 사용 가능하고 드롭다운 목록에서 사용 가능한 보안 영역 및 인터페이스 그룹에 인터페이스를 매핑하려면 다음과 같이 합니다.

a) **Security Zones(보안 영역)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.

- b) **Interface Groups**(인터페이스 그룹) 열에서 해당 인터페이스의 인터페이스 그룹을 선택합니다.
- c) **VRF** 열에서 인터페이스의 VRF 구성을 선택합니다.



참고 마이그레이션의 일부로 위협 방어 HA 쌍을 설정하는 경우 기본 및 보조 피어 모두에 대해 보안 영역 및 인터페이스 그룹을 추가하거나 자동으로 생성할 수 있습니다. 보조 피어의 보안 영역 및 인터페이스 그룹은 기본 피어와 동일합니다.

단계 3 보안 영역, 인터페이스 그룹 및 VRF를 수동으로 매핑하거나 자동으로 생성할 수 있습니다.

단계 4 보안 영역, 인터페이스 그룹 및 VRF를 수동으로 매핑하려면 다음과 같이 합니다.

- a) **Add SZ, IG & VRF**(SZ, IG 및 VRF 추가)를 클릭합니다.
- b) **Add SZ, IG and VRF**(SZ, IG 및 VRF 추가) 대화 상자에서 편집 아이콘을 클릭하고 VRF에 지정할 이름을 입력한 다음 녹색 확인 표시를 클릭합니다. 편집 아이콘을 다시 클릭하여 VRF 이름을 수정할 수도 있습니다.



참고 병합 구성 마이그레이션을 수행 중이고 컨텍스트 중 하나에 VPN 구성이 있는 경우, 전역 라우터로 직접 마이그레이션되므로 여기에 인터페이스에 매핑할 수 있도록 표시되지 않습니다.

- c) **Security Zone**(보안 영역) 열에 보안 영역 이름을 입력합니다. 허용되는 최대 문자 수는 48자입니다. 마찬가지로 인터페이스 그룹을 추가할 수 있습니다.
- d) **Close**(닫기)를 클릭합니다.

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

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

Secure Firewall 마이그레이션 툴은 이러한 보안 영역에 ASA 인터페이스와 같은 이름(예: **outside**(외부) 또는 **inside**(내부))를 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 그룹은 ASA 인터페이스와 동일한 모드를 사용합니다. 예를 들어 ASA 논리적 인터페이스가 L3 모드인 경우 인터페이스에 대해 생성된 보안 영역 및 인터페이스 그룹도 L3 모드입니다.

단계 5 모든 인터페이스를 적절한 보안 영역, 인터페이스 그룹 및 VRF에 매핑했으면 **Next**(다음)를 클릭합니다.

최적화, 구성 검토 및 검증

마이그레이션된 ASA 구성을 Firewall Management Center로 푸시하기 전에 구성을 최적화하고 신중하게 검토하여 해당 구성이 올바르게 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.

소스 ASA 디바이스는 CSM 또는 ASDM에서 관리할 수 있습니다. 소스/수신 주소 또는 소스/대상 서비스에 둘 이상의 항목(개체 또는 인라인 값)을 입력할 경우, CSM 또는 ASDM에서는 개체 그룹을 자동으로 생성합니다. CSM 및 ASDM에서 사용되는 이러한 개체 그룹의 명명 규칙은 각각 CSM_INLINE 및 DM_INLINE입니다.

인라인 그룹화 CSM 또는 ASDM 관리 컨피그레이션을 지우도록 선택하는 경우 미리 정의된 개체가 실제 개체 또는 멤버 이름으로 대체됩니다. CSM 또는 ASDM 관리 컨피그레이션을 지우지 않으면 마이그레이션 시 미리 정의된 개체 이름이 유지됩니다.

예를 들어 10.21.44.189 및 10.21.44.190은 개체 그룹의 멤버이며 미리 정의된 이름(예: object-group DM_INLINE_NETWORK_1 및 object-group DM_INLINE_NETWORK_2)으로 변경됩니다.



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 ASA에 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.

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) **Proceed**(진행)를 클릭하여 ACL 최적화를 진행합니다. 마이그레이션을 위해 식별된 중복 ACL, 새도우 ACL 및 비활성 ACL 규칙이 표시됩니다.

ACL 최적화를 분석하는 데 걸리는 시간은 소스 구성 파일 크기에 따라 달라집니다. 예상 시간이 표시됩니다.

최적화를 위해 고려된 총 ACL 규칙의 요약이 포함된 보고서가 표시됩니다. 최적화 보고서 및 해당 구성 요소에 대한 자세한 내용은 [ACL 최적화 보고, 93 페이지](#)를 참고하십시오.

Redundant ACL(중복 ACL), **Shadow ACLs**(새도우 ACL) 및 **Disable ACLs**(비활성 ACL) 탭은 ACL 최적화 보고서에 데이터가 있는 경우에만 나타납니다.

ACL은 서로 다른 기본 규칙의 중복, 새도우 및 비활성 ACL에 모두 표시됩니다.



참고 중복, 새도우 또는 비활성 ACL 아래에 표시되는 ACL 항목은 기본 ACL로 간주되지 않습니다.

- b) 식별된 ACL 최적화 규칙을 다운로드하려면 **Download Report**(보고서 다운로드)를 클릭합니다.
 c) 규칙을 선택하고 **Actions**(작업) > **Migrate as disabled**(비활성화된 항목으로 마이그레이션) 또는 **Do not migration**(마이그레이션하지 않음)을 선택하고 작업 중 하나를 적용합니다.
 d) **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 ASA 구성 파일에 다시 쉽게 매핑할 수 있습니다. 예를 들어 ASA 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.

Actions(작업) 드롭다운의 **Rule Action(규칙 작업)** 대화 상자에서 **ACP** 또는 **Prefilter(사전 필터)** 탭을 선택할 수 있습니다.

- **ACP** - 모든 액세스 제어 규칙에는 시스템이 일치하는 트래픽을 처리하고 기록하는 방법을 결정하는 작업이 있습니다. 액세스 제어 규칙에 대해 허용, 신뢰, 모니터링, 차단 또는 차단 후 재설정 작업을 수행할 수 있습니다.
- **Prefilter(사전 필터)** - 규칙의 작업은 시스템이 일치하는 트래픽을 처리하고 기록하는 방법을 결정합니다. 단축경로(Fastpath) 지정 및 차단을 수행할 수 있습니다.



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

ACL 규칙 범주 - Secure Firewall 마이그레이션 툴은 CSM 관리 ASA 구성의 Rule(규칙) 섹션을 유지하고 Firewall Management Center에서 ACL 범주로 마이그레이션합니다.

정책 용량 및 제한 경고 - Secure Firewall 마이그레이션 툴은 마이그레이션된 규칙의 총 ACE 수를 대상 플랫폼에서 지원되는 ACE 제한과 비교합니다.

비교 결과를 기반으로 Secure Firewall 마이그레이션 툴은 마이그레이션된 ACE의 총 수가 임계값을 초과하거나 대상 디바이스의 지원되는 제한 임계값에 근접한 경우 가시적인 지표 및 경고 메시지를 표시합니다.

규칙이 ACE Count(ACE 수) 열을 초과할 경우 마이그레이션을 최적화하거나 마이그레이션하지 않도록 결정할 수 있습니다. 구축 전에 Firewall Management Center에서 푸시한 후 마이그레이션을 완료하고 이 정보를 사용하여 규칙을 최적화할 수도 있습니다.



- 참고 Secure Firewall 마이그레이션 툴은 경고에도 불구하고 마이그레이션을 차단하지 않습니다.

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 NAT 규칙의 소스 및 대상 영역을 편집하려면 **NAT**을 클릭한 후 다음 단계를 수행하십시오.

- a) 편집할 NAT 규칙 유형을 선택합니다.
- b) **Actions**(작업) 드롭다운 목록에서 **Edit**(수정)을 선택합니다.
- c) **Security Zone Update**(보안 영역 업데이트) 대화 상자에서 드롭다운 목록에서 **Source Zone**(소스 영역) 및 **Destination Zone**(대상 영역)을 선택하고 **Update**(업데이트)를 클릭합니다.

여러 NAT 규칙을 선택하여 일괄 업데이트를 수행할 수도 있습니다.

단계 4 다음 탭을 클릭하고 컨피그레이션 항목을 검토합니다.

- 액세스 제어
- 개체(액세스 목록 개체, 네트워크 개체, 포트 개체, **VPN** 개체, 보안 그룹 태그 개체 및 동적 경로 개체)
- **NAT**
- 인터페이스
- 경로
- **DHCP**
- **SNMP**
- 사이트 간 **VPN** 터널
- 원격 액세스 **VPN**
- **WebVPN**



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

액세스 목록 개체는 BGP, EIGRP, RA VPN에서 사용되는 표준 및 확장 ACL을 표시합니다.

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

마이그레이션하지 않도록 선택하는 모든 규칙은 테이블에서 회색으로 표시됩니다.

단계 5 (선택 사항) **Network Objects**(네트워크 개체) 및 **Port Objects**(포트 개체) 탭에서 모든 네트워크 개체, 네트워크 그룹, 포트 개체, 포트 그룹 및 그 값을 검토합니다. 개체 또는 개체 그룹의 이름을 변경하려면 개체를 선택하고 **Actions**(작업) > **Rename**(이름 변경)를 선택합니다.

- **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.

-  를 클릭하여 개체를 **Conflict Detected(충돌 탐지됨)** 열에서 **Objects/Groups Retained(개체/그룹이 유지됨)** 열로 이동하고  를 클릭하여 다시 뒤로 이동합니다. 대부분의 구성에서 참조되는 구성은 굵은 텍스트로 표시됩니다.
- 가장 많은 참조 수를 가진 모든 개체 및 그룹을 자동으로 선택하려면 **Auto Select(자동 선택)**를 클릭합니다. 그러나 수동 선택의 우선 순위가 더 높으므로 자동 선택을 수동으로 재정의하고 열 간에 개체를 이동할 수 있습니다.
- **Optimize(최적화)**를 클릭합니다. 마이그레이션 툴은 최적화를 수행하고 보존된 개체 및 중복 개체를 포함한 최적화 데이터가 포함된 최적화 요약을 표시합니다. 최적화 보고서의 자세한 버전은 마이그레이션 후 보고서를 참조하십시오.
- **Proceed(진행)** 및 **Validate(검증)**를 클릭합니다.



참고 보존하도록 선택되지 않은 개체 및 그룹은 마이그레이션되지 않으며, ACL 및 NAT 구성 등 사용된 구성의 보존된 개체로 교체됩니다. 이렇게 하면 마이그레이션되는 개체 목록이 완전히 최적화되고 마이그레이션되는 중복 개체가 없습니다.

단계 6 (선택 사항) 구성을 검토하는 동안 **Network Objects(네트워크 개체)** 탭 또는 **Port Objects(포트 개체)** 탭 또는 **VPN Objects(VPN 개체)**에서 **Actions(작업) > Rename(이름 바꾸기)**을 선택하여 하나 이상의 네트워크, 포트 또는 VPN 개체의 이름을 변경할 수 있습니다.

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

단계 7 **Security Group Tag Objects(보안 그룹 태그 개체)** 탭에서 모든 값을 검토합니다. 개체 또는 개체 그룹의 이름을 변경하려면 개체를 선택하고 **Actions(작업) > Rename(이름 변경)**를 선택합니다.

SGT 개체는 다중 컨텍스트 구성을 지원합니다. 태그 값은 0에서 65535 사이여야 합니다.



참고 SGT 개체 구성을 마이그레이션하려면 관리 센터 및 위협 방어 버전이 7.0 이상인지 확인하십시오.

단계 8 **Dynamic-Route Objects(유동 경로 개체)** 섹션에 마이그레이션되는 모든 지원 개체가 표시됩니다.

- Policy-List
- Prefix-List
- Route-Map
- 커뮤니티 목록
- AS-Path
- Access-List

단계 9 **Routes(경로)** 섹션에 다음 경로가 표시됩니다.

- **Static(정적)** - 모든 IPv4 및 IPv6 정적 경로를 표시합니다.
- **BGP** — 모든 BGP 경로를 표시합니다.
- **EIGRP** - 모든 EIGRP 경로를 표시합니다.

EIGRP의 경우 `more system:running` 구성이 업로드되고 키가 암호화되지 않은 경우 인증 키를 가져옵니다. 키가 소스 구성에서 암호화된 경우 EIGRP의 **Interface(인터페이스)** 섹션에서 키를 수동으로 제공할 수 있습니다. 인증 유형(`encrypted(암호화됨)`, `unencrypted(암호화되지 않음)`, `auth(인증됨)` 또는 `none(없음)`)을 선택하고 그에 따라 키를 제공합니다.

- **ECMP** - 모든 ECMP 영역 및 관련 VRF를 표시합니다.



참고 이 섹션에서는 ECMP 영역의 이름을 변경하는 작업만 수행할 수 있습니다.

- **PBR** - 모든 PBR 경로를 표시합니다.

단계 10 **DHCP** 탭에서 다음 탭을 검토하고 검증할 수 있습니다.

- **DHCP Server(DHCP 서버)**: 모든 IP 주소 풀과 해당 인터페이스를 검토합니다.
- **DHCP Relay(DHCP 릴레이)**: DHCP 릴레이 서버 IP 주소, DHCP 서버가 연결된 인터페이스 및 릴레이가 활성화된 인터페이스를 검토합니다.
- **DDNS: DDNS Update Methods(DDNS 업데이트 방법)** 탭에서 DDNS 방법 이름, 유형, DDNS 업데이트 간격 및 DHCP 서버에 의해 업데이트되도록 설정된 레코드(A 또는 PTR 레코드)를 검토합니다.



참고 **Select Features(기능 선택)** 페이지에서 DHCP 서버만 또는 릴레이와 DDNS를 함께 선택할 수 있습니다. 따라서 **Optimize, Review and Validate Configuration(구성 최적화, 검토 및 검증)** 페이지의 **DHCP Server(DHCP 서버)** 탭에 구성이 표시되는 경우 **DHCP Relay(DHCP 릴레이)** 및 **DDNS** 탭이 비어 있습니다.

단계 11 **SNMP** 탭에서 다음 탭을 검토, 검증 및 작업할 수 있습니다.

ASA 디바이스에 SNMPV1/V2 또는 SNMPV3 구성이 있는지에 따라 구성이 **SNMPV1/V2** 탭 또는 **SNMPV3** 탭에 표시됩니다.

SNMPV1/V2:

- **Host Server Name(호스트 서버 이름)**: SNMP 호스트의 호스트이름
- **IP Address(IP 주소)**: SNMP 호스트의 IP 주소
- **Community String(커뮤니티 문자열)**: 수동으로 제공해야 하는 SNMP 커뮤니티 문자열입니다. 호스트를 선택하고 **Actions (작업) (작업) > Update Community String(커뮤니티 문자열 업데이트)**

트)로 이동하여 커뮤니티 문자열을 제공합니다. 이것은 SNMP 서비스를 위해 구성된 커뮤니티 또는 사용자 이름과 동일해야 합니다.

- **Validation State**(검증 상태) : 대상 Management Center에서 생성될 호스트 서버의 검증 상태

SNMPV3:

- **User Name**(사용자 이름): SNMP 호스트의 사용자 이름
- **Authentication Password**(인증 비밀번호): 사용자의 인증 비밀번호를 제공하려면 **Actions**(작업)를 클릭합니다.
- **Encryption Password**(암호화 비밀번호): 사용자의 비공개 비밀번호를 제공하려면 **Actions**(작업)를 클릭합니다.
- **Validation State**(검증 상태) : 대상 Management Center에서 생성될 사용자의 검증 상태

단계 12 Site-to-Site VPN Tunnels(사이트 간 VPN 터널) 섹션에는 다음 목록을 포함하여 ASA에서 Firewall Management Center로 마이그레이션된 모든 지원되는 VPN 터널이 표시됩니다.

- 암호화 맵 및 경로 기반(VTI) 기반 VPN 터널.
- 인증 유형 사전 공유 키 및 인증서 기반 인증의 VPN 터널.

모든 행에 대한 검증을 위해 각 VPN 토폴로지에 대한 사전 공유 키 및 PKI 개체의 값을 입력해야 합니다. 업데이트에 실패하면 완료되지 않은 것으로 표시되고 Secure Firewall 마이그레이션 툴이 검증을 진행할 수 없습니다.



참고 라이브 연결 ASA의 경우 마이그레이션 툴이 사전 공유 키를 자동으로 검색합니다. 수동으로 업로드된 구성의 경우, **more system: running-config**를 사용하여 숨겨진 키를 검색하고 **Pre-shared Key**(사전 공유 키) 열에 수동으로 제공합니다.



참고 ASA에서 Firewall Management Center로의 트러스트 포인트 또는 PKI 개체 마이그레이션은 사전 마이그레이션 활동의 일부이며 인증서 기반 VPN 마이그레이션을 성공적으로 수행하는 데 필요합니다.

단계 13 (선택 사항) 대상 위협 방어를 허브 노드로 사용하고 하나 이상의 ASA 피어 인터페이스를 스포크 노드로 선택하여 허브 앤 스포크 VPN 토폴로지를 구성하려면 **Add Hub and Spoke Topology**(허브 및 스포크 토폴로지 추가)를 클릭합니다.



참고 IKE 버전이 동일한 스포크 노드만 선택할 수 있습니다. 예를 들어 IKEv1의 스포크 노드 하나를 선택하고 IKEv2 IKE 버전의 다른 스포크 노드를 선택할 수는 없습니다.

선택한 스포크 노드의 IKE 버전에 따라 다음을 구성하거나 확인합니다.

- **IKE Version(IKE 버전)** - 선택한 노드의 IKE 버전이 선택되었는지 확인합니다.
- **Endpoints(엔드포인트)**- 대상 위협 방어 디바이스가 허브 노드, 목록에서 선택한 스포크 노드, VPN 인터페이스 및 보호되는 소스 및 원격 네트워크로 기본적으로 선택되어 있는지 확인합니다.

• **IKE**

• **IKEv1 Settings(IKEv1 설정) 또는 IKEv2 Settings(IKEv2 설정)**

- **Authentication Type(인증 유형)**- 지원되는 두 가지 인증 방법은 사전 공유 키 및 인증서입니다. *Cisco Secure Firewall Management Center* 디바이스 설정 가이드의 [Decisioning which Authentication Method to Use\(사용할 인증 방법 결정\)](#)를 참조하십시오.

• **Advanced(고급)**

- **Enable Aggressive Mode(적극적인 모드 활성화)**—IP 주소를 알 수 없고 DNS 확인을 디바이스에서 사용할 수 없는 경우, 키 정보 교환을 위해 이 협상 방법을 선택합니다.
- **IKE Keepalive(IKE 킵얼라이브)**- keepalive 모니터링을 위해 활성화 또는 비활성화합니다.
- **Threshold(임계값)**—IKE keep alive 신뢰 구간을 지정합니다. 이 간격은 keepalive 모니터링을 시작하기 전에 피어가 유효 상태에 있도록 허용하는 시간(초)입니다. 기본값 및 최소 간격은 10초이고, 최대 간격은 3600초입니다.
- **Retry Interval(재시도 간격)**- IKE 킵얼라이브 재시도 간에 대기할 시간(초)을 지정합니다. 기본값은 2초, 최대값은 10초입니다.

Create Hub & Spoke Topology

IKE Version : ☒ IKEv1 ☐ IKEv2

Endpoints IKE **IPsec**

Crypto Map Type: ☒ Static

Transform Sets: IKEv1 IPsec Proposals *

Select...

☐ Enable Security Association (SA) Strength Enforcement

☒ Enable Reverse Route Injection

☐ Enable Perfect Forward Secrecy

Modulus Group: Select...

Lifetime Duration: 28800 Seconds (Range 120 - 2147483674)

Lifetime size: 4608000 Kbytes (Range 10 - 2147483674)

Confirm

• IPsec

- **Crypto Map Type(암호화 맵 유형)**—암호화 맵은 IPsec 보안 연결(SA)을 설정하는 데 필요한 모든 구성 요소를 결합합니다. 두 피어에서 SA를 설정하려고 시도할 때 최소 1개 이상의 호환 가능한 암호화 맵이 있어야 합니다. IPsec 보안 협상은 암호화 맵 항목에 정의된 제안을 사용하여 해당 암호화 맵의 IPsec 규칙에 지정된 데이터 흐름을 보호합니다. 이 구축의 암호화 맵에 대해 정적 또는 동적 여부를 선택합니다.
- **Transform Sets(변환 집합)** - 선택한 IKE 버전 노드에 사용할 IPsec 제안을 선택합니다.
 - **Enable Security Association (SA) Strength Enforcement(SA(Security Association) 강점 시행 활성화)**—이 체크 박스를 선택하면 하위 IPsec SA에서 사용하는 암호화 알고리즘이 상위 IKE SA에 비해 키의 비트 수와 관련하여 더 강점을 보이지 않습니다.
 - **Enable Reverse Route Injection(역방향 경로 삽입 활성화)**—이 체크 박스를 선택하면 원격 터널 그룹 목록으로 보호되는 네트워크 및 호스트의 라우팅에 정적 경로를 자동으로 삽입하는 역방향 경로 삽입을 활성화합니다.
 - **Enable Perfect Forward Secrecy(완전 순방향 비밀성 활성화)**—이 체크 박스를 선택하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했다 하더라도 후속 암호 해독에서 교환을 보호합니다.
- **Modulus Group(모듈러스 그룹)**—공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹을 선택합니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 자세한 내용은 *Cisco Secure Firewall Management Center* 디바이스 구성 가이드의 [사용할 Diffie-Hellman 모듈러스 그룹 결정](#)을 참조하십시오.

- **Lifetime Duration(수명 기간)** - 보안 연결이 만료되기 전에 보안 연결을 유지할 시간(초)입니다. 기본값은 28,800초입니다.
- **Lifetime Size(수명 크기)**—만료되기 전에 지정된 보안 연결을 사용하여 IPsec 피어 간에 전달할 수 있는 트래픽 볼륨(KB)입니다. 기본값은 4,608,000킬로바이트입니다. 무한 데이터는 허용되지 않습니다.

관리 센터의 디바이스 중 하나에 기존 사이트 간 허브 앤 스포크 VPN 구성이 있는 경우, 대상 위협 방어 디바이스를 스포크 중 하나로 추가하도록 선택할 수 있습니다. **Add to the existing Hub and Spoke Topology(기존 허브 및 스포크 토폴로지에 추가)**를 선택하고 디바이스를 추가할 토폴로지를 선택한 후 **Interface(인터페이스)** 및 **Protected Networks(보호된 네트워크)**를 선택합니다.

단계 14 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 15 Remote Access VPN(원격 액세스 VPN) 섹션에서는 원격 액세스 VPN에 해당하는 모든 개체가 ASA에서 Management Center로 마이그레이션되며 다음과 같이 표시됩니다.

- **Anyconnect Packages(AnyConnect 패키지)**- AnyConnect 패키지, Hostscan 파일(Dap.xml, Data.xml, Hostscan 패키지), 외부 브라우저 패키지를 검색하고 AnyConnect 프로파일은 마이그레이션을 위해 소스 ASA 디바이스에서 검색되어야 합니다.

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

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

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

- **AAA - Radius, LDAP, AD, LDAP, SAML 및 Local Realm**(로컬 영역) 유형의 인증 서버가 표시됩니다. 모든 AAA 서버의 키를 업데이트합니다. Secure Firewall 마이그레이션 툴 3.0부터는 Live Connect ASA에 대해 사전 공유 키가 자동으로 검색됩니다. **more system: running-config** 파일을 사용하여 숨겨진 키와 함께 소스 구성을 업로드할 수도 있습니다. 일반 텍스트 형식의 AAA 인증 키를 검색하려면 다음 단계를 수행합니다.



참고 이러한 단계는 Secure Firewall 마이그레이션 툴 외부에서 수행해야 합니다.

1. SSH 콘솔을 통해 ASA에 연결합니다.
2. `more system:running-config` 명령을 입력합니다.
3. **aaa-server and local user(aaa-server 및 로컬 사용자)** 섹션으로 이동하여 일반 텍스트 형식의 모든 AAA 구성 및 각 키 값을 찾습니다.

```
ciscoASA#more system:running-config

!

aaa-server Test-RADIUS (inside) host 2.2.2.2

    key <key in clear text> <-----The radius key is now displayed in clear text
format.

aaa-server Test-LDAP (inside) host 3.3.3.3

ldap-login-password <Password in clear text> <-----TheLDAP/AD/LDAPS 비밀번호가 이제 일
반 텍스트 형식으로 표시됩니다.

username Test_User password <Password in clear text> <-----The Local user
password is shown in clear text.
```



참고 로컬 사용자의 비밀번호가 암호화된 경우 내부에서 비밀번호를 확인하거나 Secure Firewall 마이그레이션 툴에서 새 비밀번호를 구성할 수 있습니다.

- LDAPS에는 Management Center의 도메인이 필요합니다. 암호화 유형 LDAPS에 대한 도메인을 업데이트해야 합니다.
- AD 서버에는 Firewall Management Center에 고유한 AD 기본 도메인이 필요합니다. 고유한 도메인이 식별되면 Secure Firewall 마이그레이션 툴에 표시됩니다. 충돌이 발견되면 사용자는 고유한 AD 기본 도메인을 입력해야 개체를 푸시할 수 있습니다.

암호화가 LDAPS로 설정된 AAA 서버의 경우 ASA는 IP 및 호스트 이름 또는 도메인을 지원하지만, Management Center는 호스트 이름 또는 도메인만 지원합니다. ASA 구성에 호스트 이름 또는 도메인이 포함된 경우 검색되어 표시됩니다. ASA 구성에 LDAPS용 IP 주소가 포함된 경우 **Remote Access VPN(원격 액세스 VPN)** 아래의 **AAA** 섹션에 도메인을 입력합니다. AAA 서버의 IP 주소로 확인할 수 있는 도메인을 입력해야 합니다.

유형이 AD인 AAA 서버의 경우(서버 유형은 ASA 구성에서 Microsoft임) **AD Primary Domain(AD 기본 도메인)**은 Management Center에서 구성해야 하는 필수 필드입니다. 이 필드는 ASA에서 별도로 구성되지 않으며 ASA의 LDAP-base-dn 구성에서 추출됩니다.

ldap-base-dn이 ou=Test-Ou,dc=gcevpn,dc=com인 경우

AD Primary Domain(AD 기본 도메인)은 기본 도메인을 구성하는 dc, dc=gcevpn 및 dc=com으로 시작하는 필드입니다. AD 기본 도메인은 gcevpn.com입니다.

LDAP-base-dn 예시 파일:

cn=asa,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:

여기서 dc=abc 및 dc=com은 abc.com으로 결합되어 AD 기본 도메인을 형성합니다.

cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:

AD 기본 도메인은 fwsecurity.cisco.com입니다.

AD 기본 도메인이 자동으로 검색되어 Secure Firewall 마이그레이션 툴에 표시됩니다.



참고 AD 기본 도메인 값은 각 영역 개체에 대해 고유해야 합니다. 충돌이 탐지되거나 Firewall 마이그레이션 툴이 ASA 구성에서 값을 찾을 수 없는 경우, 특정 서버에 대한 AD 기본 도메인을 입력하라는 메시지가 표시됩니다. 구성을 검증할 AD 기본 도메인을 입력합니다.

- **Address Pool(주소 풀)** - 여기에 표시된 모든 Ipv4 및 Ipv6 풀을 검토합니다.
- **Group-Policy(그룹 정책)** - 이 영역에서 사용자 프로파일, 관리 프로파일, 클라이언트 모듈 프로파일을 선택하거나 제거합니다. 이 영역에는 클라이언트 프로파일이 있는 그룹 정책, 관리 프로파일, 관리 모듈이 표시되며, 프로파일이 없는 그룹 정책이 표시됩니다. 프로파일이 AnyConnect file(AnyConnect 파일) 섹션에 추가된 경우 사전 선택된 것으로 표시됩니다. 사용자 프로파일, 관리 프로파일 및 클라이언트 모듈 프로파일을 선택하거나 제거할 수 있습니다.
특정 그룹 정책과 관련된 사용자 지정 속성이 **AnyConnect Custom Attribute(AnyConnect 사용자 지정 속성)** 탭에 표시됩니다. 사용자 지정 속성을 선택하고 검증할 수 있습니다.
- **Connection Profile(연결 프로파일)** - 여기에 표시된 모든 연결 프로파일/터널 그룹을 검토합니다.

- **Trustpoints(트러스트 포인트)** - ASA 에서 Management Center로의 트러스트 포인트 또는 PKI 개체 마이그레이션은 사전 마이그레이션 활동의 일부이며 원격 액세스 VPN을 성공적으로 마이그레이션하는 데 필요합니다. **Remote Access Interface(원격 액세스 인터페이스)** 섹션에서 전역 SSL, IKEv2 및 인터페이스에 대한 트러스트 포인트를 매핑하여 다음 마이그레이션 단계를 진행합니다. LDAPS 프로토콜이 활성화된 경우 전역 SSL 및 IKEv2 트러스트 포인트는 필수입니다.

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

ASA에서 PKI 인증서를 내보내는 방법에 대한 자세한 내용은 [ASA 에서 PKI 인증서 내보내기 및 Management Center로 가져오기](#)를 참고하십시오.

- **Certificate Maps(인증서 맵)**- 여기에는 인증서 맵이 표시됩니다.
- **VPN Load Balancing(VPN 로드 밸런싱)** - 여기에는 VPN 로드 밸런싱 구성이 표시됩니다.
VPN 로드 밸런싱의 경우, **more system: running-config** 구성이 업로드되면 Secure Firewall 마이그레이션 툴이 암호화 키를 가져옵니다. **Actions(작업) > Update Keys(키 업데이트)**를 사용하여 암호화 키를 수동으로 업데이트할 수 있습니다.
- **WebVPN** 탭에서 마이그레이션 툴은 소스 ASA 디바이스에서 탐지한 모든 WebVPN 정책을 나열합니다. WebVPN 정책에는 SSL 클라이언트리스 VPN 터널 프로토콜 구성이 포함된 모든 ASA 그룹 정책 및 SAML 인증을 사용하는 정책에서 참조되는 터널 그룹이 포함됩니다. 계속 진행하기 전에 WebVPN 설정과 관련된 탭을 검토합니다.
- **Zero Trust Application Policy(제로 트러스트 애플리케이션 정책)**: 정책을 선택하고 **Actions(작업) > Update Zero Trust Policy(제로 트러스트 정책 업데이트)** 필드로 이동하여 다른 값을 제공합니다.

- **Policy Name(정책 이름)**: 마이그레이션될 정책의 이름입니다.

- **Domain Name(도메인 이름)**: 수동으로 제공해야 하는 사용자 정의 도메인 이름입니다. 도메인 이름은 프라이빗 애플리케이션에 액세스하는 Threat Defense 인터페이스를 확인합니다. 도메인 이름은 애플리케이션 그룹의 모든 프라이빗 애플리케이션에 대한 ACS URL을 생성하는 데 사용됩니다.

- **Identity Certificate(ID 인증서)**: 마이그레이션하기 전에 대상 Management Center로 가져온 ID 인증서입니다. 이 작업은 마이그레이션 전 작업의 일부로 수행해야 합니다.

- **Security Zones(보안 영역)**: 정책과 연결된 해당 보안 영역입니다.

- **Global Port Pool(전역 포트 풀)**: 정책의 포트 범위입니다. 이 풀의 고유한 포트가 각 애플리케이션에 할당됩니다.

- 애플리케이션 그룹

- **Application Group(애플리케이션 그룹)**: 애플리케이션 그룹 이름, 재인증 간격, 보안 영역을 포함한 **Application Group Settings(애플리케이션 그룹 설정)** 을 검토합니다.

SAML IdP Metadata(SAML IdP 메타데이터) 탭에서 애플리케이션 그룹 이름, 서비스 제공자의 엔터티 ID, SAML IdP(Identity Provider)의 SSO(Single Sign-On) URL 및 IdP 인증서를 수동으로 구성하거나 **Configure Later(나중에 구성)**를 선택할 수 있습니다.

Applications(애플리케이션) 탭에서는 애플리케이션 이름, 외부 URL, 애플리케이션 URL, 애플리케이션 인증서, 애플리케이션 그룹 등의 애플리케이션 관련 설정을 검토하거나 구성할 수 있습니다.

- **Standalone Applications(독립형 애플리케이션)**: 애플리케이션 이름, 외부 URL, 애플리케이션 URL, 애플리케이션 인증서, 재인증 간격, 보안 영역 등 독립형 애플리케이션의 **Application Settings(애플리케이션 설정)**를 검토하거나 구성합니다. **SAML IdP Metadata(SAML IdP 메타데이터)** 탭에서는 독립형 애플리케이션의 IdP 메타데이터 설정을 수동으로 구성하거나 나중에 구성할 수 있습니다. 탭에는 애플리케이션 그룹 이름, 엔터티 ID, SSO(Single Sign-On) URL 및 IdP 인증서가 포함됩니다.

필드를 업데이트하려면 **Actions(작업)**를 클릭하고 다양한 필드를 업데이트하도록 선택합니다.

마이그레이션을 성공적으로 수행한 후에는 **Management Center**로 마이그레이션한 구성을 철저히 검토하고 준비가 되면 **Threat Defense** 디바이스에 구축해야 합니다.

단계 16 (선택 사항) 그리드의 각 구성 항목에 대한 세부 정보를 다운로드하려면 **Download(다운로드)**를 클릭합니다.

단계 17 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 Center**에 연결하여 기존 개체를 검토하고 마이그레이션할 개체 목록과 비교합니다. 개체가 이미 **Firewall Management Center**에 있는 경우 **Secure Firewall** 마이그레이션 툴은 다음과 같이 합니다.

- 개체의 이름과 구성이 동일한 경우 **Secure Firewall** 마이그레이션 툴은 기존 개체를 재사용하고 **Firewall Management Center**에 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 18 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 19 **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 20 검증이 완료되고 **Validation Status(검증 상태)** 대화 상자에 **Successfully Validated(검증 성공)** 메시지가 표시되면 **마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시, 94 페이지**로 진행합니다.

ACL 최적화 보고

ACL 최적화 보고서에는 다음 정보가 표시됩니다.

- 요약 시트 - ACL 최적화의 요약을 표시합니다.

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

마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시

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

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

마이그레이션된 컨피그레이션을 Firewall Management Center에 푸시

구성을 성공적으로 검증하고 모든 개체 충돌을 해결하지 않은 경우 마이그레이션된 ASA 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 요약을 검토합니다.

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

Secure Firewall 마이그레이션 툴의 새로운 최적화 기능을 통해 검색 필터를 사용하여 마이그레이션 결과를 빠르게 가져올 수 있습니다.

또한 Secure Firewall 마이그레이션 툴은 CSV 다운로드를 최적화하고 페이지 보기별로 또는 모든 규칙에 작업을 적용할 수 있도록 지원합니다.



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

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



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

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

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

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

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

문제 해결을 위해 지원 팀에 문의할 수도 있습니다.

마이그레이션 실패 지원

마이그레이션이 실패할 경우 지원 팀에 문의합니다.

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

도움말 지원 페이지가 나타납니다.

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



참고 로그 및 dB 파일은 기본적으로 다운로드하도록 선택됩니다.

3. **Download**(다운로드)를 클릭합니다.

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

4. **Email us**(이메일 문의)를 클릭하여 기술 팀에 실패 세부 정보를 이메일로 보냅니다.
다운로드한 지원 파일을 이메일에 첨부할 수도 있습니다.
5. **Visit TAC page**(TAC 페이지 방문)를 클릭하여 Cisco 지원 페이지에서 TAC 케이스를 생성합니다.



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

마이그레이션 후 보고서 검토 및 마이그레이션 완료

마이그레이션 후 보고서는 다양한 범주의 ACL 수, ACL 최적화 및 컨피그레이션 파일에서 수행된 최적화의 전체 보기에 대한 세부 정보를 제공합니다. 자세한 내용은 [최적화, 구성 검토 및 검증, 77 페이지](#)를 참조해 주십시오.

개체를 검토하고 확인합니다.

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

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

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



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

프로시저

- 단계 1 **Post-Migration Report**(마이그레이션 후 보고서)를 다운로드한 위치로 이동합니다.
- 단계 2 마이그레이션 후 보고서를 열고 내용을 신중하게 검토하여 ASA 구성이 어떻게 마이그레이션되었는지 파악합니다.
 - **Migration Summary**(마이그레이션 요약) - ASA 에서 Firewall Threat Defense로 성공적으로 마이그레이션된 구성의 요약으로, ASA 인터페이스, Firewall Management Center 호스트 이름 및 도메

인, 대상 Firewall Threat Defense 디바이스 (적용 가능한 경우) 및 성공적으로 마이그레이션된 구성 요소에 대한 정보가 포함됩니다.

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

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



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

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



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

- **Object Conflict Handling**(개체 충돌 처리) - Firewall Management Center의 기존 개체와 충돌하는 것으로 확인된 ASA 개체에 대한 세부 정보입니다. 개체의 이름과 구성이 동일한 경우 Secure Firewall 마이그레이션 툴에서 Firewall Management Center 개체를 재사용했습니다. 개체의 이름은 같지만 컨피그레이션이 다른 경우 해당 개체의 이름을 변경했습니다. 이러한 개체를 신중하게 검토하고 충돌이 적절하게 해결되었는지 확인합니다.
- **Access Control Rules, NAT, and Routes You Chose Not to Migrate**(마이그레이션하지 않도록 선택한 액세스 제어 규칙, NAT 및 경로) - Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션하지 않도록 선택한 규칙에 대한 세부 정보입니다. Secure Firewall 마이그레이션 툴에서 비활성화되고 마이그레이션되지 않은 이러한 규칙을 검토합니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
- **Partially Migrated Configuration**(부분적으로 마이그레이션된 구성) - 고급 옵션이 포함되어 있지만 고급 옵션 없이 마이그레이션될 수 있는 규칙을 비롯하여 부분적으로만 마이그레이션된 ASA 규칙에 대한 세부 정보입니다. 이러한 라인을 검토하고 Firewall Management Center에서 고급 옵션이 지원되는지 확인한 다음 지원되는 경우 해당 옵션을 수동으로 구성합니다.

- **Unsupported Configuration**(지원되지 않는 구성) - Secure Firewall 마이그레이션 툴이 해당 기능의 마이그레이션을 지원하지 않으므로 마이그레이션할 수 없는 ASA 구성 요소에 대한 세부 정보입니다. 이러한 라인을 검토하여 각 기능이 Firewall Threat Defense에서 지원되는지 확인합니다. 지원되는 경우 Firewall Management Center에서 해당 기능을 수동으로 구성합니다.
- **Expanded Access Control Policy Rules**(확장 액세스 제어 정책 규칙)- 마이그레이션 중에 단일 ASA 포인트 규칙에서 여러 Firewall Threat Defense 규칙으로 확장된 ASA 액세스 제어 정책 규칙에 대한 세부 정보입니다.
- **Actions Taken on Access Control Rules**(액세스 제어 규칙에 대해 수행된 작업)
 - **Access Rules You Chose Not to Migrate**(마이그레이션하지 않도록 선택한 액세스 규칙) - Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션하지 않도록 선택한 ASA 액세스 제어 규칙에 대한 세부 정보입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
 - **Access Rules with Rule Action Change**(규칙 작업이 변경된 액세스 규칙) - Secure Firewall 마이그레이션 툴을 사용하여 '규칙 작업'이 변경된 모든 액세스 제어 정책 규칙에 대한 세부 정보입니다. 규칙 작업 값은 Allow(허용), Trust(신뢰), Monitor(모니터링), Block(차단), Block with reset(차단 후 재설정)입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
 - **Access Control Rules that have IPS Policy and Variable Set Applied**(IPS 정책 및 변수 집합이 적용된 액세스 제어 규칙) - IPS 정책이 적용된 모든 ASA 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 Firewall Threat Defense에서 해당 기능이 지원되는지 확인합니다.
 - **Access Control Rules that have File Policy Applied**(파일 정책이 적용된 액세스 제어 규칙) - 파일 정책이 적용된 모든 ASA 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 Firewall Threat Defense에서 해당 기능이 지원되는지 확인합니다.
 - **Access Control Rules that have Rule 'Log' Setting Change**(규칙 '로그' 설정이 변경된 액세스 제어 규칙) - Secure Firewall 마이그레이션 툴을 사용하여 '로그 설정'이 변경된 ASA 액세스 제어 규칙에 대한 세부 정보입니다. 로그 설정 값은 False(거짓), Event Viewer(이벤트 뷰어), Syslog(시스템 로그)입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
 - **Access Control Rules that have failed Zone-lookup**(영역 조회가 실패한 액세스 제어 규칙) - 경로 조회 작업이 실패했으며 **Post-Migration Report**(마이그레이션 후 보고서)에 입력된 ASA 액세스 제어 규칙에 대한 세부 정보입니다. Secure Firewall 마이그레이션 툴은 소스 구성의 경로(정적 및 연결) 정보를 기반으로 경로 조회 작업을 수행하여 액세스 규칙의 대상 보안 영역을 채웁니다.
 - **Access Control Rules for Tunneled Protocols**(터널링된 프로토콜에 대한 액세스 제어 규칙) - 마이그레이션 중에 사전 필터 터널 규칙으로 마이그레이션되는 터널 규칙에 대한 세부 정보입니다.
 - **Errors/Failure on Migrated Configuration**(마이그레이션된 구성의 오류/실패) — 마이그레이션된 구성 요소를 적용하는 과정에서 마이그레이션 실패를 유발한 오류에 대한 세부 정보입니다. 아래에 보고된 오류는 잘못 마이그레이션된 구성 때문일 수도 있고, 기존 구성이

나 지원되지 않는 기능으로 인해 관리 센터에서 충돌이 발생한 것일 수도 있습니다. 대상 관리 센터로 구성을 전송하거나 재개하기 전에 이러한 오류를 검토하고 확인하십시오.



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



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

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

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

단계 4 Firewall Management Center에서 다음과 같이 합니다.

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

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

- [Threat Defense의 플랫폼 설정](#)에 설명된 SSH 및 HTTPS 액세스를 포함한 플랫폼 설정
- [시스템 로그 구성](#)에 설명된 시스템 로그 설정
- [Threat Defense 라우팅 개요](#)에 설명된 동적 라우팅
- [FlexConfig 정책](#)에 설명된 서비스 정책
- [Threat Defense VPN](#)에 설명된 VPN 컨피그레이션
- [연결 기록](#)에 설명된 연결 로그 설정

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

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

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

Secure Firewall 마이그레이션 툴 제거

모든 구성 요소는 Secure Firewall 마이그레이션 툴과 같은 폴더에 저장됩니다.

시작하기 전에

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

프로시저

단계 1 Secure Firewall 마이그레이션 툴을 배치한 폴더로 이동합니다.

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

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

단계 4 Secure Firewall 마이그레이션 툴을 배치한 폴더를 삭제합니다.



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

샘플 마이그레이션: ASA 를 Threat Defense 2100으로



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

- [유지 보수 기간 작업별](#)
- [유지 보수 기간 작업, 103 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 마이그레이션하는 디바이스 또는 컨텍스트에 대해 **show running-config** 명령을 사용하고 구성의 사본을 저장합니다. [실행 중인 컨피그레이션 보기](#)를 참고하십시오.

또는 마이그레이션하려는 디바이스 또는 컨텍스트에 대해 ASDM(Adaptive Security Device Manager)을 사용하고 **File(파일) > Show Running Configuration in New Windows**(실행 중인 컨피그레이션 표시)를 선택하여 컨피그레이션 파일을 가져옵니다.



참고 멀티 컨텍스트의 경우 **show tech-support** 명령을 사용하여 단일 파일의 모든 컨텍스트에 대한 컨피그레이션을 가져올 수 있습니다.

단계 2 구성 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 구성에 포트 채널이 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, 51 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 ASA 인터페이스와 Firewall Threat Defense 인터페이스를 매핑합니다.



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

예를 들어 의 포트 채널을 Firewall Threat Defense의 물리적 인터페이스에 매핑할 수 있습니다.

자세한 내용은 [Threat Defense 인터페이스와 ASA 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 ASA 논리적 인터페이스를 보안 영역에 수동으로 매핑합니다.

자세한 내용은 [보안 영역 및 인터페이스 그룹에 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 [마이그레이션 후 보고서 검토 및 마이그레이션 완료, 96 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, 101 페이지](#)의 내용을 참조하십시오.

프로시저

단계 1 SSH 콘솔을 통해 에 연결하고 인터페이스 구성 모드로 전환합니다.

단계 2 **shutdown** 명령을 사용하여 인터페이스를 셧다운합니다.

단계 3 (선택 사항) Firewall Management Center에 액세스하고 Firepower 2100 Series 디바이스의 동적 라우팅을 구성합니다.

자세한 내용은 [동적 라우팅](#)을 참고하십시오.

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 ASA 에 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, 105 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 ASA 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 3: 제한된 텔레메트리

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	ASA
디바이스 모델 번호	ASA의 모델 번호	ASA5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 series 2000 MHz, 1 CPU (4 cores)
소스 버전	ASA 버전	9.2 (1)

데이터 포인트	설명	예제 값
Target Management Version(대상 관리 버전)	Management Center의 대상 버전	6.5 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	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
Migration Status(마이그레이션 상태)	Management Center로의 ASA 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 4: 광범위한 텔레메트리

데이터 포인트	설명	예제 값
운영 체제	Secure Firewall 마이그레이션 툴을 실행하는 운영 체제입니다. 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 5: 소스 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	
Source Device Serial Number(소스 디바이스 일련 번호)	ASA의 일련 번호	JAF1528ACAD

데이터 포인트	설명	예제 값
Source Device Model Number(소스 디바이스 모델 번호)	ASA의 모델 번호	ASA5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 series 2000 MHz, 1 CPU (4 cores)
Source Device Version(소스 디바이스 버전)	ASA 버전	9.(2)
Source Config Counts(소스 컨피그레이션 수)	소스 컨피그레이션의 총 라인 수	504
방화벽 모드	ASA에 구성된 방화벽 모드(라우팅 또는 투명)	ROUTED
Context Mode(상황 모드)	ASA의 컨텍스트 모드. 단일 컨텍스트 또는 멀티 컨텍스트일 수 있습니다.	SINGLE
ASA 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)	ASA에 구성된 네트워크 개체의 수	34
Network Object Group Counts(네트워크 개체 그룹 수)	ASA의 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

데이터 포인트	설명	예제 값
툴에서 구문 분석할 수 없는 컨피그레이션 라인 요약		
Unparsed Config Count(구문 분석되지 않은 컨피그레이션 수)	파서에서 인식할 수 없는 컨피그레이션 라인의 수	68
Total Unparsed Access Rule Counts(구문 분석되지 않은 총 액세스 규칙 수)	구문 분석되지 않은 액세스 규칙의 총 수	3
추가 ASA 컨피그레이션 세부 정보...		
Is RA VPN Configured(RA VPN 구성 여부)	RA VPN이 ASA에 구성되었는지 여부	거짓
Is S2S VPN Configured(S2S VPN 구성 여부)	사이트 간 VPN이 ASA에 구성되었는지 여부	거짓
Is BGP Configured(BGP 구성 여부)	BGP가 ASA에 구성되었는지 여부	거짓
Is EIGRP Configured(EIGRP 구성 여부)	ASA에 EIGRP가 구성되어 있는지 여부	거짓
Is OSPF Configured(OSPF 구성 여부)	OSPF가 ASA에 구성되었는지 여부	거짓
Local Users Counts(로컬 사용자 수)	구성된 로컬 사용자의 수	0

표 6: 대상 매니지드 디바이스(Firewall Management Center) 정보

데이터 포인트	설명	예제 값
Target Management Version(대상 관리 버전)	Firewall Management Center의 대상 버전	6.5 이상
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 7: 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...		
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 8: Secure Firewall 마이그레이션 툴 성능 데이터

데이터 포인트	설명	예제 값
Conversion Time(변환 시간)	ASA 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)	ASA 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

텔레메트리 **ASA** 예시 파일

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

```
{
  "metadata": {
    "contentType": "application/json",
    "topic": "migrationtool.telemetry"
  },
  "payload": {
    "asa_config_stats": {
      "access_rules_counts": 46,
      "acl_counts": 46,
      "fqdn_based_access_rule_counts": 7,
      "is_bgp_configured": false,
      "is_eigrp_configured": false,
      "is_multicast_configured": false,
      "is_ospf_configured": false,
      "is_pbr_configured": false,
      "is_ra_vpn_configured": false,
      "is_s2s_vpn_configured": false,
      "is_snmp_configured": false,
      "local_users_counts": 0,
      "nat_rule_counts": 17,
      "network_object_counts": 34,
      "network_object_group_counts": 6,
      "port_object_counts": 85,
      "port_object_group_counts": 37,
      "sgt_based_access_rules_count": 0,
      "timerange_based_access_rule_counts": 1,
      "total_unparsed_access_rule_counts": 3,
      "unparsed_config_count": 68,
      "unsupported_access_rules_count": 3,
      "unsupported_nat_rule_count": 0
    }
  }
}
```

```

    },
    "context_mode": "SINGLE",
    "error_description": null,
    "error_message": null,
    "firewall_mode": "ROUTED",
    "migration_status": "SUCCESS",
    "migration_summary": {
      "access_control_policy": [
        [
          {
            "access_rule_counts": 0,
            "expanded_acp_rule_counts": 0,
            "name": "Doesn't Exist",
            "partially_migrated_acl_rule_counts": 3
          }
        ]
      ],
      "interface_counts": 0,
      "interface_group_counts": 0,
      "nat_Policy": [
        [
          {
            "NAT_rule_counts": 0,
            "name": "Doesn't Exist",
            "partially_migrated_nat_rule_counts": 0
          }
        ]
      ],
      "network_object_rename_counts": 1,
      "network_object_reused_counts": 21,
      "object_group_counts": 6,
      "objects_counts": 34,
      "port_object_rename_counts": 0,
      "port_object_reused_counts": 0,
      "security_zone_counts": 3,
      "static_routes_counts": 0,
      "sub_interface_counts": 0
    },
    "migration_tool_version": "1.1.0.1912",
    "source_config_counts": 504,
    "source_device_model_number": "ASA5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 series
2000 MHz, 1 CPU (4 cores)",
    "source_device_serial_number": "JAF1528ACAD",
    "source_device_version": "9.6(2)",
    "source_type": "ASA",
    "system_information": {
      "browser": "Chrome/69.0.3497.100",
      "operating_system": "Windows NT 10.0; Win64; x64"
    },
    "target_device_model": "Cisco Firepower Threat Defense for VMWare",
    "target_device_version": "75",
    "target_management_type": "Management Center",
    "target_management_version": "6.2.3.3 (build 76)",
    "time": "2018-09-28 18:17:56",
    "tool_performance": {
      "config_push_time": 7,
      "conversion_time": 14,
      "migration_time": 592
    }
  },
  "version": "1.0"
}

```




4 장

마이그레이션 문제 해결

- [Secure Firewall 마이그레이션 툴 문제 해결, 113 페이지](#)
- [문제 해결에 사용되는 로그 및 기타 파일, 114 페이지](#)
- [ASA 파일 업로드 실패 문제 해결, 114 페이지](#)

Secure Firewall 마이그레이션 툴 문제 해결

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

마이그레이션 프로세스가 실패하는 몇 가지 일반적인 시나리오는 다음과 같습니다.

- ASA 컨피그레이션 파일의 알 수 없는 문자 또는 잘못된 문자
- ASA 컨피그레이션 파일의 불완전하거나 누락된 요소
- 네트워크 연결 끊김 또는 레이턴시

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
telemetry_sessionid_timestamp.json	<migration_tool_folder>\resources\telemetry_data

ASA 파일 업로드 실패 문제 해결

ASA 구성 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.

- Secure Firewall 마이그레이션 툴에 의해 표시되는 오류 메시지 - 실패의 원인을 개략적으로 요약하여 제공합니다.
- Log file(로그 파일) - "error"라는 단어를 검색하여 실패의 원인을 확인합니다.

ASA에 대한 문제 해결 예: 개체 그룹의 멤버를 찾을 수 없음

이 예에서는 파서가 개체 그룹의 멤버 중 하나를 찾을 수 없으므로 ASA 컨피그레이션 파일 업로드 및 구문 분석이 실패했습니다.

프로시저

단계 1 오류 메시지를 검토하여 문제를 식별합니다.

이 실패로 인해 다음 오류 메시지가 생성되었습니다.

Location	오류 메시지
마이크그레이션 툴 메시지	해당 없음
마이크그레이션 전 보고서의 Configuration Lines with Errors(오류가 있는 컨피그레이션 라인) 섹션	Line#2[ERROR] group-object GROUP1 Line#3[ERROR] group-object GROUP2 Line#1[ERROR] object-group network NOV-SERVERS
로그 파일	[INFO object_group_mode.py:9491 > Parsing object-group network: [NOV-SERVERS] [ERROR object_group_mode.py:1048] [GROUP1] group not found when creating object-group network [NOV-SERVERS] [ERROR object_group_mode.py:1049] no row was found for one() [ERROR object_group_mode.py:1048] [GROUP2] group not found when creating object-group network [NOV-SERVERS] [ERROR object_group_mode.py:1049] no row was found for one()

단계 2 ASA 컨피그레이션 파일을 열고 다음과 같이 합니다.

a) NOV-SERVERS라는 이름으로 개체 그룹을 검색합니다.

ASA 컨피그레이션 파일에서 NOV-SERVERS에 대한 다음 라인이 표시됩니다.

```
object-group network NOV-SERVERS
  group-object GROUP1
  group-object GROUP2
```

b) 그룹의 각 멤버를 검색하여 ASA 컨피그레이션 파일에 포함되지 않은 멤버를 식별합니다.

단계 3 오류를 해결하려면 소스 ASA 디바이스에서 ASDM을 사용하여 다음과 같이 합니다.

a) 개체 그룹에 대해 누락된 멤버를 생성합니다.

b) 컨피그레이션 파일을 내보냅니다.

단계 4 오류가 더 이상 없으면 새 ASA 구성 파일을 Secure Firewall 마이크그레이션 툴에 업로드하고 마이크그레이션을 계속합니다.

ASA에 대한 문제 해결 예: 목록 인덱스 범위를 벗어남

이 예에서는 Secure Firewall 마이크그레이션 툴이 지원하지 않는 요소의 컨피그레이션 오류로 인해 ASA 컨피그레이션 파일 업로드 및 구문 분석이 실패했습니다.

프로시저

단계 1 오류 메시지를 검토하여 문제를 식별합니다.

이 실패로 인해 다음 오류 메시지가 생성되었습니다.

Location	오류 메시지
마이그레이션 툴 메시지	list index out of range
마이그레이션 전 보고서의 Configuration Lines with Errors(오류가 있는 컨피그레이션 라인) 섹션	해당 없음
로그 파일	[ERROR asa_config_upload.py:119] > list index out of range

단계 2 구문 분석되지 않은 파일을 열고 맨 아래로 스크롤하여 성공적으로 구문 분석된 ASA 컨피그레이션 파일의 마지막 라인을 식별합니다.

이 예에서 구문 분석되지 않은 파일의 마지막 라인은 다음과 같습니다.

```
Line#345 [SKIPPED] address 209.165.200.224 255.255.255.224
```

단계 3 ASA 컨피그레이션 파일을 열고 다음과 같이 합니다.

a) address 209.165.200.224 255.255.255.224를 찾습니다.

이 라인 다음에 오는 라인에 문제를 일으킨 컨피그레이션 요소가 포함되어 있습니다.

b) 해당 라인을 검토하여 마이그레이션이 실패한 원인을 확인합니다.

이 예에서 Secure Firewall 마이그레이션 툴이 구문 분석을 중지한 라인은 name www.example.s3.amazonaws.com입니다. 이는 구문 분석되지 않은 파일의 마지막 라인 바로 뒤에 있는 ASA 컨피그레이션 파일의 라인입니다. 이 라인에서 문제를 식별할 수 없는 경우, [Secure Firewall 마이그레이션 툴 릴리즈 노트](#)에서 알려진 문제 섹션을 검토하여 릴리스에서 알려진 문제 중 하나가 발생했는지 확인하는 것이 좋습니다.

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.