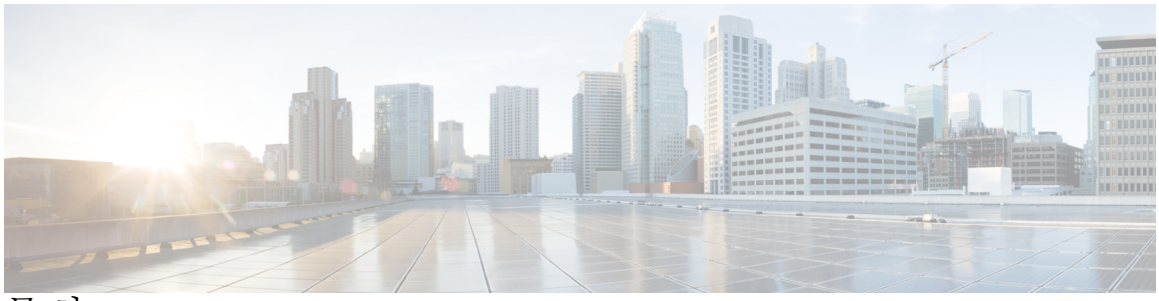
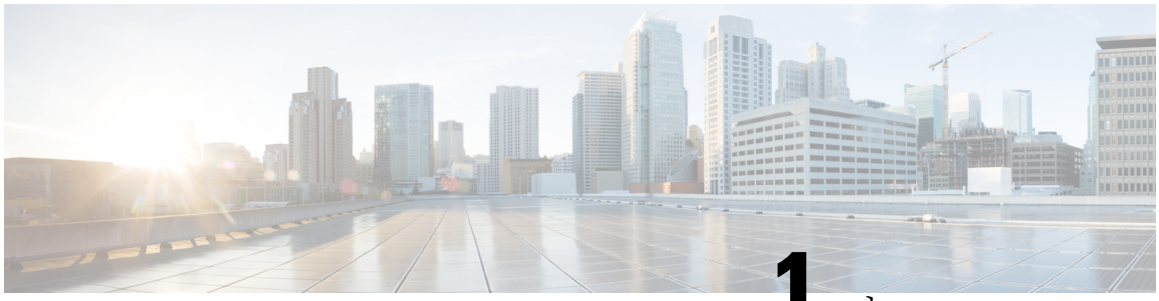
마이그레이션 툴을 사용하여 Fortinet 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션하기

최종 변경: 2024년 12월 16일

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



목 차



1 장

Secure Firewall 마이그레이션 툴 시작하기

Secure Firewall 마이그레이션 툴 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.

이 설명서에 포함된 샘플 마이그레이션 절차(샘플 마이그레이션: Fortinet를 Threat Defense 2100으로)를 참조하면 마이그레이션 프로세스를 쉽게 이해할 수 있습니다.

Secure Firewall 마이그레이션 툴은 지원되는 Fortinet 구성을 지원되는 Secure Firewall Threat Defense 플랫폼으로 전환합니다. Secure Firewall 마이그레이션 툴을 사용하면 지원되는 Fortinet 기능 및 정책을 Threat Defense로 자동 마이그레이션할 수 있습니다. 지원되지 않는 모든 기능을 수동으로 마이그레이션해야 할 수 있습니다.

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

- Fortinet 컨피그레이션 항목 중 완전히 마이그레이션되는 항목, 부분적으로 마이그레이션되는 항목, 마이그레이션이 지원되지 않는 항목, 마이그레이션에서 무시되는 항목

- 오류가 있는 Fortinet 구성 라인. Secure Firewall 마이그레이션 툴이 인식할 수 없는 Fortinet CLI를 나열합니다. 이로 인해 마이그레이션이 차단됩니다.

구문 분석 오류가 있는 경우 문제를 해결하고, 새 컨피그레이션을 다시 업로드하고, 대상 디바이스에 연결하고, 인터페이스를 Threat Defense 인터페이스에 매핑하고, 애플리케이션을 매핑하고, 보안 영역을 매핑하고, 컨피그레이션을 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, Fortinet 구성 및 **resources(**리소스**)** 폴더에 있는 로그의 사본을 저장합니다.

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

구문 분석되지 않은 파일

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**)** 페이지의 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 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 수있는 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
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 ASA**를 **Cisco Secure Firewall Threat Defense**로 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 *Cisco Secure Firewall ASA*를 *Cisco Secure Firewall Threat Defense*로 마이그레이션 책에서 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정을 참조하십시오. • 이제 Cisco ASA 디바이스에서 사이트 간 VPN 구성을 마이그레이션할 때 위협 방어 디바이스를 사용하여 사이트 간 허브 앤 스포크 VPN 토폴로지를 구성할 수 있습니다. **Optimize, Review and Validate Configuration(**구성 최적화**,** 검토 및 검증**)** 페이지의 **Site-to-Site VPN Tunnels(**사이트 간 **VPN** 터널**)** 아래에서 **Add Hub & Spoke Topology(**허브 및 스포크 토폴로지 추가**)**를 클릭합니다. 자세한 내용은 마이그레이션 툴을 사용하여 *Cisco Secure Firewall ASA*를 *Cisco Secure Firewall Threat Defense*로 마이그레이션 책에서 구성 최적화, 검토 및 검증을 참조하십시오. **Fortinet** 방화벽에서 **Cisco Secure Firewall Threat Defense**로 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 *Fortinet* 방화벽을 *Cisco Secure Firewall Threat Defense*로 마이그레이션하기 책에서 Fortinet 구성 지원을 참조하십시오.

버전	지원 기능
6.0.1	

버전	지원 기능
	이 릴리스에는 다음과 같은 새로운 기능과 개선 사항이 포함되어 있습니다. **Cisco Secure Firewall ASA**를 **Cisco Secure Firewall Threat Defense**로 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 Defense**로 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 Defense**로 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 Defense**로 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 Firewall**에서 **Cisco Secure Firewall Threat Defense**로 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 ASA**를 **Cisco Secure Firewall Threat Defense**로 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 **VRF**에 매핑 페이지에서 매핑할 수 있습니다. 이 기능을 적용하려면 ASA 버전이 9.19(x) 이상인지 확인합니다. **FDM** 매니지드 디바이스를 **Cisco Secure Firewall Threat Defense**로 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 Firewall**에서 **Cisco Secure Firewall Threat Defense**로 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 Defense**로 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 섀도 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 내용 은 마이그레이션 툴을 사용하여 *Palo Alto Networks Firewall*을 *Secure Firewall Threat Defense*로 마이그레이션 가이드의 애플리케이션으로 구성 매핑을 참조하십시오.
4.0.2	Secure Firewall 마이그레이션 툴 4.0.2에는 다음과 같은 새로운 기능 및 개선 사항이 포함되어 있습니다. • 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. .

버전	지원 기능
3.0.1	• FirePOWER Services를 포함한 ASA, Check Point, Palo Alto Networks 및 Fortinet의 경우 Secure Firewall 3100 Series는 대상 디바이스로만 지원됩니다.
3.0	Secure Firewall 마이그레이션 툴 3.0은 대상 Management Center가 7.2 이상인 경우 Fortinet에서 클라우드 제공 Firewall Management Center로의 마이그레이션을 지원합니다.
2.5.2	Secure Firewall 마이그레이션 툴 2.5.2는 Fortinet 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. • 섀도우 ACL - 첫 번째 ACL은 두 번째 ACL의 컨피그레이션을 완전히 섀도잉합니다. 참고 최적화는 Fortinet ACP 규칙 작업에만 사용할 수 있습니다. Secure Firewall 마이그레이션 툴 2.5.2는 대상 Management Center가 7.1 이상인 경우 BGP(Border Gateway Protocol) 및 유동 경로 개체 마이그레이션을 지원합니다.

버전	지원 기능
2.3	• Fortinet 방화벽 OS 버전 5.0 이상 지원 • Secure Firewall 마이그레이션 툴을 사용하여 다음과 같은 Fortinet 구성 요소를 Threat Defense로 마이그레이션할 수 있습니다. • 인터페이스 • 영역 • 고정 경로 • 네트워크 개체 및 그룹 • 서비스 개체 및 그룹 • 액세스 제어 목록 • NAT 종속 개체 (IP 풀, 가상 IP) • NAT 규칙 • VDOM • 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. 참고 시간 기반 개체는 Management Center 6.6 이상 버전에서 지원됩니다.

Secure Firewall 마이그레이션 툴 라이선싱

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

Fortinet 방화벽 구성 파일의 요구 사항 및 사전 요건

Fortinet 방화벽 컨피그레이션 파일을 수동으로 가져올 수 있습니다.

Secure Firewall 마이그레이션 툴에 수동으로 가져오는 Fortinet 방화벽 구성 파일은 다음 요구 사항을 충족해야 합니다.

- Fortinet 디바이스에서 내보낸 실행 중인 컨피그레이션이 있습니다. 방화벽 마이그레이션 툴에서는 전역 및 VDOM 단위 내보내기의 컨피그레이션 백업이 지원됩니다. 자세한 내용은 Fortinet 컨피그레이션 파일 내보내기를 참고하십시오.
- 유효한 Fortinet 방화벽 CLI 구성만 포함하고 있습니다.
- 구문 오류가 없습니다.
- 파일 확장명이 `.cfg` 또는 `.txt`입니다.
- 파일 인코딩으로 UTF-8을 사용합니다.
- 직접 코딩하거나 수동으로 변경하지 않았습니다. Fortinet 방화벽 구성을 수정하는 경우 Fortinet 방화벽 디바이스에서 수정된 구성 파일을 테스트하여 파일이 유효한 구성인지 확인하는 것이 좋습니다.

Threat Defense 디바이스의 요구 사항 및 사전 요건

Management Center로 마이그레이션할 때 대상 Threat Defense 디바이스가 추가되거나 추가되지 않을 수 있습니다. 나중에 Threat Defense 디바이스에 구축하도록 공유 정책을 Management Center로 마이그레이션할 수 있습니다. 디바이스별 정책을 Threat Defense로 마이그레이션하려면 Management Center에 추가해야 합니다. Fortinet 방화벽 구성을 Threat Defense로 마이그레이션하려는 경우 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 Threat Defense 디바이스가 컨테이너 인스턴스인 경우 Fortinet 방화벽 와 같은 수의 물리적 인터페이스, 물리적 하위 인터페이스, 포트 채널 인터페이스 및 포트 채널 하위 인터페

이스('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.

Fortinet 구성 지원

지원되는 **Fortinet** 방화벽 컨피그레이션

Secure Firewall 마이그레이션 툴은 다음 FortiNet 방화벽 구성을 완전히 마이그레이션할 수 있습니다.

- 네트워크 개체 및 그룹(와일드카드 FQDN, 와일드카드 마스크, Fortinet 동적 개체 제외)
- 서비스 개체
- 서비스 개체 그룹(중첩된 서비스 개체 그룹 제외)

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

- URL 개체
- IPv4 및 IPv6 FQDN 개체 및 그룹
- IPv6 변환 지원(인터페이스, 정적 경로, 개체, ACL 및 NAT)
- IPv6 SSL VPN
- SSL VPN 구성의 다중 인터페이스 및 인터페이스 영역
- Central SNAT
- 액세스 규칙
- NAT 규칙
- 정적 경로, 마이그레이션되지 않은 ECMP 경로
- 물리적 인터페이스

- 하위 인터페이스(하위 인터페이스 ID는 마이그레이션 시 항상 VLAN ID와 동일한 숫자로 설정됨)
- 집계 인터페이스(포트 채널)
- Secure Firewall 마이그레이션 툴은 별도의 Threat Defense 디바이스로서 Fortinet 방화벽에서 개별 VDOM 마이그레이션을 지원합니다.
- 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. **Optimize, Review and Validate Configuration(**컨피그레이션 최적화**,** 검토 및 검증**)** 페이지의 규칙에 따라 개체를 검증합니다.

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

참고

- 소스 Fortinet에서 대상 위협 방어로 표준 시간대 구성을 수동으로 마이그레이션해야 합니다.
- 시간 기반 개체는 비 위협 방어 플로우에 대해 지원되지 않으므로 비활성화됩니다.
- 시간 기반 개체는 Management Center 버전 6.6 이상에서 지원됩니다.

부분적으로 지원되는 **Fortinet** 방화벽 컨피그레이션

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

- 지원되지 않는 주소 개체가 포함된 주소 그룹입니다.
- TCP 또는 UDP 및 SCTP를 포함하는 프로토콜이 있는 서비스 개체를 포함하는 서비스 그룹입니다.

참고 SCTP 프로토콜이 제거되고 서비스 그룹이 부분적으로 마이그레이션됩니다.

지원되지 않는 **Fortinet** 방화벽 컨피그레이션

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

- 사용자 기반, 디바이스 기반 및 인터넷 서비스 ID 기반 액세스 제어 정책 규칙
- 지원되지 않는 ICMP 유형 및 코드가 포함된 서비스 개체
- 터널링 프로토콜 기반 액세스 제어 정책 규칙
- 블록 할당 옵션으로 구성된 NAT 규칙
- SCTP로 구성된 NAT 규칙
- 호스트 '0.0.0.0'으로 구성된 NAT 규칙
- 소스 또는 대상에 FQDN 개체가 있는 NAT 규칙
- 특수 문자로 시작하거나 특수 문자를 포함하는 FQDN 개체
- 와일드카드 FQDN
- Fortinet 방화벽에서는 IPv4 및 IPv6(통합 정책)을 결합하는 정책을 구성할 수 있습니다. 그러나, 마이그레이션 툴은 그러한 구성의 마이그레이션을 지원하지 않습니다.

FortiNet 방화벽 컨피그레이션 지침 및 제한 사항

변환 중에 Secure Firewall 마이그레이션 툴은 지원되는 모든 개체 및 규칙에 대해 일대일 매핑을 생성합니다(규칙 또는 정책에 사용되는지 여부와 무관). 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 인터페이스, 개체, NAT 규칙 및 경로는 마이그레이션되지 않습니다.
- 지원되지 않는 ACL 규칙은 비활성화된 규칙으로 Management Center에 마이그레이션됩니다.

Fortinet 방화벽 컨피그레이션 제한 사항

소스 FortiNet 방화벽 컨피그레이션을 마이그레이션하는 경우 다음과 같은 제한 사항이 있습니다.

- 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.
- 가상 유선, 이중 인터페이스, 터널 인터페이스, vdom-link 및 SDwan 인터페이스 또는 영역 유형인 Fortinet 방화벽 인터페이스는 지원되지 않으며 마이그레이션되지 않습니다.

  FortiNet 하드웨어 또는 소프트웨어 전환 논리적 인터페이스는 위협 방어 L3-인터페이스로 마이그레이션됩니다. 하드웨어 또는 소프트웨어 전환 멤버 인터페이스는 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션되지 않습니다.

- 와일드카드 FQDN, 와일드카드 IP, 동적 개체 및 제외 그룹과 같은 개체의 마이그레이션은 지원되지 않습니다.
- 투명 모드 또는 투명 VDOM의 Fortinet 방화벽 디바이스는 마이그레이션할 수 없습니다.
- 중첩된 서비스 개체 그룹 및 포트 그룹은 Management Center에서 지원되지 않습니다. 변환 과정에서 Secure Firewall 마이그레이션 툴은 참조된 중첩 개체 그룹 또는 포트 그룹의 콘텐츠를 확장합니다.
- Secure Firewall 마이그레이션 툴은 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 Management Center 규칙으로 변환됩니다.

Fortinet 방화벽 마이그레이션 지침

Secure 마이그레이션 툴은 위협 방어 구성에 대한 모범 사례를 사용합니다.

ACL 로그 옵션의 마이그레이션은 위협 방어의 모범 사례를 따릅니다. 규칙에 대한 로그 옵션은 소스 FortiNet 방화벽 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.

Threat Defense 디바이스에 대한 지침 및 제한 사항

구성을 위협 방어로 마이그레이션하려는 경우 다음 지침 및 제한 사항을 고려하십시오.

- 경로, 인터페이스 등 기존 디바이스별 구성이 위협 방어에 있는 경우 푸시 마이그레이션 중에 Secure Firewall 마이그레이션 툴이 디바이스를 자동으로 정리하고 구성에서 덮어씁니다.

참고 디바이스(대상 위협 방어) 구성 데이터의 원치 않는 손실을 방지하려면 마이그레이션 전에 디바이스를 수동으로 정리하는 것이 좋습니다.

- FortiNet 하드웨어 또는 소프트웨어 전환 논리적 인터페이스는 위협 방어 L3-인터페이스로 마이그레이션됩니다. 하드웨어 또는 소프트웨어 전환 멤버 인터페이스는 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션되지 않습니다.

  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.

마이그레이션에 지원되는 플랫폼

다음 Fortinet 및 Threat Defense 플랫폼은 Secure Firewall 마이그레이션 툴을 사용한 마이그레이션에 지원됩니다. 지원되는 Threat Defense 플랫폼에 대한 자세한 내용은 Cisco Secure Firewall 호환성 가이드에서 참고하십시오.

지원되는 대상 **Threat Defense** 플랫폼

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

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Secure Firewall 4200 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 Threat Defense Virtual사전 요건 및 사전 스테이징에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense Virtual 시작하기 및 Azure를 참고하십시오.
- AWS 클라우드의 Threat Defense Virtual 사전 요구 사항 및 사전 스테이징에 대한 자세한 내용은 Threat Defense Virtual 사전 요건을 참고하십시오.

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

참고 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션을 성공적으로 수행하려면 먼저 Management Center 또는 Threat Defense Virtual을 사전 스테이징하는 사전 요건을 충족해야 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, 23 페이지에 설명된 대로 마이그레이션에 지원되는 Management Center 소프트웨어 버전.
- 다음에 설명된 대로 Fortinet 인터페이스에서 마이그레이션하려는 모든 기능을 포함하는 Threat Defense용 스마트 라이선스를 얻고 설치해야 합니다.
  - Cisco.com에 있는 Cisco 스마트 어카운트의 Getting Started(시작하기) 섹션
  - Cisco Smart Software Manager에 Firewall Management Center를 등록합니다.
  - Firewall 시스템 라이선싱
  - Management Center에서 REST API를 활성화해야 합니다.

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

보안 클라우드 제어에서 클라우드 제공 Firewall Management Center에 액세스할 수 있습니다. 보안 클라우드 제어는 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 관리를 참고하십시오.

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

보안 클라우드 제어 지역

보안 클라우드 제어는 3개의 서로 다른 지역에서 사용할 수 있으며, 지역은 URL 확장명으로 식별할 수 있습니다.

표 *1:* 보안 클라우드 제어 지역 및 *URL*

지역	보안 클라우드 제어 **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

다음은 지원되는 Secure Firewall 마이그레이션 툴, Fortinet 및 마이그레이션용 Threat Defense 버전입니다.

지원되는 Secure Firewall 마이그레이션 툴 버전

software.cisco.com에 게시된 버전은 Cisco 엔지니어링 및 지원 조직에서 공식적으로 지원하는 버전입니다. software.cisco.com 에서 최신 버전의 Secure Firewall 마이그레이션 툴을 다운로드하는 것이 좋습니다.

지원되는 Fortinet 방화벽 버전

Secure Firewall 마이그레이션 툴은 FortiNet 방화벽 OS 5.0.x 이상 버전을 실행하는 Threat Defense로의 마이그레이션을 지원합니다.

소스 Fortinet 방화벽 컨피그레이션에 지원되는 Management Center 버전

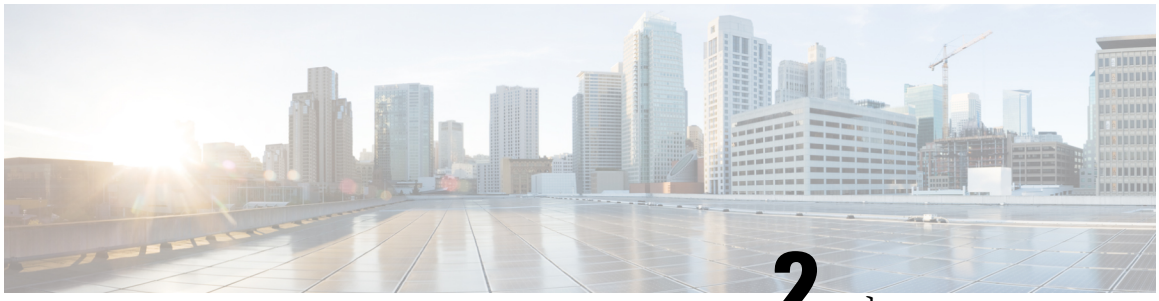
Fortinet 방화벽의 경우 Secure Firewall 마이그레이션 툴은 6.2.3.3 이상 버전을 실행하는 Management Center에서 관리되는 Threat Defense 디바이스로의 마이그레이션을 지원합니다.

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

지원되는 Threat Defense 버전

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

Threat Defense의 운영체제 및 호스팅 환경 요구 사항을 포함한 Cisco Firewall 소프트웨어 및 하드웨어 호환성에 대한 자세한 내용은 Cisco Firewall 호환성 가이드를 참고하십시오.

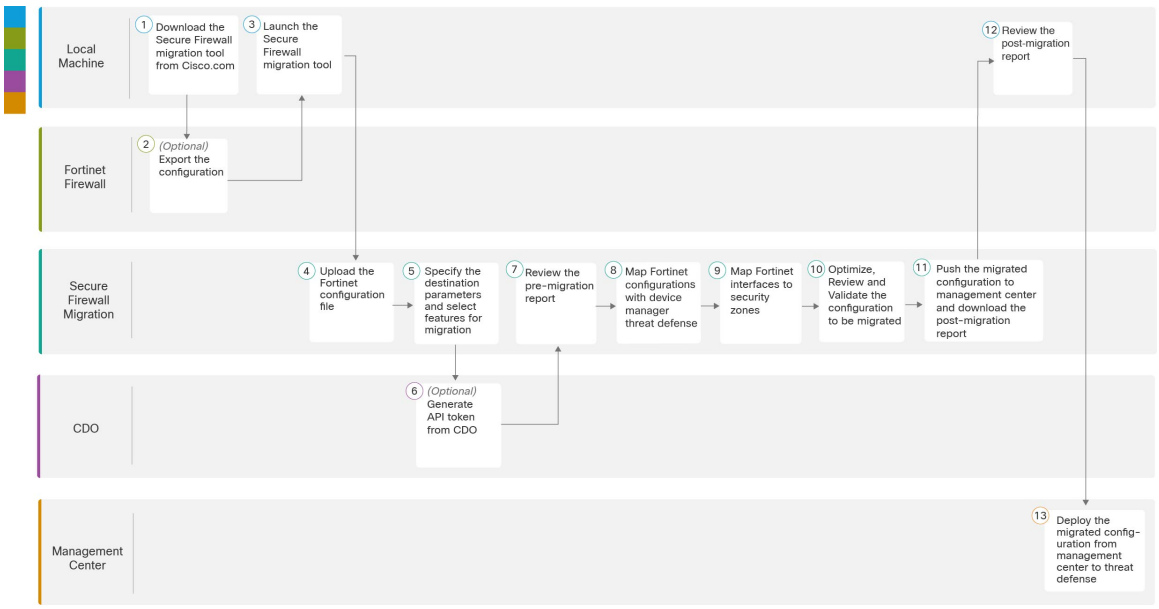


2 장

Fortinet Firewall을 Threat Defense로 마이그레이션 워크플로우

엔드 투 엔드 절차

다음 순서도는 Secure Firewall 마이그레이션 툴을 사용하여 Fortinet 방화벽을 Threat Defense로 마이그레이션하는 워크플로우를 보여줍니다.



	업무 환경	단계
1	Fortnet 방화벽	로컬 시스템으로 구성을 내보냅니다. Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드를 참조하십시오.
2	Fortinet 방화벽	구성 파일 내보내기: Fortinet 방화벽에서 구성을 내보내려면 Fortinet 방화벽에서 컨피그레이션 내보내기를 참조하십시오.
3	로컬 컴퓨터	로컬 컴퓨터에서 Secure Firewall 마이그레이션 툴을 실행합니다(Secure Firewall 마이그레이션 툴 실행 참조).
4	Secure Firewall 마이그레이션 툴	Fortinet 방화벽에서 내보낸 Fortinet 구성 파일을 업로드합니다. Fortinet 구성 파일 업로드를 참조하십시오.
5	Secure Firewall 마이그레이션 툴	이 단계에서 마이그레이션의 대상 매개변수를 지정할 수 있습니다. 자세한 단계는 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정을 참고하십시오. .
6	보안 클라우드 제어	(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 지정를 참조하십시오.
7	Secure Firewall 마이그레이션 툴	마이그레이션 전 보고서를 다운로드한 위치로 이동하여 보고서를 검토합니다. 자세한 단계는 마이그레이션 전 보고서 검토를 참고하십시오.
8	Secure Firewall 마이그레이션 툴	Fortinet 구성이 올바르게 마이그레이션되도록 하려면 Fortinet 인터페이스를 적절한 위협 방어 인터페이스 개체, 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 단계는 Fortinet Firewall 구성과 Threat Defense 인터페이스 매핑을 참조하십시오.
9	Secure Firewall 마이그레이션 툴	Fortinet 인터페이스를 적절한 보안 영역에 매핑합니다. 자세한 단계는 Fortinet 인터페이스를 보안 영역 및 에 매핑을 참조하십시오.
10	Secure Firewall 마이그레이션 툴	구성을 최적화하고 신중하게 검토하여 구성이 올바른지 확인하고 Threat Defense 디바이스를 구성하는 방법과 일치하는지 확인합니다. 자세한 단계는 최적화, 구성 검토 및 검증을 참고하십시오.
11	Secure Firewall 마이그레이션 툴	마이그레이션 프로세스의 이 단계에서는 마이그레이션된 구성을 Management Center로 전송하며, 마이그레이션 후 보고서를 다운로드할 수 있습니다. 자세한 단계는 마이그레이션된 컨피그레이션을 Management Center에 푸시를 참고하십시오.
12	로컬 컴퓨터	마이그레이션 후 보고서를 다운로드한 위치로 이동하여 보고서를 검토합니다. 자세한 단계는 마이그레이션 후 보고서 검토 및 마이그레이션 완료를 참고하십시오.

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

마이그레이션 사전 요건

Fortinet 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.

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/type으로 이동하여 **Firewall** 마이그레이션 툴을 클릭합니다.

위 링크를 클릭하면 Firewall NGFW Virtual 아래의 Secure Firewall 마이그레이션 툴로 이동합니다. 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.

Fortinet 방화벽에서 컨피그레이션 내보내기

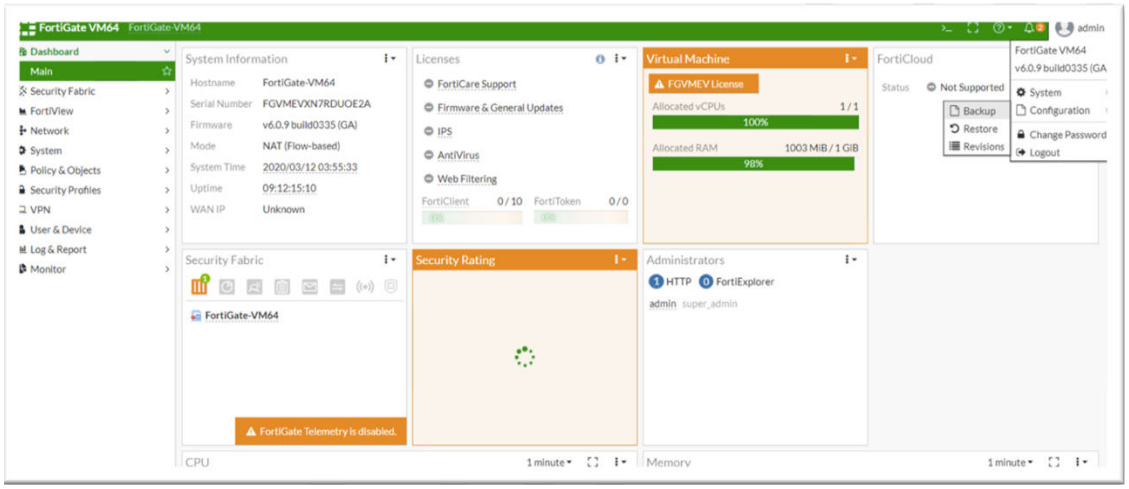
다음과 같은 방법으로 Fortinet 방화벽 컨피그레이션을 내보낼 수 있습니다.

Fortinet 방화벽 GUI에서 Fortinet 방화벽 컨피그레이션 내보내기

Fortinet 방화벽 GUI에서 컨피그레이션을 추출하려면 다음 단계를 수행합니다.

프로시저

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



단계 2 백업을 로컬 PC 또는 USB 디스크로 전송합니다.

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

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

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

단계 4 **OK(확인)**를 선택합니다.

컨피그레이션 파일을 저장할 위치를 묻는 메시지가 웹 브라우저에 표시됩니다.

컨피그레이션 파일의 확장명은 **.conf**입니다.

다음에 수행할 작업

Fortinet 구성 파일 업로드

FortiManager에서 Fortinet 방화벽 컨피그레이션 내보내기

FortiManager에서 관련 디바이스 컨피그레이션을 추출할 수 있습니다.

프로시저

단계 **1** FortiManager에 로그인합니다.

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

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

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

다운로드한 파일은 확장명이 .conf인 파일 형식입니다.

다음에 수행할 작업

Fortinet 구성 파일 업로드

마이그레이션 실행

Secure Firewall 마이그레이션 툴 실행

이 작업은 Secure Firewall 마이그레이션 툴의 데스크톱 버전을 사용하는 경우에만 적용됩니다. 보안 클라우드 제어에서 호스팅되는 마이그레이션 툴의 클라우드 버전을 사용하는 경우, Fortinet 구성 파일 업로드로 건너뜁니다.

참고 Secure Firewall 마이그레이션 툴을 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.com에서 Secure Firewall 마이그레이션 툴 다운로드
- 마이그레이션에 지원되는 대상 Management Center, 22 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 설정을 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.

  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 열기를 참고하십시오.

  참고
  MAC 터미널 압축 방법을 사용합니다.

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

Cisco Success Network로 통계를 전송하는 데 동의하면 Cisco.com 계정을 사용하여 로그인하라는 메시지가 표시됩니다. Cisco Success Network로 통계를 보내지 않도록 선택하는 경우 로컬 자격 증명을 사용하여 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(CCO**로 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 8단계로 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 확인하는 링크를 클릭합니다.

단계 **11** **Proceed(**진행**)**를 클릭합니다.

다음에 수행할 작업

다음 단계로 진행할 수 있습니다.

- Secure Firewall 마이그레이션 툴을 사용하여 Fortinet 방화벽에서 정보를 추출해야 하는 경우 Fortinet 방화벽에서 컨피그레이션 내보내기로 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 및 데모 FTD 디바이스와 같은 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 처음 부터 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.

Fortinet 구성 파일 업로드

시작하기 전에

소스 Fortinet 디바이스에서 컨피그레이션 파일을 `.conf` 또는 `.txt`로 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** Secure Firewall 마이그레이션 툴이 컨피그레이션 파일을 업로드합니다. 대규모 컨피그레이션 파일의 경우 이 단계는 시간이 더 오래 걸립니다. 콘솔에서는 구문 분석 중인 Fortinet 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 Fortinet에 해당하는지 여부가 나와 있습니다.

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

단계 **3** **Start Parsing(**구문 분석 시작**)**을 클릭합니다.

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

단계 **4** 업로드된 구성 파일에서 Secure Firewall 마이그레이션 툴이 감지하고 구문 분석한 요소에 대한 요약을 검토합니다.

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

다음에 수행할 작업

Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 33 페이지

Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정

시작하기 전에

보안 클라우드 제어에서 호스팅되는 마이그레이션 툴의 클라우드 버전을 사용하는 경우 단계 3로 건너뜁니다.

- 온프레미스 Firewall Management Center용 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 Center를 참조하십시오.
- (선택 사항) 인터페이스 및 경로와 같은 디바이스별 구성을 마이그레이션하려면 대상을 추가합니다. Threat Defense 인 경우 Management Center에 대상 Threat Defense 디바이스를 추가합니다. Firewall Management Center에 디바이스 추가 참고
- **Review and Validate(**검토 및 검증**)** 페이지에서 ACL에 IPS 또는 파일 정책을 적용해야 하는 경우 마이그레이션 전에 Management Center에서 정책을 생성하는 것이 매우 권장됩니다. Secure Firewall 마이그레이션 툴이 연결된 Management Center에서 정책을 가져오므로 동일한 정책을 사용합니다. 새 정책을 생성하고 여러 액세스 제어 목록에 할당하면 성능이 저하될 수 있으며 푸시가 실패할 수도 있습니다.

프로시저

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

- 온프레미스 Firewall Management Center로 마이그레이션하려면 다음을 수행합니다.

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

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

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

- 클라우드 제공 Firewall Management Center로 마이그레이션하려면 다음을 수행합니다.

a) **Cloud** 사용 **FMC** 라디오 버튼을 클릭합니다.
b) 지역을 선택하고 보안 클라우드 제어 API 토큰을 붙여넣습니다. API 토큰을 생성합니다. 보안 클라우드 제어에서 다음 단계를 수행합니다.

1. 보안 클라우드 제어에 로그인합니다.
2. 오른쪽 상단에서 **Preferences(**환경 설정**)** > **General Preferences(**일반 환경설정**)**로 이동하여 **My Tokens(**내 토큰**)** 섹션의 API 토큰을 복사합니다.

c) **Connect(**연결**)**를 클릭하고 **2**단계로 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 Management Center에 로그인하여 해당 Management Center에서 관리되는 Threat Defense 디바이스 목록을 검색합니다. 콘솔에서 이 단계의 진행 상황을 볼 수 있습니다.

단계 **3** **Proceed(**진행**)**를 클릭합니다.

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

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

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

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

  원격 구축이 활성화된 상태에서 Management Center 또는 Threat Defense 6.7 이상으로의 Fortinet 방화벽 마이그레이션은 Secure Firewall 마이그레이션 툴에서 지원됩니다. 하지만 인터페이스와 경로는 수동으로 마이그레이션해야 합니다.

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

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

단계 **5** **Proceed(**진행**)**를 클릭합니다.

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

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

- 대상 Threat Defense 디바이스로 마이그레이션하는 경우 Secure Firewall 마이그레이션 툴이 **Device Configuration(**디바이스 구성**)** 및 **Shared Configuration(**공유 구성**)** 섹션의 Fortinet 구성에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.
- Management Center로 마이그레이션하는 경우 Secure Firewall 마이그레이션 툴이 **Device Configuration(**디바이스 구성**)** 및 **Shared Configuration(**공유 구성**)** 및 **Optimization(**최적화**)** 섹션에서 Fortinet 구성에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.
- Fortinet 방화벽에서 구성을 마이그레이션할 때 Fortinet 방화벽에 VPN이 구성되어 있는 경우 **Select Features(**기능 선택**)** 창에서 다음을 수행해야 합니다.
  - 마이그레이션 툴은 **Device Configuration(**디바이스 설정**)**아래에 사이트 간 VPN 기능이 표시됩니다. 요구 사항에 따라 **Policy Based (Crypto Map)(**정책 기반**(**암호화 맵**))** 또는 **Route Based (VTI)(**경로 기반 **(VTI))**를 선택합니다.
  - 마이그레이션 툴의 **Shared Configuration(**공유 구성**)** 아래에 원격 액세스 VPN 기능이 표시됩니다.
  - **SSL VPN** 또는 **IPsec VPN**과 **SSL VPN** 둘 다 선택합니다.

    참고
    사전 공유 키 기반(PSK 기반) 또는 인증서 기반 인증은 원격 액세스 VPN 구성에 대해 Management Center에서 지원되지 않으므로 **IPsec VPN**만 선택할 수 없습니다.

  Fortinet 방화벽 구성에 사이트 간 및 원격 액세스 VPN이 구성되어 있는 경우, 이는 **Select Features(**기능 선택**)** 창에 기본적으로 선택됩니다. 필요한 경우 확인란을 사용하여 선택을 취소합니다.

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

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

- (선택 사항) **Optimization(**최적화**)** 섹션에서 **Migrate only referenced objects(**참조된 개체만 마이그레이션**)**를 선택하여 액세스 제어 정책 및 NAT 정책에서 참조되는 개체만 마이그레이션합니다.

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

단계 **7** **Proceed(**진행**)**를 클릭합니다.

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

단계 **9** Secure Firewall 마이그레이션 툴에서 변환한 요소의 요약을 검토합니다.

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

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

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

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.

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.

- Threat Defense로 성공적으로 마이그레이션할 수 있는 지원되는 Fortinet 구성 요소 및 마이그레이션을 위해 선택한 특정 Fortinet 기능의 요약입니다.
- **Configuration Lines with Errors(**오류가 있는 구성 라인**)** - Secure Firewall 마이그레이션 툴이 구문 분석할 수 없으므로, 마이그레이션할 수 없는 Fortinet 구성 요소에 대한 세부 정보입니다. 계속 진행하기 전에 Fortinet 구성에서 이러한 오류를 해결하고 새 구성 파일을 내보낸 다음 Secure Firewall 마이그레이션 툴에 새 구성 파일을 업로드합니다.

- **Partially Supported Configuration(**부분적으로 지원되는 구성**)** - 부분적으로만 마이그레이션할 수 있는 Fortinet 구성 요소에 대한 세부 정보입니다. 이러한 컨피그레이션 요소에는 고급 옵션이 있는 규칙 및 개체가 포함되는데, 이 경우 고급 옵션 없이 규칙 또는 개체를 마이그레이션할 수 있습니다. 이러한 라인을 검토하고 Management Center에서 고급 옵션이 지원되는지 확인한 다음, 지원되는 경우 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션을 완료한 후 해당 옵션을 수동으로 구성하도록 계획합니다.
- **Unsupported Configuration(**지원되지 않는 구성**)** - Secure Firewall 마이그레이션 툴이 해당 기능의 마이그레이션을 지원하지 않으므로 마이그레이션할 수 없는 Fortinet 구성 요소에 대한 세부 정보입니다. 이러한 라인을 검토하고 Management Center에서 각 기능이 지원되는지 확인한 다음, 지원되는 경우 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션을 완료한 후 해당 기능을 수동으로 구성하도록 계획합니다.
- **Ignored Configuration(**무시된 구성**)** - Management Center 또는 Secure Firewall 마이그레이션 툴에서 지원되지 않기 때문에 무시되는 Fortinet 구성 요소의 세부 정보입니다. Secure Firewall 마이그레이션 툴은 이러한 라인을 구문 분석하지 않습니다. 이러한 라인을 검토하고 Management Center에서 각 기능이 지원되는지 확인한 다음, 지원되는 경우 해당 기능을 수동으로 구성하도록 계획합니다.

Management Center 및 Threat Defense에서 지원되는 기능에 대한 자세한 내용은 Management Center 컨피그레이션 가이드를 참고하십시오.

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

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

다음에 수행할 작업

Fortinet Firewall 구성과 Threat Defense 인터페이스 매핑

Fortinet Firewall 구성과 Threat Defense 인터페이스 매핑

Threat Defense 디바이스에는 Fortinet 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 Threat Defense 디바이스의 인터페이스 목록을 검색합니다. 기본적으로 Secure Firewall 마이그레이션 툴은 인터페이스 ID에 따라 Fortinet의 인터페이스와 Threat Defense 디바이스를 매핑합니다.

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

- 대상 Threat Defense가 네이티브 유형인 경우:
  - Threat Defense에서 같거나 더 많은 수의 Fortinet 인터페이스 또는 PC(Port Channel) 데이터 인터페이스(Fortinet 구성의 관리 전용 및 하위 인터페이스 제외)를 사용해야 합니다. 이 수가 더 적은 경우 대상 Threat Defense에 필요한 인터페이스 유형을 추가합니다.

- 하위 인터페이스는 물리적 인터페이스 또는 포트 채널 매핑을 기반으로 Secure Firewall 마이그레이션 툴에서 생성됩니다.

- 대상 Threat Defense가 컨테이너 유형인 경우:
  - Threat Defense에서 같거나 더 많은 수의 Fortinet 인터페이스, 물리적 하위 인터페이스, 포트 채널 또는 포트 채널 하위 인터페이스(Fortinet 구성의 관리 전용 인터페이스 제외)를 사용해야 합니다. 이 수가 더 적은 경우 대상 Threat Defense에 필요한 인터페이스 유형을 추가합니다. 예를 들어, 대상 Threat Defense의 물리적 인터페이스 및 물리적 하위 인터페이스 수가 Fortinet 보다 100개 적을 경우 대상 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

Management Center에 연결하고 대상을 Threat Defense로 선택했는지 확인합니다. 자세한 내용은 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 33 페이지를 참고하십시오.

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

프로시저

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

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

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

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

다음에 수행할 작업

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

Fortinet 인터페이스를 보안 영역 및 에 매핑

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

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

Secure Firewall 마이그레이션 툴을 사용하면 보안 영역이 있는 인터페이스를 일대일로 매핑할 수 있습니다. 보안 영역이 인터페이스에 매핑된 경우 Management Center에서 허용하더라도 다른 인터페이스에 매핑될 수 없습니다. Management Center의 보안 영역에 대한 자세한 내용은 *Cisco Secure Firewall Management Center* 디바이스 구성 설명서에서 보안 영역 및 인터페이스 그룹를 참조하십시오.

프로시저

단계 **1** Management Center에 존재하는, 즉 구성 파일에서 보안 영역 유형 개체로 사용 가능하고 드롭다운 목록에서 사용 가능한 보안 영역 및 인터페이스 그룹에 인터페이스를 매핑하려면 다음과 같이 합니다.

a) **Security Zones(**보안 영역**)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.
b) **Interface Groups(**인터페이스 그룹**)** 열에서 해당 인터페이스의 인터페이스 그룹을 선택합니다.

단계 **2** Management Center에 존재하는 보안 영역에 인터페이스를 매핑하려면 **Security Zones(**보안 영역**)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.

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

보안 영역을 수동으로 매핑하려면 다음과 같이 합니다.

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

자동 생성을 통해 보안 영역을 매핑하려면 다음과 같이 합니다.

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

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

단계 **4** 모든 인터페이스를 적절한 보안 영역에 매핑했으면 **Next(**다음**)**를 클릭합니다.

최적화, 구성 검토 및 검증

마이그레이션된 Fortinet 구성을 Management Center로 푸시하기 전에 구성을 최적화하고 신중하게 검토하여 해당 구성이 올바르며 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 Management Center에 이미 있는 IPS(Intrusion Prevention System, 침입 방지 시스템) 정책 및 파일 정책을 가져와 마이그레이션 중인 액세스 제어 규칙에 연결할 수 있도록 합니다.

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

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

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

참고 기본적으로 인라인 그룹화 옵션은 활성화되어 있습니다.

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

Secure Firewall 마이그레이션 툴 **ACL** 최적화 개요

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

ACL 최적화는 다음 ACL 유형을 지원합니다.

- 중복 ACL - 두 ACL에 동일한 컨피그레이션 및 규칙 집합이 있는 경우 기본이 아닌 ACL을 제거해도 네트워크에 영향을 주지 않습니다. 예를 들어, 액세스 거부에 대해 정의된 규칙 없이 동일

한 네트워크에서 FTP 및 IP 트래픽을 허용하는 두 규칙이 있는 경우 첫 번째 규칙을 삭제할 수 있습니다.

- 섀도우 ACL - 첫 번째 ACL은 두 번째 ACL의 컨피그레이션을 완전히 섀도잉합니다. 두 규칙에 유사한 트래픽이 있는 경우, 두 번째 규칙은 액세스 목록의 뒷부분에 나타나므로 어떤 트래픽에도 적용되지 않습니다. 두 규칙이 트래픽에 대해 서로 다른 작업을 지정하는 경우, 섀도잉된 규칙을 이동하거나 규칙 중 하나를 편집하여 필요한 정책을 구현할 수 있습니다. 예를 들어 기본 규칙은 IP 트래픽을 거부할 수 있으며, 섀도잉된 규칙은 지정된 소스 또는 대상에 대한 FTP 트래픽을 허용할 수 있습니다.

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

참고 최적화는 ACP 규칙에 대해서만 Fortinet 에 사용할 수 있습니다.

- 비활성화된 ACL은 최적화 프로세스 중에 고려되지 않습니다.
- 소스 ACL은 해당 ACE(인라인 값)로 확장된 후 다음 매개변수에 대해 비교됩니다.
  - 소스 및 대상 영역
  - 소스 및 대상 네트워크
  - 소스 및 대상 포트

Download Report(보고서 다운로드**)**를 클릭하여 ACL 이름 및 Excel 파일로 표로 작성된 해당 이중 및 숨겨진 ACL을 검토합니다. 자세한 ACL 정보를 보려면 세부 **ACL** 정보 시트를 사용합니다. **Applications(**애플리케이션**)** 열에는 Fortinet 방화벽의 ACL과 연결된 애플리케이션이 나열됩니다.

프로시저

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

a) 테이블의 각 항목에 대해 매핑을 검토하고 올바른지 확인합니다.

마이그레이션된 액세스 정책 규칙은 ACL 이름을 접두사로 사용하고 ACL 정책 ID를 추가하므로 Fortinet 구성 파일에 다시 쉽게 매핑할 수 있습니다. 예를 들어 Fortinet ACL의 이름이 "inside_access"인 경우 ACL의 첫 번째 규칙(또는 ACE) 라인은 "inside_access_# 1"로 지정됩니다. TCP/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) 하나 이상의 액세스 제어 정책에 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.

d) 하나 이상의 액세스 제어 정책에 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.

e) 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 Management Center에 이미 구성된 시스템 로그 정책을 선택할 수 있습니다.

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

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

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

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

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

단계 **2** 다음 탭을 클릭하고 컨피그레이션 항목을 검토합니다.

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

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

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

마이그레이션하지 않도록 선택하는 모든 규칙은 테이블에서 회색으로 표시됩니다.

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

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

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

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

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

- 사전 공유 키를 업데이트 할 사이트 간 VPN 구성 항목을 선택합니다.
- 테이블을 편집 가능한 Excel 시트로 내보내려면 다운로드()를 클릭합니다.
- 각 VPN 설정에 대한 각 열에 사전 공유 키를 입력하고 파일을 저장합니다. IKE의 IKEv1 및 IKEv2 버전을 모두 포함하는 VPN 설정의 경우에는 두 값을 쉼표로 구분하여 열에 입력합니다.
- 업로드()를 클릭합니다. 마이그레이션 툴이 Excel의 항목을 읽고 VPN 구성의 해당 사전 공유 키 열에 자동으로 추가합니다.

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

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

단계 **7** **Remote Access VPN(**원격 액세스 **VPN)** 섹션에서는 원격 액세스 VPN에 해당하는 모든 개체가 Fortinet 에서 Management Center로 마이그레이션되며 다음과 같이 표시됩니다.

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

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

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

  소스 방화벽에서 올바른 Dap.xml 파일이 검색되는지 확인합니다. 구성 파일에 있는 dap.xml에 대해 검증이 수행됩니다. 검증에 필요한 모든 파일을 선택하고 업로드해야 합니다. 업데이트에 실패하면 완료되지 않은 것으로 표시되고 Secure Firewall 마이그레이션 툴이 검증을 진행하지 않습니다.
- **Address Pool(**주소 풀**)** - 여기에 표시된 모든 Ipv4 및 Ipv6 풀을 검토합니다.
- **Group-Policy(**그룹 정책**)** - 이 영역에서 사용자 프로파일, 관리 프로파일, 클라이언트 모듈 프로파일을 선택하거나 제거합니다. 이 영역에는 클라이언트 프로파일이 있는 그룹 정책, 관리 프로파일, 관리 모듈이 표시되며, 프로파일이 없는 그룹 정책이 표시됩니다. 프로파일이 AnyConnect file(AnyConnect 파일) 섹션에 추가된 경우 사전 선택된 것으로 표시됩니다. 사용자 프로파일, 관리 프로파일 및 클라이언트 모듈 프로파일을 선택하거나 제거할 수 있습니다.
- **Connection Profile(**연결 프로파일**)** - 여기에 표시된 모든 연결 프로파일/터널 그룹을 검토합니다.
- **Trustpoints(**트러스트 포인트**)** - Fortinet 방화벽 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.

  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 Fortinet 방화벽에서 사용할 수 있는 경우 **Override SAML(SAML** 재정의**)** 옵션에서 선택할 수 있습니다.

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

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

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

- 개체의 이름과 구성이 동일한 경우 Secure Firewall 마이그레이션 툴은 기존 개체를 재사용하고 Management Center에 새 개체를 생성하지 않습니다.

- 개체의 이름은 같지만 구성이 다른 경우 Secure Firewall 마이그레이션 툴이 개체 충돌을 보고합니다.

콘솔에서 검증 진행 상황을 볼 수 있습니다.

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

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

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

b) 탭을 클릭하고 개체를 검토합니다.

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

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

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

e) **Resolve(**해결**)**를 클릭합니다.

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

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

단계 **11** 검증이 완료되고 **Validation Status(**검증 상태**)** 대화 상자에 **Successfully Validated(**검증 성공**)** 메시지가 표시되면 마이그레이션된 컨피그레이션을 Management Center에 푸시, 45 페이지로 진행합니다.

마이그레이션된 컨피그레이션을 Management Center에 푸시

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

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

참고 Secure Firewall 마이그레이션 툴이 마이그레이션된 구성을 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 Fortinet 구성을 Management Center에 보냅니다.

Secure Firewall 마이그레이션 툴에 마이그레이션 진행 상황의 요약이 표시됩니다. 콘솔에서 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 언제라도 지원 페이지에서 TAC 케이스를 열 수 있습니다.

마이그레이션 후 보고서 검토 및 마이그레이션 완료

마이그레이션 후 보고서는 다양한 범주의 ACL 수, ACL 최적화 및 컨피그레이션 파일에서 수행된 최적화의 전체 보기에 대한 세부 정보를 제공합니다. 자세한 내용은 최적화, 구성 검토 및 검증, 40 페이지을 참조해 주십시오.

개체를 검토하고 확인합니다.

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

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

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

참고 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 Fortinet 구성이 어떻게 마이그레이션되었는지 파악합니다.

- **Migration Summary(**마이그레이션 요약**)** - Fortinet에서 Threat Defense 로 성공적으로 마이그레이션된 구성의 요약으로, Fortinet 인터페이스, Management Center 호스트 이름 및 도메인, 대상 Threat Defense 디바이스 (적용 가능한 경우) 및 성공적으로 마이그레이션된 구성 요소에 대한 정보가 포함됩니다.
- **Selective Policy Migration(**선택적 정책 마이그레이션**)** - 마이그레이션하도록 선택한 특정 Fortinet 기능에 대한 세부 정보를 Device Configuration Features(디바이스 구성 기능), Shared Configuration Features(공유 구성 기능), Optimization(최적화)의 세 범주에서 확인할 수 있습니다.
- **Fortinet Interface to Threat Defense Interface Mapping**(ASA FPS 포함 ASA FDM 매니지드 디바이스 인터페이스-Threat Defense 인터페이스 매핑) - 성공적으로 마이그레이션된 인터페이스와 Fortinet 구성의 인터페이스를 Threat Defense 디바이스의 인터페이스에 매핑한 방법에 대한 세부 정보입니다. 이러한 매핑이 예상과 일치하는지 확인합니다.

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

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

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

- **Object Conflict Handling(**개체 충돌 처리**)** - Management Center의 기존 개체와 충돌하는 것으로 확인된 Fortinet 개체에 대한 세부 정보입니다. 개체의 이름과 구성이 동일한 경우 Secure Firewall 마이그레이션 툴에서 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 Fortinet 규칙에 대한 세부 정보입니다. 이러한 라인을 검토하고 Management Center에서 고급 옵션이 지원되는지 확인한 다음 지원되는 경우 해당 옵션을 수동으로 구성합니다.

- **Unsupported Configuration(**지원되지 않는 구성**)** - Secure Firewall 마이그레이션 툴이 해당 기능의 마이그레이션을 지원하지 않으므로 마이그레이션할 수 없는 Fortinet 구성 요소에 대한 세부 정보입니다. 이러한 라인을 검토하여 각 기능이 Threat Defense 에서 지원되는지 확인합니다. 지원되는 경우 Management Center에서 해당 기능을 수동으로 구성합니다.

- **Expanded Access Control Policy Rules(**확장 액세스 제어 정책 규칙**)**- 마이그레이션 중에 단일 Fortinet 포인트 규칙에서 여러 Threat Defense 규칙으로 확장된 Fortinet 액세스 제어 정책 규칙에 대한 세부 정보입니다.

- **Actions Taken on Access Control Rules(**액세스 제어 규칙에 대해 수행된 작업**)**

  - **Access Rules You Chose Not to Migrate(**마이그레이션하지 않도록 선택한 액세스 규칙**)** - Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션하지 않도록 선택한 Fortinet 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 Fortinet 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 Threat Defense 에서 해당 기능이 지원되는지 확인합니다.

- **Access Control Rules that have File Policy Applied(**파일 정책이 적용된 액세스 제어 규칙**)** - 파일 정책이 적용된 모든 Fortinet 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 Threat Defense 에서 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 Fortinet 액세스 제어 규칙에 대한 세부 정보입니다. 로그 설정 값은 False(거짓), Event Viewer(이벤트 뷰어), Syslog(시스템 로그)입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.

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

참고
Review and Validate(검토 및 검증**)** 페이지에서 ACL에 IPS 또는 파일 정책을 적용해야 하는 경우 마이그레이션 전에 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.

Management Center 및 Threat Defense 에서 지원되는 기능에 대한 자세한 내용은 Management Center 컨피그레이션 가이드, 버전 6.2.3을 참고하십시오.

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

단계 **4** Management Center에서 다음과 같이 합니다.

a) Threat Defense 디바이스에 대해 마이그레이션된 컨피그레이션을 검토하여 다음을 비롯한 모든 예상 규칙 및 기타 컨피그레이션 항목이 마이그레이션되었는지 확인합니다.

- ACL(액세스 제어 목록)
- NAT(Network Address Translation) 규칙
- 포트 및 네트워크 개체
- 경로
- 인터페이스

b) 마이그레이션되지 않은 부분적으로 지원되는 항목 및 규칙, 지원되지 않는 항목 및 규칙, 무시된 항목 및 규칙, 비활성화된 항목 및 규칙을 모두 구성합니다.

이러한 항목 및 규칙에 대한 정보는 Management Center 컨피그레이션 가이드를 참고하십시오. 다음은 수동 구성이 필요한 컨피그레이션 항목의 예입니다.

- Threat Defense의 플랫폼 설정에 설명된 SSH 및 HTTPS 액세스를 포함한 플랫폼 설정
- 시스템 로그 구성에 설명된 시스템 로그 설정
- Threat Defense 라우팅 개요에 설명된 동적 라우팅

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

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

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

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

Secure Firewall 마이그레이션 툴 제거

모든 구성 요소는 Secure Firewall 마이그레이션 툴과 같은 폴더에 저장됩니다.

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: Fortinet를 Threat Defense 2100으로

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

- 유지 보수 기간 작업별
- 유지 보수 기간 작업

유지 보수 기간 작업별

시작하기 전에

Management Center를 설치하고 구축했는지 확인합니다. 자세한 내용은 해당 Firepower Management Center 하드웨어 설치 가이드 및 해당 Firepower Management Center 시작 가이드를 참고하십시오.

프로시저

단계 **1** 마이그레이션할 소스 Fortinet에서 전역 또는 VDOM별 컨피그레이션의 사본을 저장합니다.

단계 **2** 네트워크에 Firepower 2100 Series 디바이스를 구축하고 인터페이스를 연결한 다음 어플라이언스의 전원을 켭니다.

자세한 내용은 Management Center를 사용하는 2100 Series용 Cisco Threat Defense 빠른 시작 가이드를 참고하십시오.

단계 **3** Management Center에서 관리할 Firepower 2100 Series 디바이스를 등록합니다.

자세한 내용은 Management Center에 디바이스 추가를 참고하십시오.

단계 **4** (선택 사항) 소스 Fortinet 컨피그레이션에 집계 인터페이스가 있는 경우 대상 Firepower 2100 Series 디바이스에서 포트 채널(EtherChannels)을 생성합니다.

자세한 내용은 EtherChannel 및 이중 인터페이스 구성을 참고하십시오.

단계 **5** https://software.cisco.com/download/home/286306503/type에서 Secure Firewall 마이그레이션 툴의 최신 버전을 다운로드하여 실행합니다.

자세한 내용은 Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드, 27 페이지을 참고하십시오.

단계 **6** Secure Firewall 마이그레이션 툴을 실행하고 대상 매개변수를 지정할 때 Management Center에 등록한 Firepower 2100 Series 디바이스를 선택하십시오.

자세한 내용은 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 33 페이지을 참고하십시오.

단계 **7** Fortinet 인터페이스와 Threat Defense 인터페이스를 매핑합니다.

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

예를 들어 Fortinet의 집계 인터페이스를 Threat Defense 의 물리적 인터페이스에 매핑할 수 있습니다.

자세한 내용은 Fortinet Firewall 구성과 Threat Defense 인터페이스 매핑을 참고하십시오.

단계 **8** 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 Fortinet 논리적 인터페이스를 보안 영역에 수동으로 매핑합니다.

자세한 내용은 Fortinet 인터페이스를 보안 영역 및 에 매핑을 참고하십시오.

단계 **9** 이 가이드의 지침에 따라 마이그레이션할 컨피그레이션을 순차적으로 검토 및 검증한 다음 컨피그레이션을 Management Center로 푸시합니다.

단계 **10** 마이그레이션 후 보고서를 검토하고 Threat Defense 에 다른 컨피그레이션을 수동으로 설정하고 구축한 다음 마이그레이션을 완료합니다.

자세한 내용은 를 참고하십시오.

단계 **11** 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, 51 페이지의 내용을 참조하십시오.

프로시저

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

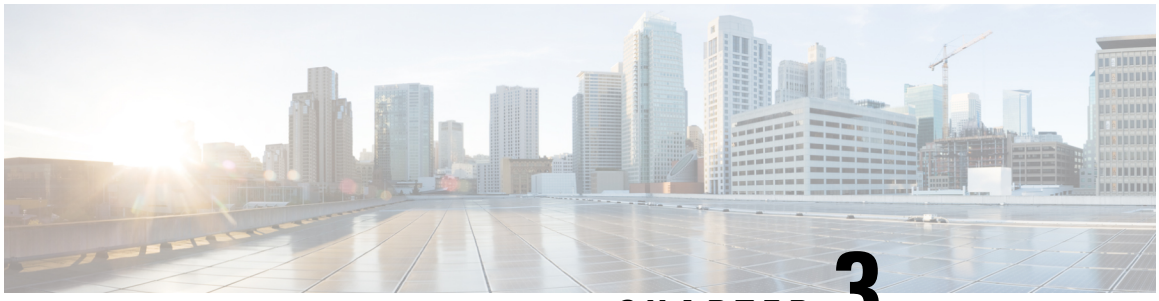
단계 **2** 주변 스위칭 인프라에서 Firepower 2100 Series 디바이스 인터페이스 IP 주소에 대한 기본 ping 테스트를 수행하여 액세스 가능한지 확인합니다.

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

단계 **4** Firepower 2100 Series 디바이스에 새 IP 주소를 할당하고 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 **5** Firepower 2100 디바이스에 대해 관리 Management Center 내에서 포괄적인 테스트 계획을 실행하고 로그를 모니터링합니다.



CHAPTER 3

Cisco Success Network - 텔레메트리 데이터

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 Fortinet 구성을 Management Center로 푸시하면 푸시 서비스가 해당 위치에서 텔레메트리 데이터 파일을 읽고 데이터가 클라우드에 성공적으로 업로드된 후 이 파일을 삭제합니다.

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

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

표 ***2:*** 제한된 텔레메트리

데이터 포인트	설명	예제 값
시간	텔레메트리 데이터가 수집되는 시간 및 날짜	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)
Target Management Version(대상 관리 버전)	Management Center의 대상 버전	6.5 이상

Cisco Success Network - 텔레메트리 데이터

데이터 포인트	설명	예제 값
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 ***3:*** 광범위한 텔레메트리

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

표 ***4:*** 소스 ***Fortinet*** 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	Fortinet
Source Device Serial Number(소스 디바이스 일련 번호)	Fortinet의 일련 번호	디바이스의 일련 번호(있는 경우)
Source Device Model Number(소스 디바이스 모델 번호)	Fortinet의 모델 번호	FGT80E
Source Device Version(소스 디바이스 버전)	Fortinet의 버전	6.0.6
Source Config Counts(소스 컨피그레이션 수)	소스 컨피그레이션의 총 라인 수	504

Cisco Success Network - 텔레메트리 데이터

데이터 포인트	설명	예제 값
방화벽 모드	Fortinet에 구성된 방화벽 모드(라우팅 또는 투명)	ROUTED
Context Mode(상황 모드)	Fortinet의 컨텍스트 모드. 단일 컨텍스트 또는 멀티 컨텍스트일 수 있습니다.	SINGLE
Fortinet 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)	Fortinet에 구성된 네트워크 개체의 수	34
Network Object Group Counts(네트워크 개체 그룹 수)	Fortinet의 네트워크 개체 그룹 수	6
Port Object Counts(포트 개체 수)	포트 개체의 수	85
Port Object Group Counts(포트 개체 그룹 수)	포트 개체 그룹의 수	37
Unsupported Access Rules Count(지원되지 않는 액세스 규칙 수)	지원되지 않는 액세스 규칙의 총 수	3
Unsupported NAT Rule Count(지원되지 않는 NAT 규칙 수)	지원되지 않는 NAT 액세스 규칙의 총 수	0
FQDN Based Access Rule Counts(FQDN 기반 액세스 규칙 수)	FQDN 기반 액세스 규칙의 수	7
Time range Based Access Rule Counts(시간 범위 기반 액세스 규칙 수)	시간 범위 기반 액세스 규칙의 수	1
SGT Based Access Rule Counts(SGT 기반 액세스 규칙 수)	SGT 기반 액세스 규칙의 수	0
툴에서 구문 분석할 수 없는 컨피그레이션 라인 요약		
Unparsed Config Count(구문 분석되지 않은 컨피그레이션 수)	파서에서 인식할 수 없는 컨피그레이션 라인의 수	68
Total Unparsed Access Rule Counts(구문 분석되지 않은 총 액세스 규칙 수)	구문 분석되지 않은 액세스 규칙의 총 수	3
추가 **Fortinet** 컨피그레이션 세부 정보**...**		

Cisco Success Network - 텔레메트리 데이터

데이터 포인트	설명	예제 값
Is RA VPN Configured(RA VPN 구성 여부)	RA VPN이 Fortinet에 구성되었는지 여부	거짓
Is S2S VPN Configured(S2S VPN 구성 여부)	사이트 간 VPN이 Fortinet에 구성되었는지 여부	거짓
Is BGP Configured(BGP 구성 여부)	BGP가 Fortinet에 구성되었는지 여부	거짓
Is OSPF Configured(OSPF 구성 여부)	OSPF가 Fortinet에 구성되었는지 여부	거짓
Local Users Counts(로컬 사용자 수)	구성된 로컬 사용자의 수	0

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

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

표 ***6:*** 마이그레이션 요약

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

Cisco Success Network - 텔레메트리 데이터

데이터 포인트	설명	예제 값
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
Security Zone Counts(보안 영역 수)	생성된 보안 영역의 수	3
Network Object Reused Counts(재사용 네트워크 개체 수)	재사용된 개체의 수	21
Network Object Rename Counts(이름 변경 네트워크 개체 수)	이름이 변경된 개체의 수	1
Port Object Reused Counts(재사용 포트 개체 수)	재사용된 포트 개체의 수	0
Port Object Rename Counts(이름 변경 포트 개체 수)	이름이 변경된 포트 개체의 수	0

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

데이터 포인트	설명	예제 값
Conversion Time(변환 시간)	Fortinet 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)	Fortinet 컨피그레이션의 Management Center로의 마이그레이션 상태	성공

Cisco Success Network - 텔레메트리 데이터

데이터 포인트	설명	예제 값
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 **Fortinet** 예시 파일

다음은 FortiNet 컨피그레이션을 Threat Defense로 마이그레이션하는 경우 텔레메트리 데이터 파일의 예입니다.

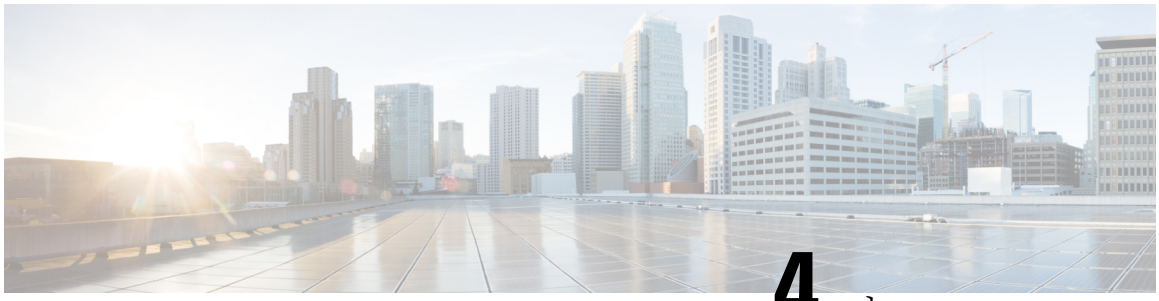

```
{
    "metadata": {
        "contentType": "application/json",
        "topic": "migrationtool.telemetry"
    },
    "payload": {
        "fortinet_config_stats": {
            "Ipv6_access_rule_counts": 3,
            "Ipv6_bgp_count": 0,
            "Ipv6_nat_rule_count": 3,
            "Ipv6_network_counts": 3,
            "Ipv6_static_route_counts": 6,
            "access_rules_counts": 62,
            "acl_counts": 62,
            "fqdn_based_access_rule_counts": 2,
            "nat_rule_counts": 27,
            "network_object_counts": 59,
            "network_object_group_counts": 11,
            "no_of_fqdn_based_objects": 9,
            "port_object_counts": 166,
            "port_object_group_counts": 37,
            "timerange_based_access_rule_counts": 0,
            "total_unparsed_access_rule_counts": 0,
            "tunneling_protocol_based_access_rule_counts": 0,
            "unparsed_config_count": 0,
            "unsupported_access_rules_count": 0,
            "unsupported_nat_rule_count": 0
        },
        "context_mode": "SINGLE",
        "error_description": null,
        "error_message": null,
        "firewall_mode": "ROUTED",
        "log_info_acl_count": 0,
        "migration_status": "SUCCESS",
        "migration_summary": {
            "access_control_policy": [
                [
                    {
                        "access_rule_counts": 62,
                        "apply_file_policy_rule_counts": 0,
                        "apply_ips_policy_rule_counts": 0,
                        "apply_log_rule_counts": 0,
                        "do_not_migrate_rule_counts": 0,
                        "enable_hit_count": false,
                        "expanded_acp_rule_counts": 1,
                        "name": "FTD-Mig-ACP-1602513965",
```

Cisco Success Network - 텔레메트리 데이터


```
                    "partially_migrated_acl_rule_counts": 0,
                    "time_based_acl_count": 0,
                    "total_acl_element_counts": 69,
                    "update_rule_action_counts": 0
                }
            ]
        ],
        "interface_counts": 20,
        "interface_group_counts": 0,
        "interface_group_manually_created_counts": 0,
        "ip_sla_monitor_count": 0,
        "nat_Policy": [
            [
                {
                    "NAT_rule_counts": 27,
                    "do_not_migrate_rule_counts": 0,
                    "name": "FTD-Mig-1602513959",
                    "partially_migrated_nat_rule_counts": 0
                }
            ]
        ],
        "network_object_rename_counts": 0,
        "network_object_reused_counts": 37,
        "object_group_counts": 2,
        "objects_counts": 35,
        "port_object_rename_counts": 0,
        "port_object_reused_counts": 10,
        "prefilter_control_policy": [
            [
                {
                    "do_not_migrate_rule_counts": 0,
                    "name": null,
                    "partially_migrated_acl_rule_counts": 0,
                    "prefilter_rule_counts": 0
                }
            ]
        ],
        "security_zone_counts": 19,
        "security_zone_manually_created_counts": 0,
        "static_routes_counts": 9,
        "sub_interface_counts": 20,
        "time_out": false
    },
    "migration_tool_version": "2.3",
    "mtu_info": {
        "interface_name": null,
        "mtu_value": null
    },
    "rule_change_acl_count": 0,
    "selective_policy": {
        "acl": true,
        "acl_policy": true,
        "application": false,
        "csm": true,
        "interface": true,
        "interface_groups": true,
        "migrate_tunneled_routes": false,
        "nat": true,
        "network_object": true,
        "policy_assignment": true,
        "populate_sz": false,
        "port_object": true,
        "routes": true,
        "security_zones": true,
```

Cisco Success Network - 텔레메트리 데이터


```
                "unreferenced": true
            },
            "source_config_counts": 0,
            "source_device_model_number": "FGT80E",
            "source_device_serial_number": null,
            "source_device_version": "6.0.6",
            "source_type": "FORTINET",
            "system_information": {
                "browser": "Chrome/85.0.4183.121",
                "operating_system": "Windows NT 10.0; Win64; x64"
            },
            "target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
            "target_device_version": "76",
            "target_management_type": "6.6.0 (build 56)",
            "target_management_version": "6.6.0 (build 56)",
            "template_version": "1.1",
            "time": "2020-10-12 20:16:15",
            "tool_analytics_data": {
                "objectsplit_100_count": 0
            },
            "tool_performance": {
                "config_push_time": 533,
                "conversion_time": 3,
                "migration_time": 1108
            }
        },
        "version": "1.0"
    }
```



4 장

마이그레이션 문제 해결

Secure Firewall 마이그레이션 툴 문제 해결

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

마이그레이션 프로세스가 실패하는 몇 가지 일반적인 시나리오는 다음과 같습니다.

- Fortinet 컨피그레이션 파일의 알 수 없는 문자 또는 잘못된 문자
- Fortinet 컨피그레이션 파일의 불완전하거나 누락 된 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 언제라도 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.

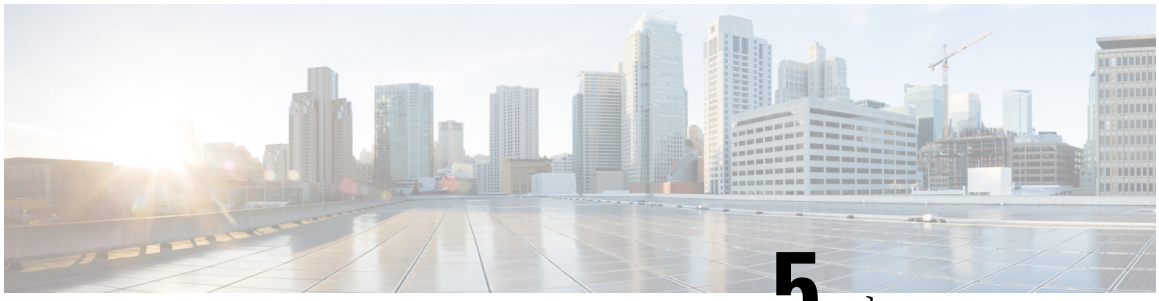
파일	위치
로그 파일	*<migration_tool_folder>*\logs
마이그레이션 전 보고서	*<migration_tool_folder>*\resources
마이그레이션 후 보고서	*<migration_tool_folder>*\resources
구문 분석되지 않은 파일	*<migration_tool_folder>*\resources

FortiNet 파일 업로드 실패 문제 해결

FortiNet 구성 파일이 업로드되지 않는 경우, 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.
- 마이그레이션 전 보고서(Pre-migration report) - Configuration Lines with Errors(오류가 있는 컨피그레이션 라인) 섹션을 검토하여 FortiNet 컨피그레이션 파일의 어떤 라인에서 실패가 발생했는지 확인합니다.
- Log file(로그 파일) - "error"라는 단어를 검색하여 실패의 원인을 확인합니다.
- Unparsed file(구문 분석되지 않은 파일) - 파일의 끝을 확인하여 성공적으로 구문 분석된 FortiNet 컨피그레이션 파일의 마지막으로 무시된 라인을 식별합니다.



5 장

Secure Firewall 마이그레이션 FAQ

Secure Firewall 마이그레이션 툴 FAQ(자주 묻는 질문)

Q. Secure Firewall 마이그레이션 툴 릴리스 3.0.1에서 지원되는 새로운 기능은 무엇입니까?

A. Secure Firewall 마이그레이션 툴 3.0.1은 이제 Fortinet에서의 마이그레이션을 위한 대상 디바이스로서만 Secure Firewall 3100 시리즈를 지원합니다.

Q. Secure Firewall 마이그레이션 툴 릴리스 3.0에서 지원되는 새로운 기능은 무엇입니까?

A. 릴리스 3.0에서는 다음 기능이 지원됩니다.

- 클라우드 제공 Firewall Management Center로 마이그레이션

Q. Secure Firewall 마이그레이션 툴 릴리스 2.5.2에서 지원되는 새로운 기능은 무엇입니까?

A. Fortinet에 대한 ACL 최적화.

Q. Secure Firewall 마이그레이션 툴 2.3에서 정책을 마이그레이션할 수 있는 소스 및 대상 플랫폼은 무엇입니까?

A. 현재 Secure Firewall 마이그레이션 툴은 지원되는 FortiNet 방화벽 플랫폼에서 위협 방어 플랫폼으로 정책을 마이그레이션할 수 있습니다. 자세한 내용은 마이그레이션에 지원되는 플랫폼을 참고하십시오.

Q. Secure Firewall 마이그레이션 툴 2.3에서 지원되는 새로운 기능은 무엇입니까?

A. Secure Firewall 마이그레이션 툴 2.3은 지원되는 FortiNet 플랫폼에서 위협 방어 플랫폼으로 정책을 마이그레이션할 수 있습니다.

Q. 지원되는 소스 디바이스 및 코드 버전은 무엇입니까?

A. Secure Firewall 마이그레이션 툴을 사용하여 FortiOS 5.0 이상을 실행하는 단일 또는 다중 VDOM Fortinet 방화벽에서 컨피그레이션을 마이그레이션할 수 있습니다. 디바이스 목록에 대한 자세한 내용은 마이그레이션에 지원되는 플랫폼을 참고하십시오.

Q. Fortinet 방화벽이 인터페이스 그룹을 지원합니까?

A. 아니요. Fortinet 방화벽은 위협 방어로의 변환을 위한 인터페이스 그룹을 지원하지 않습니다.

Q. Secure Firewall 마이그레이션 툴이 지원하는 마이그레이션 기능은 무엇입니까?

A. Secure Firewall 마이그레이션 툴은 위협 방어로의 L3/L4 Fortinet 구성 마이그레이션을 지원하며 다음 Fortinet 구성을 마이그레이션할 수 있습니다.

- 네트워크 개체 및 그룹(지원되지 않는 일부 개체 유형 제외)
- 서비스 개체(소스 및 대상에 대해 구성된 서비스 개체 제외)
- 서비스 개체 그룹(중첩된 서비스 개체 그룹 제외)

참고 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)
- 액세스 규칙
- NAT 규칙
- VIP 및 IP 풀을 사용하는 NAT(중앙 NAT는 지원되지 않음)
- 정적 경로, 마이그레이션되지 않은 ECMP 경로

- 물리적 인터페이스
- 하위 인터페이스
- 포트 채널
- 영역
- 시간 기반 개체

Q. NAT는 Management Center에서 지원되지 않는 FQDN을 사용합니다. 어떻게 해야 합니까?

A. NAT 필드의 FQDN-주소-개체 사용은 Secure Firewall 마이그레이션 툴 및 Management Center에서 지원되지 않습니다. 소스와 동일한 컨피그레이션을 복제하려면 마이그레이션 후 FQDN으로 매핑된 전체 IP 주소 집합을 수동으로 구성해야 합니다.

Q. 소스 방화벽에 대상보다 많은 인터페이스가 있는 경우 어떻게 해야 합니까?

A. 소스 방화벽에 대상보다 많은 인터페이스가 있는 경우 마이그레이션을 시작하기 전에 위협 방어에서 하위 인터페이스를 생성합니다.

Q. Secure Firewall 마이그레이션 툴은 집계 인터페이스(포트 채널)를 마이그레이션합니까?

A. Secure Firewall 마이그레이션 툴은 집계 인터페이스(포트 채널)를 마이그레이션하지 않습니다. 마이그레이션을 시작하기 전에 Management Center에서 포트 채널 인터페이스를 구성해야 합니다.

Q. 무시된 컨피그레이션 파일을 어떻게 해야 합니까?

A. Ignored(무시된) 컨피그레이션 파일에는 Fortinet에만 해당되며 Management Center와 무관한 행이 포함되어 있습니다. 따라서 무시됩니다. 무시된 컨피그레이션을 신중하게 검토해야 합니다. 무시된 섹션에 반영되는 모든 무관한 세부사항은 Management Center에서 수동으로 구성해야 합니다.

Q. 마이그레이션 전 보고서에 오류가 있습니다. 인터페이스를 무시하고 계속할 수 있습니까?

A. 인터페이스 없이 진행하도록 선택하는 경우 경로도 마이그레이션되지 않습니다.

Q. 구문 분석 실패의 일반적인 원인은 무엇입니까?

A. 인터페이스에 여러 IP 주소 또는 서브넷이 할당된 IP 주소(예: /32 또는 /128)가 있는 경우 구문 분석 실패가 발생합니다. 계속하려면 IP 주소를 수정하고 마이그레이션을 다시 시도해야 합니다.

Q. Fortinet 컨피그레이션을 내보내려면 어떻게 해야 합니까?

A. Fortinet 컨피그레이션을 FortiManager에서 디바이스를 관리하는 경우 Fortigate 디바이스 또는 FortiManager에서 추출하여 내보낼 수 있습니다. 자세한 내용은 Fortinet 방화벽에서 컨피그레이션 내보내기를 참고하십시오.

Q. Secure Firewall 마이그레이션 툴에 도입된 새로운 기능을 사용하는 데 적용되는 Management Center에 대한 종속성이 있습니까?

A. 예. 시간 기반 개체 기능은 대상 Management Center 6.6 이상에서 지원됩니다.