마이그레이션 준비

Firewall 마이그레이션 툴에 대한 지침 및 제한 사항

Fortinet 컨피그레이션

Fortinet 컨피그레이션은 다음 요구 사항을 충족해야 합니다.

- 마이그레이션에 지원되는 플랫폼, 7 페이지에 설명된 대로 마이그레이션에 지원되는 Fortinet 컨피그레이션.
- 마이그레이션에 지원되는 소프트웨어 버전, 8 페이지에 설명된 대로 마이그레이션에 지원되는 Fortinet 버전.

(선택 사항) 대상 **Threat Defense** 디바이스

Secure Firewall Management Center로 마이그레이션할 때 대상 threat defense 디바이스가 추가되거나 추가되지 않을 수 있습니다.

나중에 위협 방어 디바이스에 구축하도록 공유 정책을 management center로 마이그레이션할 수 있습니다. 디바이스별 정책을 위협 방어로 마이그레이션하려면 management center에 추가해야 합니다.

- 대상 위협 방어 디바이스는 다음 요구 사항을 충족해야 합니다.
  - Threat Defense 디바이스 관련 지침 및 제한 사항, 6 페이지에 설명된 대로 하드웨어 디바이스에 대한 지침을 따르는 디바이스
  - 마이그레이션에 지원되는 플랫폼, 7 페이지에 설명된 대로 마이그레이션 대상으로 지원되는 디바이스

- 마이그레이션에 지원되는 소프트웨어 버전, 8 페이지에 설명된 대로 마이그레이션에 지원되는 위협 방어 소프트웨어 버전
- management center에 등록된 위협 방어 디바이스

Management Center

- 마이그레이션에 지원되는 소프트웨어 버전, 8 페이지에 설명된 대로 마이그레이션에 지원되는 Mangement Center 소프트웨어 버전.
- 다음에 설명된 대로 Fortinet 인터페이스에서 마이그레이션하려는 모든 기능을 포함하는 위협 방어용 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
- 클라우드 제공 FMC에 설명된 대로 3.0부터는 클라우드 제공 management center으로의 마이그레이션이 가능합니다.

Firewall Migration Tool

- Firewall 마이그레이션 툴을 실행하는 데 사용하는 시스템이 Firewall 마이그레이션 툴의 플랫폼 요구 사항, 9 페이지에 설명된 요구 사항을 충족하는지 확인합니다.
- Firewall 마이그레이션 툴을 사용할 때는 다음 제한 내에서 일괄 푸시의 배치 크기를 구성할 수 있습니다.

컨피그레이션 항목	배치 크기 제한	기본값
개체	500	50
ACL	1,000	1,000
NAT	1,000	1,000
경로	1,000	1,000

참고 개체의 경우 API 배치 크기는 500개를 초과할 수 없습니다. Firewall 마이그레이션 툴은 값을 50으로 재설정하고 일괄 푸시를 진행합니다.

ACL, 경로 및 NAT 규칙의 경우 배치 크기는 각각 1000개를 초과할 수 없습니다. Firewall 마이그레이션 툴은 값을 1000으로 재설정하고 일괄 푸시를 진행합니다.

<migration_tool_folder>\app_config.txt에 있는 app_config 파일에서 배치 크기 제한을 구성할 수 있습니다.

참고 변경 사항을 적용하려면 애플리케이션을 재시작합니다.

- Firewall 마이그레이션 툴에서 컨피그레이션 푸시를 시작한 후에는 마이그레이션이 완료될 때까지 management center에서 컨피그레이션을 변경하거나 업데이트하지 마십시오.

FortiNet 방화벽 컨피그레이션 지침 및 제한 사항

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

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 파일

Fortinet 방화벽 컨피그레이션 파일을 수동으로 가져올 수 있습니다.

Firewall 마이그레이션 툴에 수동으로 가져오는 FortiNet 방화벽 컨피그레이션 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 컨피그레이션만 포함하고 있습니다.
- 구문 오류가 없습니다.
- 확장명이 .conf 또는 .txt인 파일 형식을 갖습니다.
- UTF-8 파일 인코딩을 사용합니다.
- 직접 코딩하거나 수동으로 변경하지 않았습니다. FortiNet 방화벽 컨피그레이션을 수정하는 경우 FortiNet 방화벽 디바이스에서 수정된 컨피그레이션 파일을 테스트하여 파일이 유효한 컨피그레이션인지 확인하는 것이 좋습니다.

Fortinet 방화벽 컨피그레이션 제한 사항

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

- 시스템 컨피그레이션은 마이그레이션되지 않습니다.

- Firewall 마이그레이션 툴은 50개가 넘는 인터페이스에 적용되는 단일 ACL 정책의 마이그레이션을 지원하지 않습니다. 50개 이상의 인터페이스에 적용된 ACL 정책은 수동으로 마이그레이션해야 합니다.
- 동적 라우팅 및 VPN과 같은 FortiNet 방화벽 컨피그레이션은 Threat Defense로 마이그레이션할 수 없습니다. 이러한 컨피그레이션은 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 FTD L3-인터페이스로 마이그레이션됩니다. 하드웨어 또는 소프트웨어 전환 멤버 인터페이스는 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 Firewall 마이그레이션 툴은 참조된 중첩 개체 그룹 또는 포트 그룹의 콘텐츠를 확장합니다.
- Firewall 마이그레이션 툴은 한 라인에 있는 소스 및 목적지 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

방화벽 마이그레이션 툴은 위협 방어 컨피그레이션에 대한 모범 사례를 사용합니다.

ACL 로그 옵션의 마이그레이션은 Threat Defense의 모범 사례를 따릅니다. 규칙에 대한 로그 옵션은 소스 FortiNet 방화벽 컨피그레이션에 따라 활성화되거나 비활성화됩니다. **deny(**거부**)** 작업이 있는 규칙의 경우 Firewall 마이그레이션 툴은 연결 시작 시 기록을 구성합니다. 작업이 **permit(**허용**)**인 경우 Firewall 마이그레이션 툴은 연결 종료 시 기록을 구성합니다.

지원되는 **Fortinet** 방화벽 컨피그레이션

Firewall 마이그레이션 툴은 다음 FortiNet 방화벽 컨피그레이션을 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.

- IPv4 및 IPv6 FQDN 개체 및 그룹
- IPv6 변환 지원(인터페이스, 정적 경로, 개체, ACL 및 NAT)
- 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)
- Firewall 마이그레이션 툴은 별도의 Threat Defense 디바이스로서 Fortinet 방화벽에서 개별 VDOM 마이그레이션을 지원합니다.
- 시간 기반 개체 - Firewall 마이그레이션 툴이 액세스 규칙을 참조하는 시간 기반 개체를 탐지하면 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 FTD로 표준 시간대 구성을 수동으로 마이그레이션해야 합니다.
- 시간 기반 개체는 비 FTD 플로우에 대해 지원되지 않으므로 비활성화됩니다.
- 시간 기반 개체는 FMC 버전 6.6 이상에서 지원됩니다.

부분적으로 지원되는 **Fortinet** 방화벽 컨피그레이션

Firewall 마이그레이션 툴은 다음 FortiNet 방화벽 컨피그레이션의 마이그레이션을 부분적으로 지원합니다. 이러한 컨피그레이션 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 마이그레이션 됩니다.

지원되지 않는 **Fortinet** 방화벽 컨피그레이션

Firewall 마이그레이션 툴은 다음 FortiNet 방화벽 컨피그레이션의 마이그레이션을 지원하지 않습니다. Management Center에서 이러한 컨피그레이션을 지원하는 경우 마이그레이션이 완료된 후 수동으로 컨피그레이션을 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
- Fortinet에서는 IPv4 및 IPv6(통합 정책)을 결합하는 정책을 구성할 수 있습니다.

참고 이 정책은 Firewall 마이그레이션 툴에서 지원되지 않습니다.

Threat Defense 디바이스 관련 지침 및 제한 사항

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

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

참고 디바이스(대상 위협 방어) 컨피그레이션 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 Firewall 마이그레이션 툴을 사용하여 마이그레이션되지 않습니다.

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

- 위협 방어 디바이스는 독립형 디바이스 또는 컨테이너 인스턴스일 수 있습니다. 클러스터 또는 고가용성 컨피그레이션의 일부가 아니어야 합니다.
  - 대상 위협 방어 디바이스가 컨테이너 인스턴스인 경우 최소한 와 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 위협 방어 디바이스에 필요한 인터페이스 유형을 추가해야 합니다.
    - 하위 인터페이스는 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.

마이그레이션에 지원되는 플랫폼

다음 Fortinet 및 위협 방어 플랫폼은 Firewall Migration Tool에 의한 마이그레이션에 지원됩니다. 지원되는 위협 방어 플랫폼에 대한 자세한 내용은 Cisco Secure Firewall 호환성 가이드를 참고하십시오.

지원되는 대상 **Threat Defense** 플랫폼

Firewall Migration Tool을 사용하여 소스 컨피그레이션을 위협 방어 플랫폼의 다음과 같은 독립형 또는 컨테이너 인스턴스로 마이그레이션할 수 있습니다.

- Firepower 1000 Series
- Firepower 2100 시리즈
- Firepower 4100 Series
- 다음을 포함하는 Firepower 9300 시리즈:
  - 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 위협 방어

Firewall Migration Tool은 Microsoft Azure 클라우드에 대한 threat defense virtual로의 마이그레이션을 지원합니다.

Azure의 threat defense virtual사전 요건 및 사전 스테이징에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense Virtual 시작하기 및 Azure를 참고하십시오.

Firewall Migration Tool은 AWS 클라우드에 대한 threat defense virtual로의 마이그레이션을 지원합니다.

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 Firewall Migration Tool에는 Microsoft Azure 또는 AWS 클라우드에서 management center에 연결하고 클라우드의 management center로 컨피그레이션을 마이그레이션하기 위한 네트워크 연결이 필요합니다.

참고 Firewall Migration Tool을 사용하여 마이그레이션을 성공적으로 수행하려면 먼저 management center또는 Threat Defense Virtual을 사전 스테이징하는 사전 요건을 충족해야 합니다.

마이그레이션에 지원되는 소프트웨어 버전

다음은 마이그레이션에 대해 지원되는 Fortinet 및 위협 방어 버전입니다.

지원되는 **Fortinet** 방화벽 버전

Firewall Migration Tool은 FortiNet 방화벽 OS 5.0 이상 버전을 실행하는 위협 방어로의 마이그레이션을 지원합니다.

소스 **Fortinet** 방화벽 컨피그레이션에 지원되는 **Management Center** 버전

FortiNet 방화벽의 경우 Firewall Migration Tool은 6.2.3.3 이상 버전을 실행하는 management center에서 관리되는 위협 방어 디바이스로의 마이그레이션을 지원합니다.

참고 6.7 위협 방어 디바이스로의 마이그레이션은 현재 지원되지 않습니다. 따라서 디바이스가 management center 액세스용 데이터 인터페이스로 구성된 경우 마이그레이션이 실패할 수 있습니다.

지원되는 **Threat Defense** 버전

Firewall Migration Tool에서는 위협 방어 6.5 이상 버전을 실행하는 디바이스로의 마이그레이션을 권장합니다.

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

Firewall 마이그레이션 툴의 플랫폼 요구 사항

Firewall 마이그레이션 툴에는 다음과 같은 인프라 및 플랫폼 요구 사항이 있습니다.

- 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