마이그레이션 정보

Firewall 마이그레이션 툴 소개

설명서

이 문서 *Firewall* 마이그레이션 툴로 *Fortinet*을 위협 방어로 마이그레이션에 나온 모든 정보는 최신 버전의 Firewall 마이그레이션 툴을 가리킵니다. 최신 버전의 Firewall 마이그레이션 툴을 다운로드하려면 Cisco.com에서 Firewall 마이그레이션 툴 다운로드에 나온 지침을 따르십시오.

2.3부터 Firewall 마이그레이션 툴은 Fortinet 방화벽 컨피그레이션을 위협 방어로 마이그레이션하는 것을 지원합니다. Firewall 마이그레이션 툴은 FortiNet 컨피그레이션을 위협 방어로 마이그레이션하는 데 사용됩니다.

Firewall Migration Tool 섹션

Firewall Migration Tool는 지원되는 Fortinet 컨피그레이션을 지원되는 위협 방어 플랫폼으로 변환합니다. Firewall 마이그레이션 툴을 사용하면 지원되는 Fortinet 기능 및 정책의 마이그레이션을 자동화할 수 있습니다. 지원되지 않는 기능을 수동으로 마이그레이션해야 할 수 있습니다.

Firewall 마이그레이션 툴은 Fortinet 정보를 수집하고 구문 분석한 다음 마지막으로 management center에 푸시합니다. 구문 분석 단계에서 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 컨피그레이션 라인. 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 위협 방어 인터페이스에 매핑하고, 애플리케이션을 매핑하고, 보안 영역을 매핑하고, 컨피그레이션을 검토하고 검증할 수 있습니다. 그런 다음 컨피그레이션을 대상 디바이스로 마이그레이션할 수 있습니다.

Firewall 마이그레이션 툴은 진행 상황을 저장하고 마이그레이션 프로세스 중에 두 단계로 마이그레이션을 다시 시작할 수 있도록 합니다.

- **Fortinet** 컨피그레이션 파일의 구문 분석 완료 후

참고 구문 분석 오류가 있거나 구문 분석 전에 종료하는 경우 Firewall 마이그레이션 툴에서 처음부터 작업을 다시 실행해야 합니다.

- **Optimize, Review and Validate(**최적화**,** 검토 및 검증**)** 페이지

참고 이 단계에서 Firewall 마이그레이션 툴을 종료하고 다시 실행하면 **Optimize, Review and Validate(**최적화**,** 검토 및 검증**)** 페이지가 표시됩니다.

콘솔

Firewall 마이그레이션 툴을 실행하면 콘솔이 열립니다. 이 콘솔에서는 Firewall 마이그레이션 툴의 각 단계 진행 상황에 대한 자세한 정보를 제공합니다. 콘솔의 내용은 Firewall 마이그레이션 툴 로그 파일에도 작성됩니다.

Firewall 마이그레이션 툴이 열려 실행 중인 동안에는 콘솔이 열려 있어야 합니다.

중요 웹 인터페이스가 실행 중인 브라우저를 닫아 Firewall 마이그레이션 툴을 종료하면 콘솔은 백그라운드에서 계속 실행됩니다. Firewall 마이그레이션 툴을 완전히 종료하려면 키보드에서 Command 키 + C를 눌러 콘솔을 종료합니다.

로그

Firewall 마이그레이션 툴은 각 마이그레이션의 로그를 생성합니다. 로그에는 마이그레이션의 각 단계에서 어떤 일이 발생하는지에 대한 세부 정보가 포함되며, 마이그레이션이 실패 할 경우 원인을 파악하는 데 도움이 될 수 있습니다.

Firewall 마이그레이션 툴의 로그 파일은 다음 위치에서 찾을 수 있습니다.
`<migration_tool_folder>\logs`

리소스

Firewall 마이그레이션 툴은 마이그레이션 전 보고서, 마이그레이션 후 보고서, Fortinet 컨피그레이션 및 `resources` 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`

Firewall 마이그레이션 툴에서 검색

Optimize, Review and Validate(최적화**,** 검토 및 검증**)** 페이지의 항목과 같이 Firewall 마이그레이션 툴에 표시되는 테이블의 항목을 검색할 수 있습니다.

테이블의 열 또는 행에서 항목을 검색하려면 테이블 위의 검색( )를 클릭하고 필드에 검색어를 입력합니다. Firewall 마이그레이션 툴이 테이블 행을 필터링하고 검색어가 포함된 행만 표시합니다.

단일 열에서 항목을 검색하려면 열 제목에 있는 **Search(**검색**)** 필드에 검색어를 입력합니다. Firewall 마이그레이션 툴이 테이블 행을 필터링하고 검색어와 일치하는 행만 표시합니다.

포트

Firewall 마이그레이션 툴은 포트 8321-8331 및 포트 8888의 12개 포트 중 하나에서 실행할 때 텔레메트리를 지원합니다. 기본적으로 Firewall 마이그레이션 툴은 포트 8888을 사용합니다. 포트를 변경하려면 `app_config` 파일에서 포트 정보를 업데이트합니다. 업데이트 후 포트 변경 사항을 적용하려면 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 Firewall 마이그레이션 툴에 다른 포트를 사용할 수 없습니다.

Firewall 마이그레이션 툴의 이력

버전	지원 기능
3.0	Firewall 마이그레이션 툴 3.0은 다음을 지원합니다. • 대상 management center이 7.2 이상인 경우 Fortinet에서 클라우드 제공 management center으로의 마이그레이션이 지원됩니다.

버전	지원 기능
2.5.2	현재 Firewall 마이크레이션 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 컨피그레이션 및 규칙 집합이 있는 경우 기본이 아닌 ACL을 제거해도 네트워크에 영향을 주지 않습니다. • 새도우 ACL - 첫 번째 ACL은 두 번째 ACL의 컨피그레이션을 완전히 새도잉합니다. 참고 최적화는 Fortinet ACP 규칙 작업에만 사용할 수 있습니다. Firewall 마이그레이션 툴 2.5.2는 대상 management center이 7.1 이상인 경우 BGP(Border Gateway Protocol) 및 동적 경로 개체 마이그레이션을 지원합니다.
2.3	• Fortinet 방화벽 OS 버전 5.0 이상 지원 • Firewall 마이그레이션 툴을 사용하여 다음과 같은 FortiNet 컨피그레이션 요소를 위협 방어로 마이그레이션할 수 있습니다. • Interfaces • 영역 • 고정 경로 • 네트워크 개체 및 그룹 • 서비스 개체 및 그룹 • Access Control List • NAT 종속 개체 (IP 풀, 가상 IP) • NAT 규칙 • VDOM • 시간 기반 개체 - Firewall 마이그레이션 툴이 액세스 규칙을 참조하는 시간 기반 개체를 탐지하면 Firewall 마이그레이션 툴은 시간 기반 개체를 마이그레이션하고 개별 액세스 규칙과 매핑합니다. Review and Validate Configuration(컨피그레이션 검토 및 검증) 페이지의 규칙에 따라 개체를 검증합니다. 참고 시간 기반 개체는 management center 6.6 이상 버전에서 지원됩니다.

Firewall 마이그레이션 툴 라이선싱

Firewall 마이그레이션 툴 애플리케이션은 무료이며 라이선스가 필요하지 않습니다. 그러나 위협 방어를 성공적으로 등록하고 정책을 구축하려면 관련 위협 방어 기능에 필요한 라이선스가 management center에 있어야 합니다.

면책조항

Firewall 마이그레이션 툴("툴")은 지원되는 서드파티 제품 컨피그레이션을 유효하게 라이선스가 부여되고 지원되는 플랫폼에 대한 Cisco Secure Firewall Threat Defense("Threat Defense") 컨피그레이션으로 쉽게 변환할 수 있도록 설계되었습니다. 툴에서 생성한 보안 정책 및 컨피그레이션은 변환을 완료한 후 수동 컨피그레이션이 필요할 수 있습니다. 컨피그레이션을 검토하고 테스트하여 구현 전에 정확하고 완전한지 확인할 책임은 전적으로 귀하에게 있습니다. 이 툴은 "있는 그대로" 제공되며, Cisco는 이 툴이 귀하의 비즈니스 요구 사항을 충족하거나 귀하의 기존 시스템에서 작동할 것임을 진술하거나 보증하지 않습니다.