Threat Defense 2100으로 Fortinet 마이그레이션 - 예

Firewall Threat Defense 2100으로 마이그레이션 - 예

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

유지 보수 기간 전에 다음 작업 수행

시작하기 전에

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

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 시리즈용 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 Firewall Migration Tool의 최신 버전을 다운로드하여 실행합니다.

자세한 내용은 Cisco.com에서 Firewall 마이그레이션 툴 다운로드를 참고하십시오.

단계 **6** Firewall Migration Tool을 실행하고 대상 매개변수를 지정할 때 management center에 등록한 Firepower 2100 Series 디바이스를 선택하십시오.

자세한 내용은 Firewall 마이그레이션 툴의 대상 매개변수 지정를 참고하십시오.

단계 **7** Fortinet 인터페이스와 threat defense 인터페이스를 매핑합니다.

참고 Firewall Migration Tool를 사용하면 Fortinet 인터페이스 유형을 threat defense 인터페이스 유형에 매핑할 수 있습니다.

예를 들어 Fortinet의 집계 인터페이스를 threat defense의 물리적 인터페이스에 매핑할 수 있습니다.

자세한 내용은 Threat Defense 인터페이스와 Fortinet 인터페이스 매핑을 참고하십시오.

단계 **8** 논리적 영역을 보안 영역에 매핑하는 동안 **Auto-Create(**자동 생성**)**를 클릭하여 Firewall Migration Tool이 새 보안 영역을 생성하도록 허용합니다. 기존 보안 영역을 사용하려면 Fortinet 논리적 인터페이스를 보안 영역에 수동으로 매핑합니다.

자세한 내용은 보안 영역 및 인터페이스 그룹에 ASA Fortinet 논리적 인터페이스 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 defense에 다른 컨피그레이션을 수동으로 설정하고 구축한 다음 마이그레이션을 완료합니다.

자세한 내용은 마이그레이션 후 보고서 검토 및 마이그레이션 완료를 참고하십시오.

단계 **11** 마이그레이션을 계획하는 동안 생성한 테스트 계획을 사용하여 Firepower 2100 Series 디바이스를 테스트합니다.

유지 보수 기간 동안 다음 작업 수행

시작하기 전에

유지 보수 기간 전에 수행해야 하는 모든 작업을 완료했는지 확인합니다. 유지 보수 기간 전에 다음 작업 수행, 1 페이지의 내용을 참조하십시오.

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.

Threat Defense 2100으로 Fortinet 마이그레이션 - 예

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 디바이스에 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.

Threat Defense 2100으로 Fortinet 마이그레이션 - 예