원활한 전환: Palo Alto Firewall에서 Cisco FTD로 마이그레이션

목차

소개

이 문서에서는 FMT 버전 6.0을 사용하여 Palo Alto 방화벽에서 Cisco FTD 시스템으로 전환하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Palo Alto 방화벽에서 현재 실행 중인 컨피그레이션을 XML 형식(*.xml)으로 내보냅니다.
- Palo Alto Firewall CLI에 액세스하고 show routing route 명령을 실행한 다음 출력을 텍스트 파일(*.txt)로 저장합니다.
- 컨피그레이션 파일(*.xml)과 라우팅 출력 파일(*.txt)을 단일 ZIP 아카이브(*.zip)로 압축합니다.

사용되는 구성 요소

이 문서의 정보는 Palo Alto Firewall 버전 8.4.x 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Firepower 마이그레이션 도구(FMT)

FMT는 엔지니어링 팀이 기존 벤더 방화벽을 Cisco NGFW(Next-Generation Firewall)/FTD(Firepower Threat Defense)로 전환하는 데 도움이 됩니다. Cisco 웹 사이트에서 다운로드한 FMT의 최신 버전을 작동해야 합니다.

마이그레이션 지침

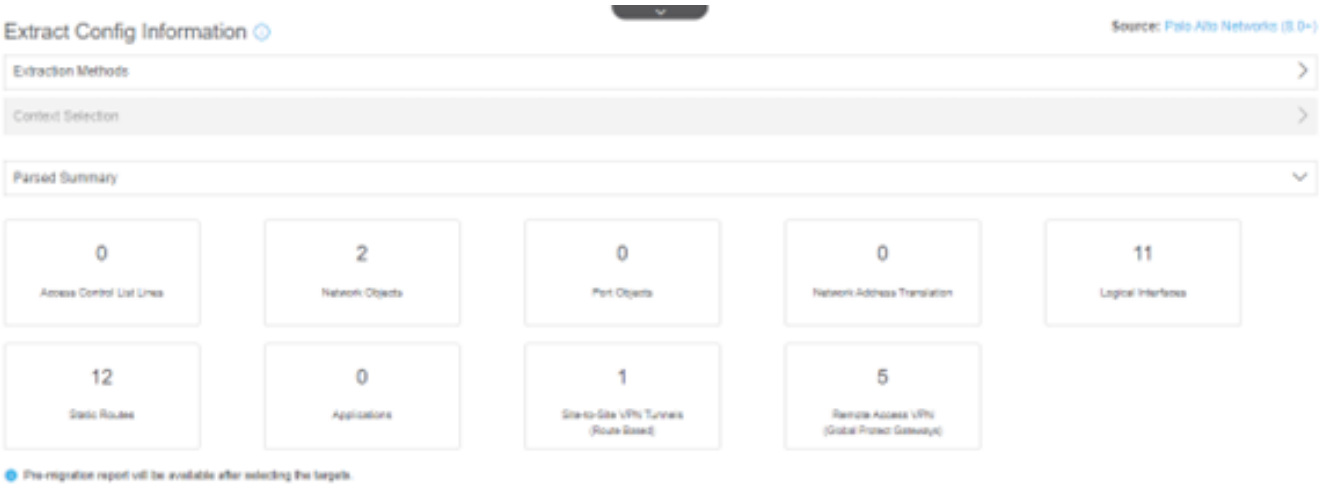
1. 마이그레이션 전 체크리스트

- 마이그레이션 프로세스를 시작하기 전에 FTD가 FMC에 추가되었는지 확인합니다.
- 관리 권한이 있는 새 사용자 계정이 FMC에 생성되었습니다.
- 내보낸 Palo Alto 실행 configuration file.xml은 확장자가 .zip으로 압축되어야 합니다.
- NGFW/FTD는 물리적 또는 하위 인터페이스 수가 같아야 하며, 포트 채널은 Palo Alto 방화벽 인터페이스와 같아야 합니다.

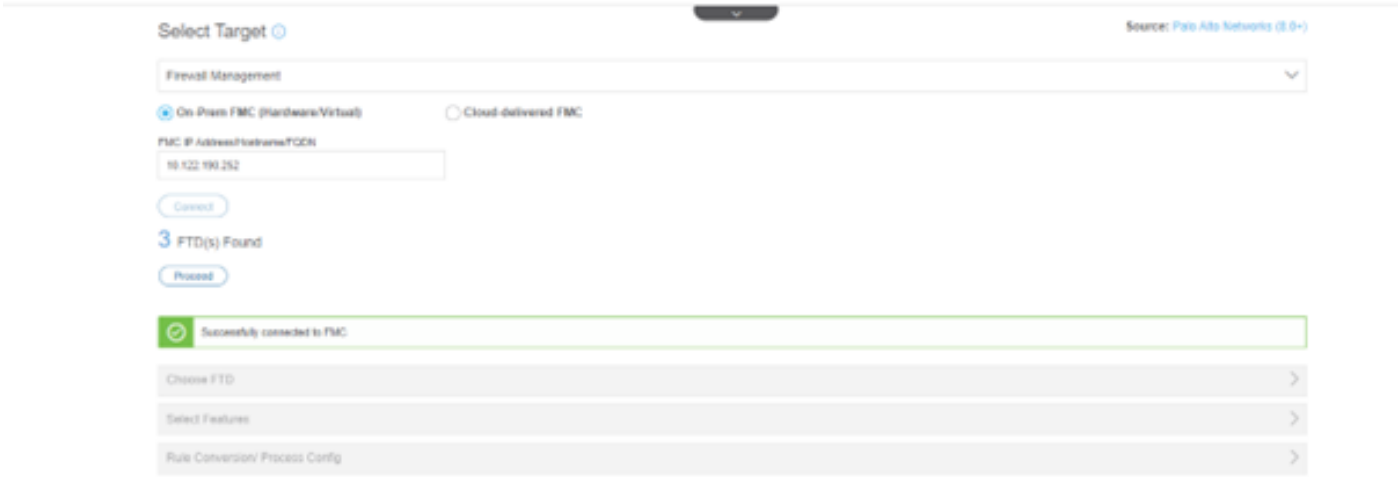
2. 마이그레이션 툴 사용

- FMT tool.exe를 다운로드하고 관리자로 실행합니다.
- FMT에서 로그인하려면 CEC ID 또는 cisco 사용자 계정이 필요합니다.
- Post Successful Login(로그인 성공 후 게시) 툴은 사용자가 방화벽 공급업체를 선택하고 해당 *.zip 파일을 업로드할 수 있는 대시보드를 표시합니다. 다음 이미지를 참조하십시오.

- 마이그레이션을 진행하기 전에 오른쪽에서 제공되는 지침을 주의 깊게 검토하십시오.
- 시작할 준비가 되면 마이그레이션 시작을 클릭합니다.
- Palo Alto 방화벽의 컨피그레이션 설정이 포함된 저장된 *.zip 파일을 업로드합니다.
- 컨피그레이션 파일이 업로드되면 구문 분석된 콘텐츠의 요약을 확인하고 next(다음)를 클릭할 수 있습니다. 다음 이미지를 참조하십시오.



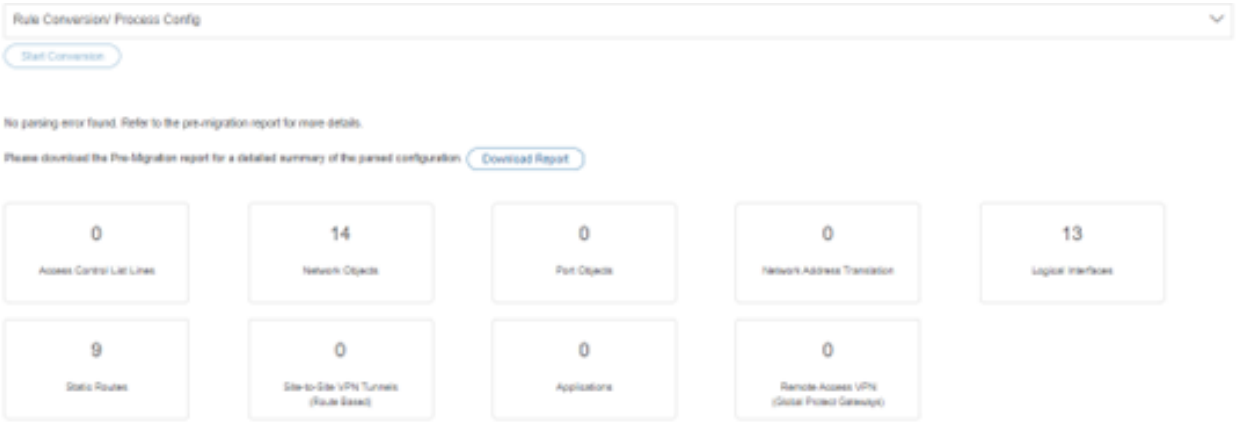
- FMC의 IP 주소를 입력하고 로그인합니다.
- 이 툴은 FMC에 등록된 활성 FTD를 검색합니다.
- 마이그레이션할 FTD를 선택하고 다음 이미지에 표시된 대로 Proceed(진행)를 클릭합니다.



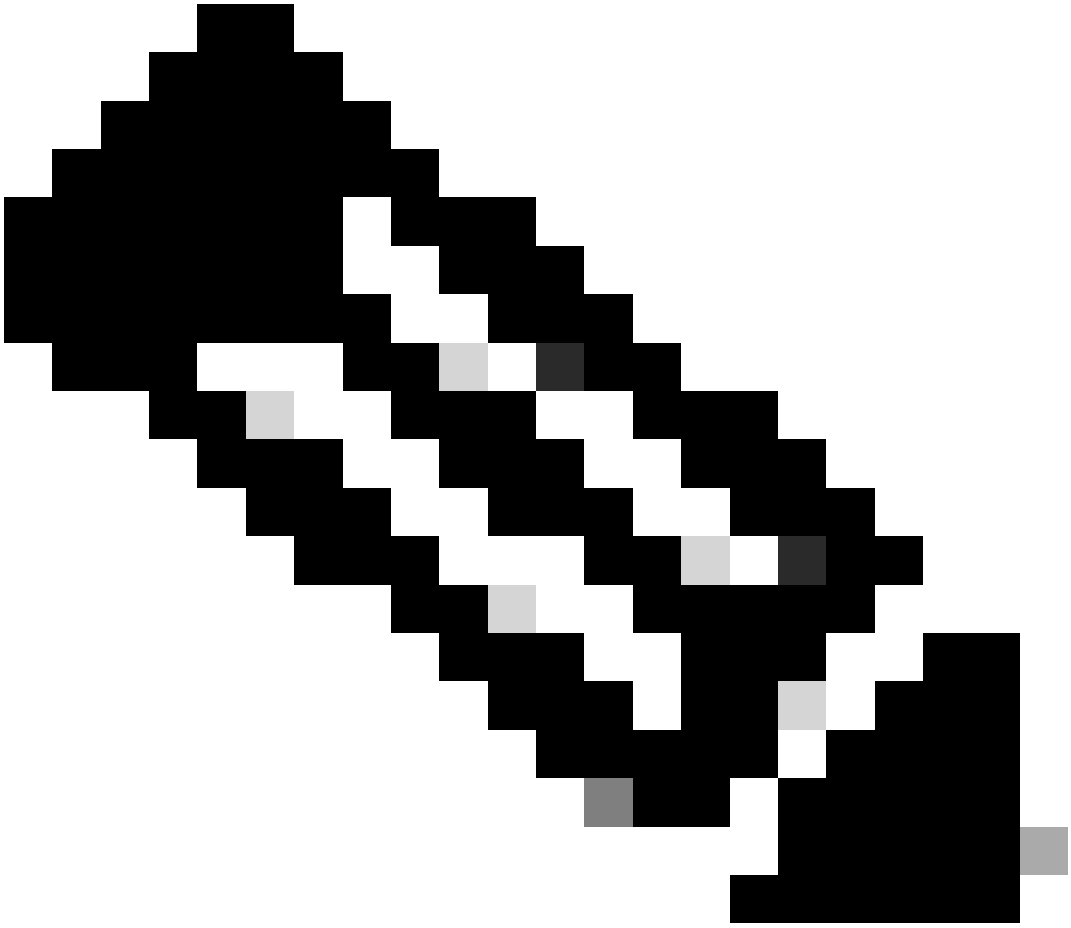
- 고객의 요구 사항에 따라 마이그레이션할 특정 기능을 선택합니다. Palo Alto 방화벽은 FTD와 다른 기능을 갖추고 있습니다.
- Proceed(진행)를 클릭하고 다음 이미지에서 참조를 참조합니다.

- 선택한 내용에 따라 FMT가 변환을 실행합니다. Pre-Migration Report(마이그레이션 전 보고

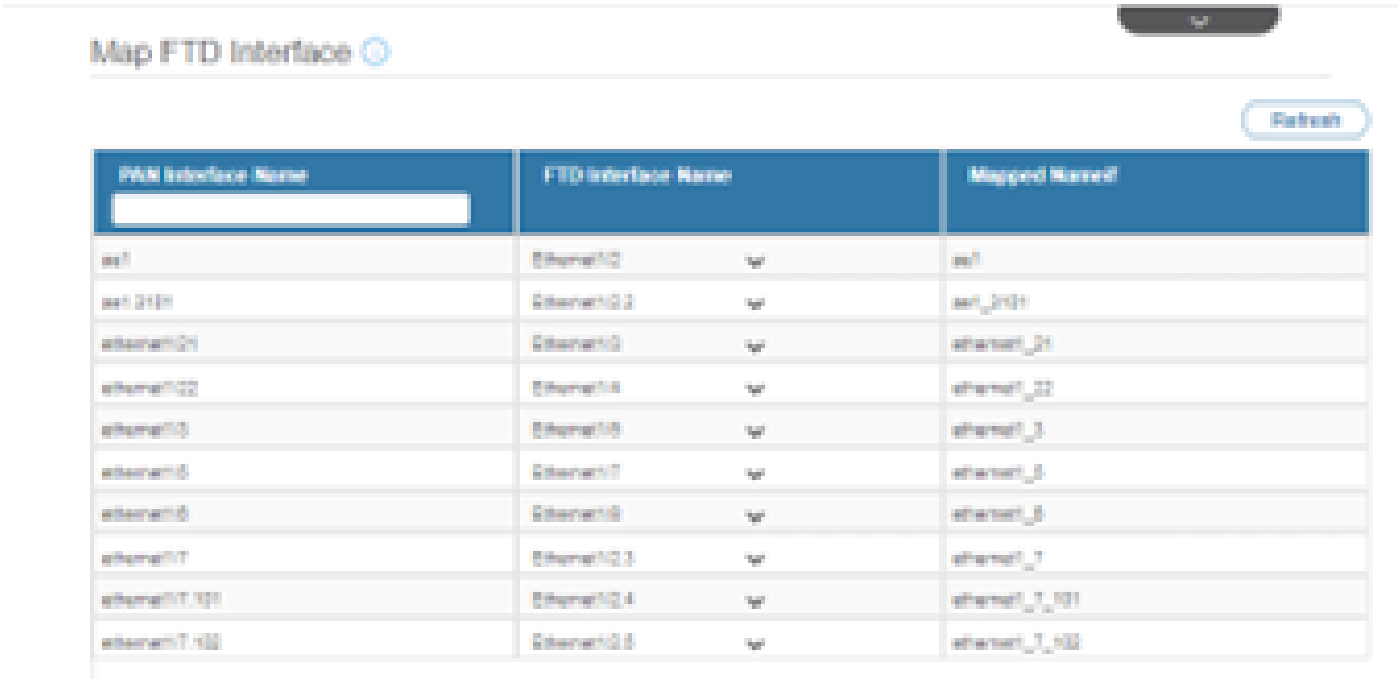
서)에서 변경 사항을 검토한 다음 Proceed(진행)를 클릭합니다. 지침은 다음 이미지를 참조하십시오.



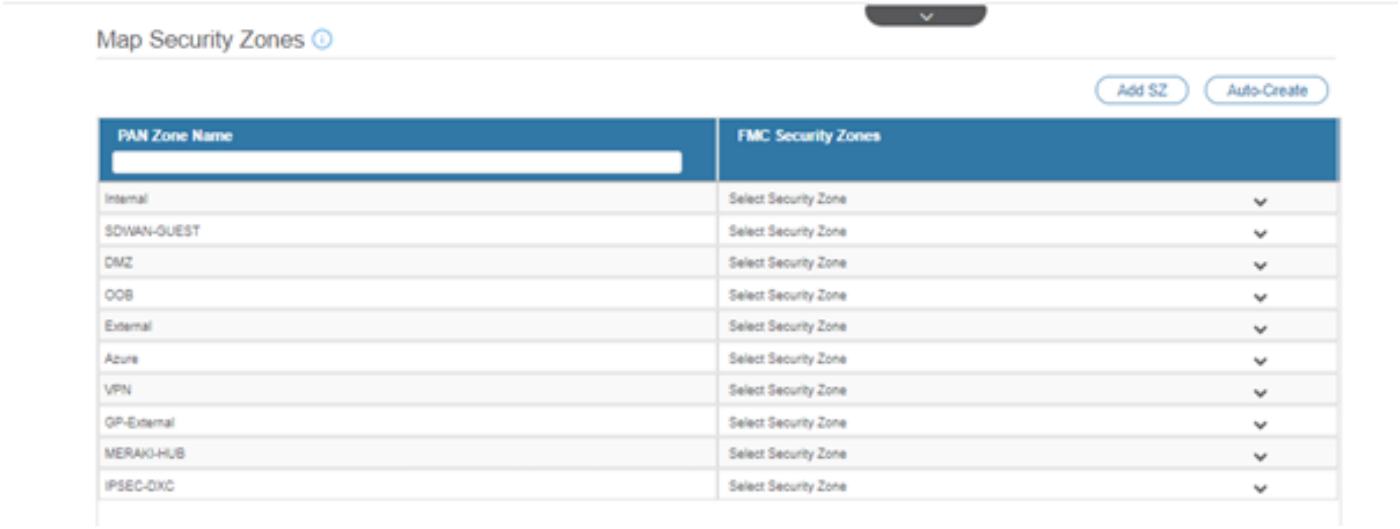
- Palo Alto 방화벽의 인터페이스를 FTD의 인터페이스에 매핑합니다. 자세한 내용은 다음 이미지를 참조하십시오.



참고: NGFW/FTD는 물리적 또는 하위 인터페이스 수가 같아야 하며, 하위 인터페이스를 포함한 Palo Alto 방화벽 인터페이스와 포트 채널이 같아야 합니다.



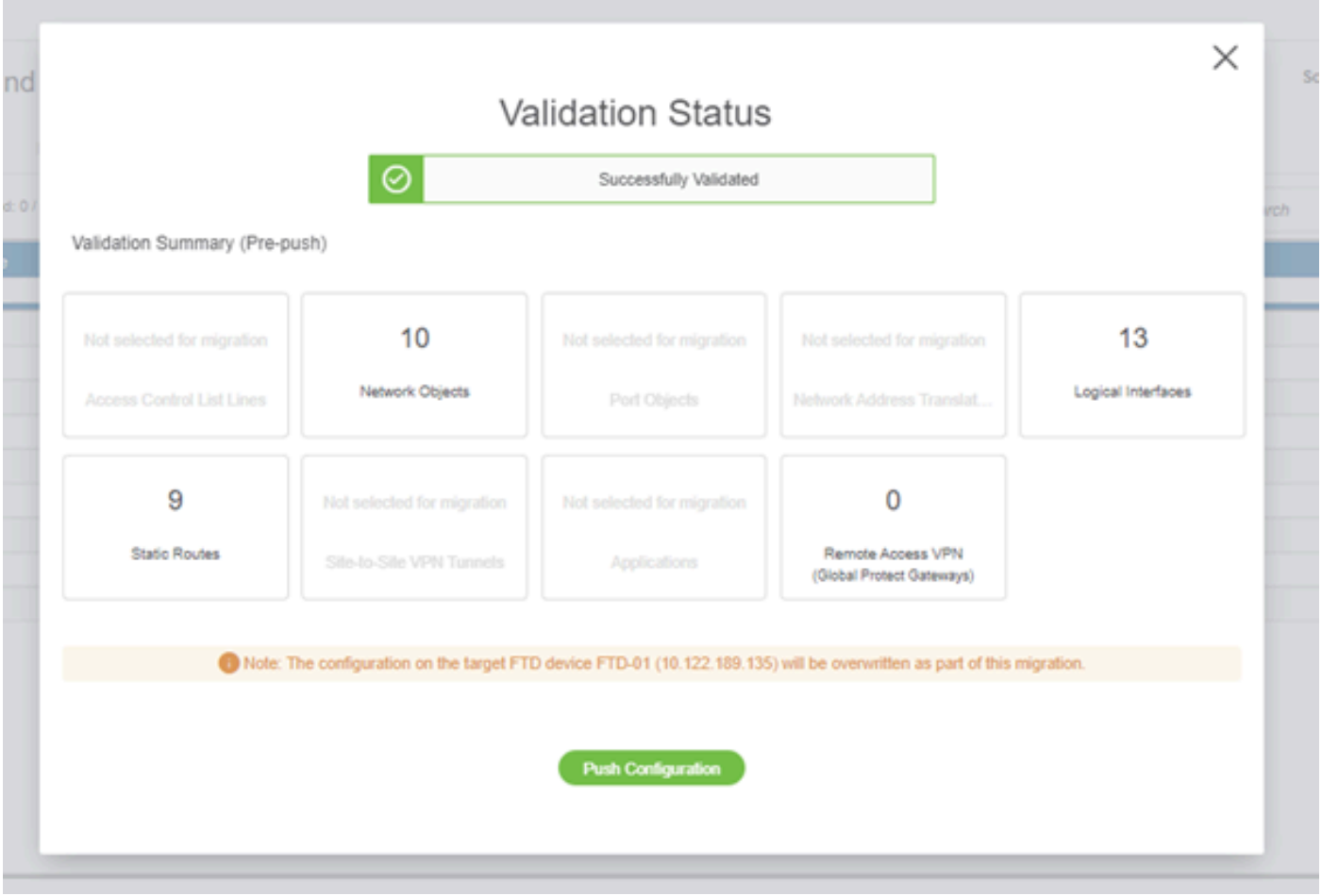
- 영역에 대한 매핑을 결정합니다. 이 매핑은 수동으로 수행하거나 자동 생성 기능을 사용하여 수행할 수 있습니다. 시각화는 다음 이미지를 참조하십시오.



- 애플리케이션 차단 프로필을 할당합니다. 애플리케이션 매핑이 없는 랩 디바이스이므로 기본 설정을 계속 사용할 수 있습니다. Next(다음)를 클릭하고 제공된 이미지를 참조하십시오.

- 필요에 따라 ACL, 객체, 인터페이스 및 경로를 최적화합니다. 최소 컨피그레이션의 랩 설정이므로 기본 옵션을 계속 진행할 수 있습니다. 그런 다음 다음 이미지를 참조하여 Validate를 클릭합니다.

- 검증에 성공한 후 컨피그레이션을 대상 FTD에 구축할 준비가 되었습니다. 자세한 내용은 다음 이미지를 참조하십시오.



- Push Configuration(푸시 컨피그레이션)은 마이그레이션된 컨피그레이션을 FMC에 저장하고 FTD에 자동으로 구축됩니다.
- 마이그레이션 중에 문제가 발생할 경우 언제든지 TAC 케이스를 열어 추가 지원을 요청하십시오.

3. 사후 - 마이그레이션 검증

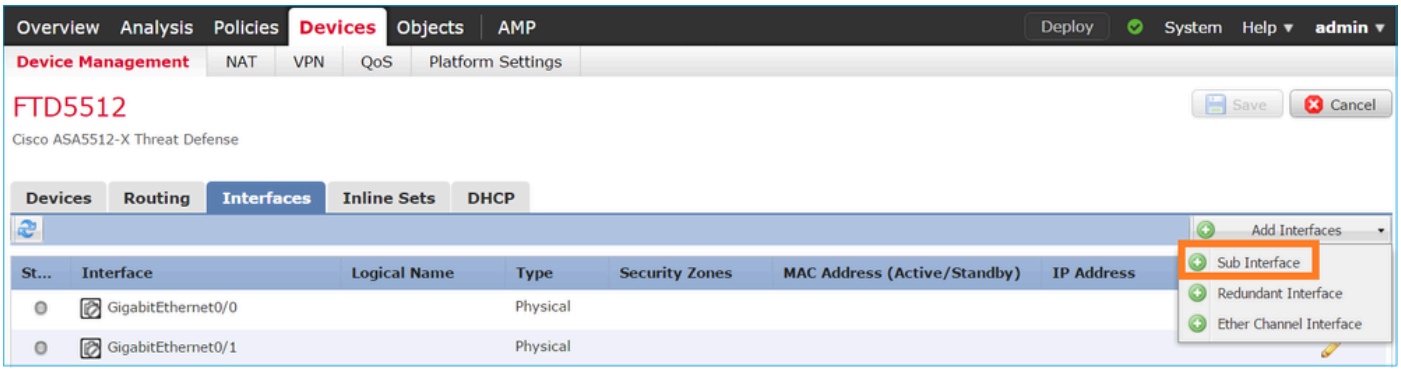
- FTD 및 FMC의 컨피그레이션을 검증합니다.
- 디바이스 ACL, 정책, 연결 및 기타 고급 기능 테스트
- 변경 사항을 수행하기 전에 롤백 지점을 생성합니다.
- 프로덕션 환경에서 Go-Live하기 전에 랩 환경에서 마이그레이션 테스트

알려진 문제

1. FTD에 인터페이스가 없습니다.

- Palo Alto CLI에 로그인하고 show interface all을 실행합니다. FTD의 인터페이스 수가 같거나 더 많아야 합니다.
- FMC GUI를 통해 하위 인터페이스, 포트 채널 또는 물리적 인터페이스 중 하나 이상의 인터페이스를 생성합니다.
- FMC GUI Device(FMC GUI 디바이스) > Device Management(디바이스 관리)로 이동하여 필요한 인터페이스를 생성할 FTD를 클릭합니다. Interface(인터페이스) 섹션의 오른쪽 코너 드롭다운 메뉴에서 Create Sub-interface/BVI(하위 인터페이스/BVI 생성)를 선택하여 그에 따라

인터페이스를 생성하고 해당 인터페이스를 연결합니다. 컨피그레이션을 저장하고 디바이스에 동기화합니다.



- Show interface ip brief를 실행하여 FTD에 인터페이스가 생성되었는지 확인하고 인터페이스 매핑을 위한 마이그레이션을 진행합니다.

2. 라우팅 테이블

- Show routing route 또는 Show routing route summary를 실행하여 Palo Alto 방화벽의 라우팅 테이블을 확인합니다.
- 경로를 FTD로 마이그레이션하기 전에 테이블을 확인하고 프로젝트에 필요한 필수 경로를 선택합니다.
- Show route all 및 show route summary를 사용하여 FTD에서 동일한 라우팅 테이블을 검증합니다.

3. 최적화

- [객체 최적화] 패널이 회색으로 비활성화되어 있습니다. 경우에 따라 FMC에서 수동 객체를 만들고 매핑해야 합니다. FTD에서 객체를 보려면 실행 중 표시를 사용합니다 | 개체 및 Palo Alto에서 Show address <object name>을 사용합니다.
- 애플리케이션 마이그레이션을 수행하려면 마이그레이션 전에 Palo Alto 방화벽에 대한 감사가 필요합니다. FTD에는 전용 IPS 디바이스가 있거나 FTD에서 이 기능을 활성화할 수 있으므로 고객 요구 사항에 따라 애플리케이션 마이그레이션 작업을 계획해야 합니다.
- Palo Alto 방화벽의 NAT 컨피그레이션은 show running nat-policy로 확인되어야 하며, FTD에 사용자 지정 NAT 정책이 있어야 합니다. FTD에서는 Show Running nat로 볼 수 있습니다.

결론

Palo Alto 방화벽은 FMT의 도움을 받아 Cisco FTD로 성공적으로 마이그레이션되었습니다. FTD에서 마이그레이션 후 문제가 발생할 경우, 트러블슈팅을 위해 TAC 케이스를 추가로 엽니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.