Cisco ETD(Email Threat Defense)를 Cisco Secure Access와 통합하는 단계:

목차

소개

이 문서에서는 ETD SMTP 인라인 모드에서 Cisco ETD(Email Threat Defense)를 Cisco SA(Secure Access) for Email DLP와 통합하는 단계를 설명합니다. 이렇게 하면 ETD를 통과하는 모든 아웃바운드 이메일은 Cisco SA(Secure Access)의 도움을 받아 DLP를 검사합니다.

개요

오늘날의 분산된 업무 환경에서는 이메일이 여전히 기업의 주요 커뮤니케이션 툴로 사용되고 있으며, 그 결과 사이버 공격과 데이터 유출의 가장 빈번한 공격 대상이 되고 있습니다. Cisco는 이와 같이 진화하는 과제를 해결하기 위해 ETD(Email Threat Defense)와 Secure Access DLP(Email Data Loss Prevention)를 통해 이메일 보안에 대한 포괄적인 접근 방식을 제공합니다.

Cisco Email Threat Defense의 위협 탐지 기능과 Secure Access Email DLP의 강력한 데이터 보호 기능을 결합하여 멀티레이어 방어 전략을 수립할 수 있습니다. 이러한 접근 방식은 외부 사용자로부터 받은 편지함을 보호할 뿐 아니라 사용자의 위치나 이메일 액세스 방식과 상관없이 중요한 기업 데이터를 엄격한 통제 하에 두도록 보장합니다.

사전 요구 사항

아래 콘솔에 액세스합니다.

1. 인라인 모드의 Cisco ETD(Email Threat Defense Console).

   ETD 콘솔은 이메일 보안 상태를 위한 중앙 집중식 관리 플레인으로 작동합니다. 이 콘솔에 액세스하는 것은 지능형 위협을 차단하기 위해 환경을 구성하는 첫 번째 단계입니다.

   - "인라인 모드"가 중요한 이유:ETD가 인라인 모드에서 구성되는 경우, 이메일 흐름의 경로에 있는 MTA(Mail Transfer Agent) 또는 직접 통합의 역할을 합니다. 이렇게 하면 시스템은 메시지를 수신자의 받은 편지함으로 전달하기 전에 검사, 차단 또는 수정할 수 있습니다.
2. Cisco SA(Secure Access Console)

Cisco Secure Access는 DLP(Data Loss Prevention)를 비롯한 다양한 보안 서비스를 응집력 있는 단일 아키텍처로 통합하는 통합 클라우드 기반 보안 플랫폼입니다.

- SA 콘솔이 필요한 이유: Secure Access 콘솔은 조직의 보안 정책을 위한 오케스트레이션 허브입니다. ETD가 위협별 이메일 흐름을 처리하는 반면, Secure Access Console에서는 민감한 데이터가 식별되어 기업 전반에서 처리되는 방식을 제어하는 광범위한 DLP 정책을 정의합니다.
- 콘솔 역할: 이 콘솔을 통해 관리자는 데이터 분류 규칙(예: PII, 신용 카드 번호 또는 내부 프로젝트 코드 식별)을 생성하고 적용할 수 있습니다. SA 콘솔에 액세스하면 이메일 DLP 정책이 전반적인 보안 전략과 동기화되어 두 이메일 트래픽 모두에서 일관되게 시행될 수 있습니다.

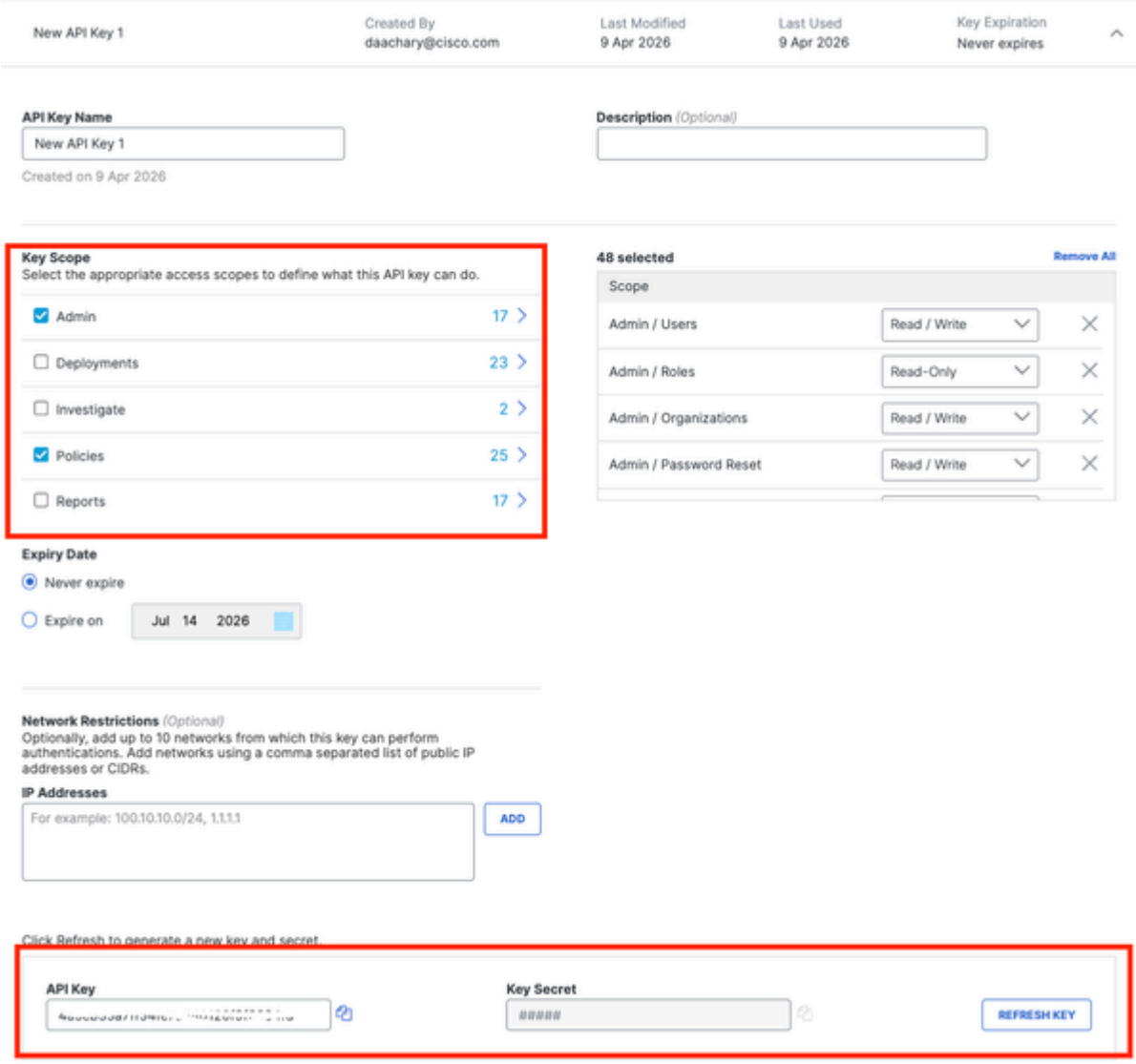
구성

통합 단계

1단계: Cisco Secure Access에서 API 자격 증명 생성

먼저 Secure Access 콘솔 내에서 연결을 인증하기 위해 필요한 API 자격 증명을 생성해야 합니다.

1. Cisco Secure Access Dashboard에 로그인합니다.
2. Admin>API Keys로 이동합니다.
3. 새 API 키를 만드는 옵션을 선택합니다.
4. 키에 AdminandPolicy 범위를 할당합니다.

- [스크린샷: Secure Access API Key Configuration(보안 액세스 API 키 구성)]
- 

2단계: 키 만료 구성

조직의 보안 정책에 따라 API 키의 라이프사이클을 정의합니다.

- 옵션 1: Never Expire(만료 안 함) - 수동 회전 없이 중단 없는 서비스를 제공합니다.
- 옵션 2: Specific Date(특정 날짜) - 정의된 만료 일정을 설정합니다.
  - 중요 참고:만료 날짜를 설정하도록 선택하는 경우 순환 프로세스를 계획해야 합니다. DLP 서비스의 중단을 방지하려면 만료일 전에 ETD 콘솔에서 API 키를 재구성해야 합니다.

3단계: 자격 증명 보호

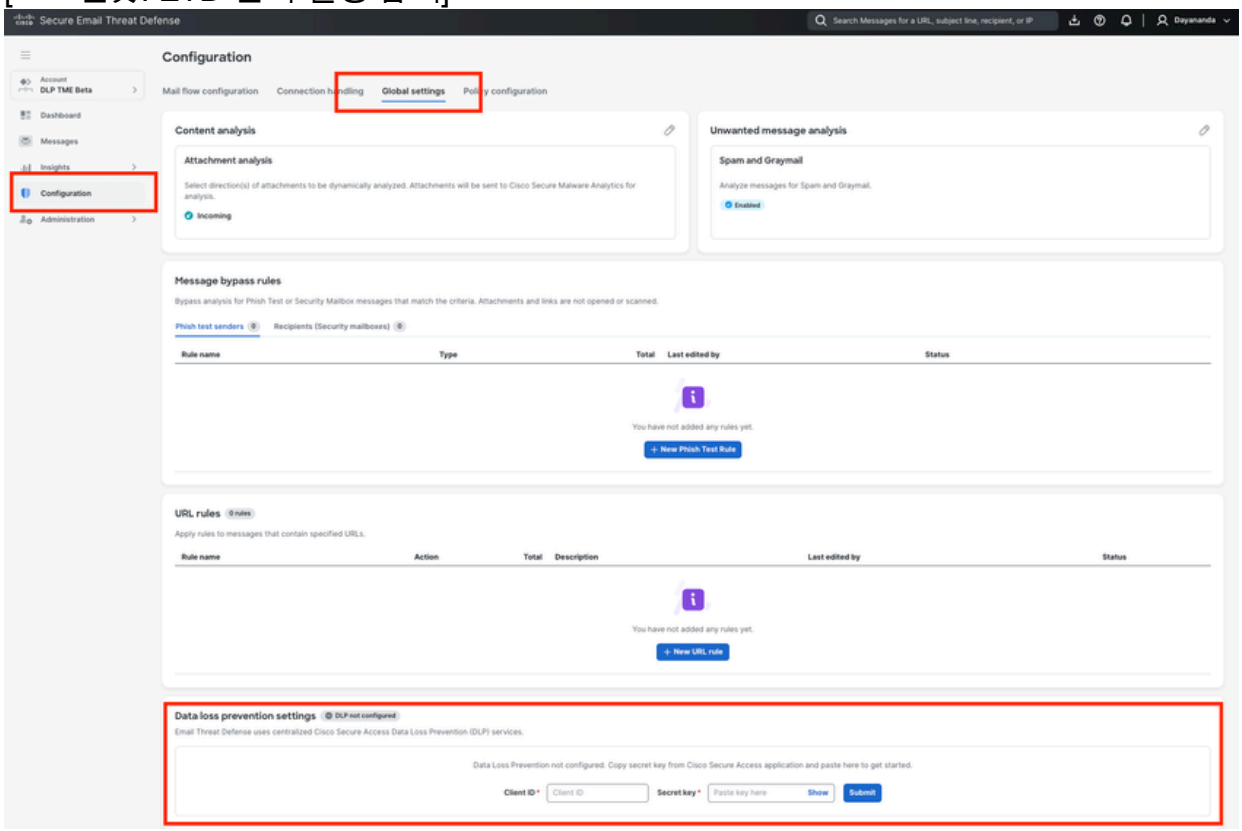
키가 생성되면 API Key(API 키) 및 Key Secret(키 암호)가 표시됩니다.

- 작업:이러한 자격 증명을 안전한 위치(예: 비밀번호 관리자)에 복사하여 저장합니다.
- 경고:이 화면을 벗어나면 Key Secret이 표시되지 않습니다. 분실한 경우 새 키 쌍을 생성해야 합니다.

4단계: ETD 구성 액세스

자격 증명이 보호되면 ETD 콘솔로 이동하여 연결을 완료합니다.

1. Cisco ETDconsole에 로그인합니다.
2. Configuration>Global Settings로 이동합니다.
   - [스크린샷: ETD 전역 설정 탐색]
   -



5단계: 통합 마무리

Secure Access에서 얻은 자격 증명을 입력하여 핸드셰이크를 완료합니다.

1. Global Settings(전역 설정) 메뉴에서 DLP(Data Loss Prevention) 섹션을 찾습니다.
2. 3단계에서 저장한 클라이언트 ID(API 키) 및 암호 키(키 암호)를 입력합니다.
3. 변경 사항을 저장합니다.

검증에 성공하면 Cisco ETD와 Cisco Secure Access 간의 통합이 완료되며, DLP 정책을 이메일 트래픽 전반에 적용할 준비가 완료됩니다.

이제 ETD와 Secure Access의 통합이 완료되었습니다.
참고: 이메일 DLP에 대한 Cisco Secure Access에서 DLP 정책을 생성하려면 "Cisco SA(Secure Access) 및 Cisco ETD(Email Threat Defense)에서 이메일 DLP 정책을 구성하는 방법"을 참조하십시오.

문제 해결 참고 사항

통합 프로세스 도중 또는 이후에 문제가 발생하는 경우 다음과 같은 일반적인 시나리오 및 교정 단계를 검토합니다.

1. ETD에서 허용되지 않는 API 자격 증명

- 증상:ETD에서 클라이언트 ID 및 비밀 키를 입력하면 시스템에서 인증 오류를 반환합니다.
- 해결 방법:
  - API 키가 정확한 필수 범위("Admin" 및"Policy")로 생성되었는지 확인합니다. 다른 범위를 선택했거나 누락된 경우 연결이 실패합니다.
  - 클라이언트 ID 또는 비밀 키를 ETD 콘솔에 붙여넣을 때 실수로 선행 또는 후행 공백이 복사되지 않았는지 확인합니다.

2. 분실 또는 분실한 주요 비밀

- 증상:Secure Access API 생성 화면에서 빠져나갔으므로 키 암호를 더 이상 볼 수 없습니다.
- 해결 방법: 보안상의 이유로 키 암호는 생성 시 한 번만 표시됩니다. 안전하게 저장하지 않은 경우 Secure Access에서 불완전한 API 키를 삭제하고 새 키를 생성해야 합니다.

3. DLP 정책이 이메일 트래픽에 적용되지 않음

- 증상: 통합이 성공한 것으로 표시되지만 구성된 DLP 정책이 민감한 이메일을 포착하거나 차단하지 못합니다.
- 해결 방법:
  - API 만료 확인: API 키 만료에 대해 "특정 날짜 선택"을 선택한 경우(2단계) 키가 만료되지 않았는지 확인합니다. 가 있는 경우 새 키 쌍을 생성하여 적용해야 합니다.
  - ETD 구축 모드 확인:Cisco ETD가 인라인 모드에서 구축되었는지 확인합니다. ETD는

Secure Access DLP 판정에 따라 메시지를 능동적으로 차단하거나 수정하려면 DM(Direct Mail Flow) 경로에 있어야 합니다.
- 동기화 시간: 초기 통합 후, DLP 규칙을 테스트하기 전에 백엔드 시스템이 정책을 동기화할 수 있도록 몇 분간 허용합니다.

4. 안정기간 이후의 서비스 중단

- 증상:DLP 시행은 몇 달 동안 올바르게 작동한 후 갑자기 작동을 멈춥니다.
- 해결 방법: 이 문제는 만료된 API 키로 인해 발생하는 경우가 가장 많습니다. Admin -> API Keys in Cisco Secure Access로 이동하여 ETD에 사용된 키의 상태를 확인합니다. 만료 날짜에 도달하기 전에 ETD에서 자격 증명을 업데이트하기 위한 키 순환 프로세스를 구현합니다.

요약

Cisco ETD(Email Threat Defense)와 Cisco SA(Secure Access)의 통합은 통합 DLP(Data Loss Prevention) 전략을 수립하는 데 있어 매우 중요한 단계입니다. 관리자는 Secure Access Console에서 "Admin" 및 "Policy" 범위를 사용하여 보안 API 키를 생성하고 ETD의 Global Settings 내에서 이러한 자격 증명을 구성함으로써 두 플랫폼 간에 원활한 통신 브리지를 생성합니다.

이 핸드셰이크가 완료되면 ETD는 이메일 메타데이터를 Secure Access DLP 엔진에 능동적으로 핸드오프할 수 있습니다. 이를 통해 조직은 단일 중앙 집중식 대시보드(Secure Access)에서 모든 데이터 보호 정책을 관리하는 동시에 이메일 트래픽(ETD)에 대한 심층적인 가시성과 시행을 유지할 수 있습니다.

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.