보안 ICAP를 사용하여 온프레미스 DLP와 보안 액세스 통합

목차

소개

이 문서에서는 보안 ICAP를 사용하여 온프레미스 DLP(Data Loss Prevention) 서버와 보안 액세스를 통합하는 방법에 대해 설명합니다.

개요

Umbrella를 온프레미스 DLP 솔루션과 통합하여 중앙 집중식 이벤트 관리 및 리미디에이션 워크플로를 지원할 수 있습니다. 이 통합에서는 Secure ICAP(Internet Content Adaptation Protocol)를 사용하여 추가 분석을 위해 DLP 정책을 위반하는 HTTP/S 트래픽을 온프레미스 DLP 서버로 전달합니다.

온프레미스 DLP 서버와 보안 액세스 통합

- 통합에서는 추가 검사를 위해 DLP 정책을 위반하는 HTTP/S 트래픽을 온프레미스 DLP 서버로 안전하게 전송하는 보안 ICAP를 사용합니다.
- Secure ICAP는 TLS를 사용하여 트래픽을 암호화하고 Umbrella 대시보드에 업로드된 인증서로 DLP 서버를 인증합니다.
- 보안 강화를 위해 Umbrella IP 주소에서 DLP 서버의 ICAP 포트로의 트래픽만 허용하도록 인바운드 방화벽 규칙을 제한합니다.

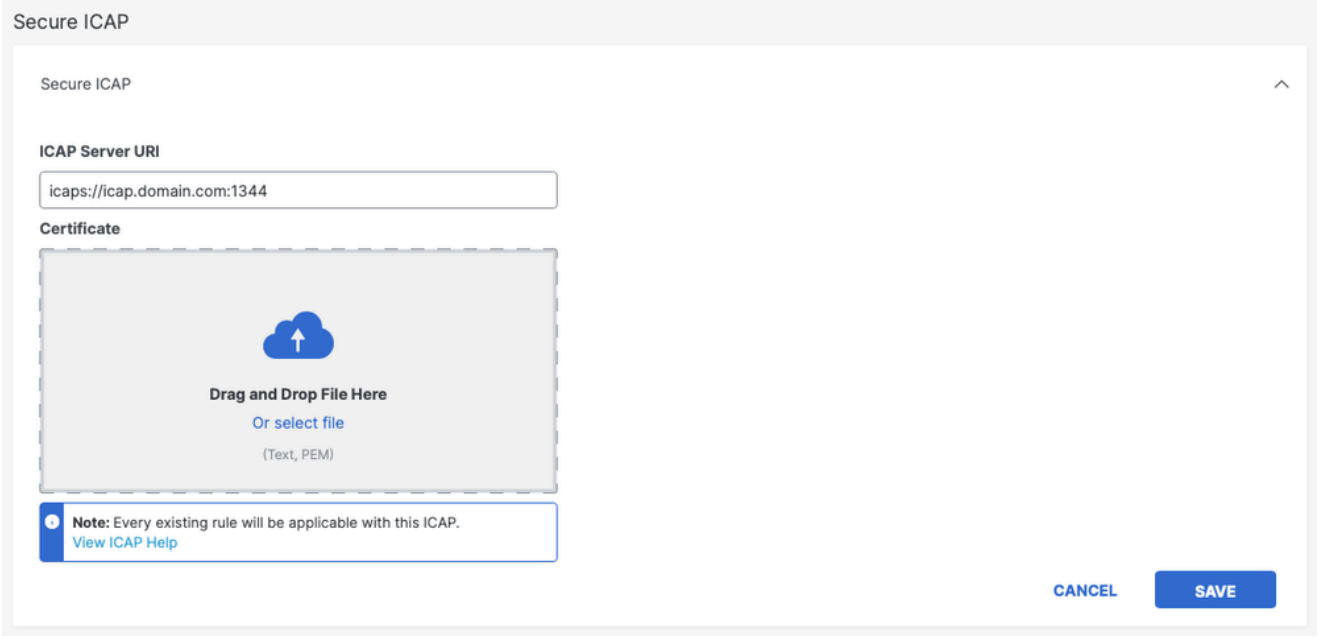
허용할 필수 IP 주소

보안 ICAP 트래픽을 허용하려면 다음 Umbrella IP 주소를 방화벽에 추가합니다.

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

Secure ICAP 통합 사용

1. 온프레미스 DLP 서버 온보드:
    - Umbrella 대시보드에서 Admin(관리) > Authentication(인증) > ICAP로 이동합니다.
    - Secure ICAP를 활성화하려면 DLP 서버 인증서를 업로드합니다.



2. 온프레미스 DLP 서버로 트래픽을 전달하도록 실시간 DLP 규칙을 구성합니다.

    - 규칙 컨피그레이션에서 ICAPsection을 사용하여 전달을 활성화합니다.
    - 모든 실시간 DLP 활성 규칙은 기본적으로 활성화되어 있습니다.

온-프레미스 DLP 서버로 전송된 데이터

- Umbrella는 전체 HTTP/S 메시지(본문 및 헤더)를 온프레미스 DLP 서버로 전송합니다.
- 사용자 지정 헤더가 포함되어 있습니다.
    - X-Authenticated-User:사용자 ID
    - X-Authenticated-Groups:사용자 그룹 ID
    - X-Client-IP:클라이언트 IP 주소

지원되는 위반 이벤트

모니터링되고 차단된 실시간 DLP 위반 이벤트는 모두 Secure ICAP를 통해 전송됩니다.

DLP 서버에서 ICAP 활성화

DLP 솔루션 설명서 및 지원을 참조하여 임베디드 ICAP 서버를 활성화합니다. ICAP(Secure ICAP 아님)만 지원되는 경우 Secure ICAP를 활성화하려면 온프레미스 DLP 서버 앞에 TLS 종료 구성 요소(Stunnel 등)를 구축합니다.

관련 리소스

추가 지침: Secure ICAP 관리 Umbrella 설명서를 참조하십시오.

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.