Umbrella Roaming Client의 IP 레이어 시행 기능을 위한 단종

목차

[소개](#)

[개요](#)

[추가 정보](#)

소개

이 문서에서는 IP Layer Enforcement가 2022년 7월 31일에 단종된다는 Cisco Umbrella 발표에 대해 설명합니다.

개요

IP Layer Enforcement는 일부 Cisco Umbrella 패키지에 대해 Umbrella Intelligent Proxy를 사용할 수 있는 로밍 클라이언트에 대한 선택적 기능입니다.

2021년 8월 31일 이후 고객이 주문한 Cisco Umbrella 패키지에는 IP Layer Enforcement가 더 이상 포함되지 않습니다. 이전에 IP Layer Enforcement 옵션이 포함된 패키지를 주문한 고객의 경우 이 기능은 2022년 7월 31일까지 계속 작동합니다. IP Layer Enforcement를 운영하는 데 필요한 클라우드 측 서비스는 2022년 7월 31일에 종료됩니다.

Cisco Umbrella DNS Essentials 및 DNS Advantage 패키지는 배포가 간단하고 관리하기 쉬운 강력한 DNS 보안 솔루션을 제공합니다. 이러한 DNS 패키지는 Umbrella DNS 요청(DNS 레이어 시행을 통해)으로 시작되는 모든 연결(악의적인 IP 주소로 확인되는 미확인, 분류되지 않은 도메인)에 대해서도 악의적인 서버로부터 DNS 가입자를 계속 보호합니다.

Cisco Umbrella SIG(Secure Internet Gateway) 패키지에는 모든 트래픽(DNS, IP, 웹 등)에 적용되는 더욱 향상된 보안 범위가 포함되어 있습니다. SIG에는 웹 포트(IP 또는 도메인 대상)의 모든 트래픽을 분석하는 SWG(Secure Web Gateway) 및 SWG 외에 클라우드 기반 방화벽에 레이어가 설정되는 CDFW(Cloud Delivered Firewall)가 포함됩니다. 이를 통해 IP Layer Enforcement를 통한 DNS를 넘어 DNS 이상의 보호를 제공하기 위한 엔드포인트 소프트웨어의 요구 사항까지 포함하여 Cisco 클라우드 보안 효율성의 포트폴리오가 향상됩니다. Umbrella SIG 패키지는 DNS 이상의 커버리지가 필요한 모든 사용자에게 권장됩니다.

Cisco Umbrella로 네트워크 스택을 보호하고 지금 Cisco Umbrella 계정 관리자와 통화하여 Cisco Secure Internet Gateway 솔루션에 대해 자세히 알아보십시오.

추가 정보

AnyConnect 버전 지원

IP Layer Enforcement는 IP Layer Enforcement end-of-life 날짜를 통해 AnyConnect 버전 4.x에서 지원됩니다. 버전 5.x는 IP 레이어 시행을 지원하지 않습니다. Cisco Secure Client Branded Client에는 IP Layer Enforcement 지원이 포함되지 않습니다. 기존 AnyConnect 사용자는 IP Layer Enforcement End-of-Life 날짜를 통해 IP Layer Enforcement 기능을 사용하려면 AnyConnect 4.x 클라이언트를 계속 사용해야 합니다.

Cisco 대안

Cisco Secure Endpoint(이전의 AMP)는 IP 위협에 대한 온디바이스 보호 기능을 제공합니다. 여기에는 새 프로세스의 새 연결을 평가하는 "DFC"라는 기능이 포함됩니다. 이 기능은 Umbrella IPLE 기능을 더 보완하기 위해 확장될 예정입니다. ELA에 Cisco Secure Endpoint를 추가하는 방법은 어카운트 매니저에게 문의하십시오.

SIG는 SWG의 모든 웹 트래픽과 클라우드 방화벽을 통한 모든 공용 인터넷 트래픽에 대한 커버리지를 제공합니다. IPLE 블록의 95% 이상이 SWG가 지원하는 웹 트래픽입니다! (TCP 443 및 80을 통한 웹 트래픽). 이 기능은 SWG에서 제공하며 IPLE에서 구동하지 않습니다.

조직의 IPLE 부가 가치 보기

조직의 현재 IP 레이어 시행 블록(백만 로그 라인 기준)을 계산하려면 다음 단계를 수행합니다.

1. Umbrella Dashboard(Umbrella 대시보드)에 로그인하고 Activity Search(활동 검색) 보고서를 엽니다.
2. "IP Layer Enforcement" 로그 유형("All"에서 변경)으로 이동합니다.
3. 1,000,000행의 CSV를 내보내고 내보낸 보고서를 다운로드합니다.
4. "Malware(악성코드)" 또는 "Botnet(봇넷)" 카테고리가 포함되지 않은 모든 라인을 필터링합니다.
 - "Unauthorized IP Tunnel Traffic"을 제외합니다. 이 카테고리는 시행 목록이 아닌 IPSec 터널을 통과하는 트래픽입니다. 자동으로 서비스에서 삭제됩니다.
 - 트래픽 포트를 확인합니다. 포트 443 및 80은 SIG Essentials 패키지에서 완전히 지원되었을 것입니다.
5. 총 블록 수는 조직의 블록 수입입니다. 이를 "Total Requests(총 요청)" 보고서의 총 DNS 요청과 비교하여 효율성 비율을 계산합니다.

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.