Tor 차단을 위한 Umbrella 구성

목차

소개

이 문서에서는 Umbrella로 Tor를 차단하는 방법을 설명합니다.

개요

토르 네트워크는 자원자가 운영하는 릴레이를 사용하여 분산된 익명 네트워크를 호스팅합니다. 트래픽 분석의 위험을 줄이기 위해 단일 지점에서 사용자를 대상에 연결할 수 없도록 보장합니다. Tor는 많은 합법적인 용도를 가지고 있지만 네트워크 관리자가 기업 네트워크에서 모든 Tor 기반 트래픽을 차단하려는 이유가 있습니다.

요컨대, Umbrella로 토르를 완전히 차단하는 것은 불가능하다. Proxy/Anonymizer 범주를 차단할 경우 torproject.org이 차단됩니다. 그러나 사용자 소유 장치에는 이미 Tor 브라우저가 설치되어 있고 이를 네트워크로 가져올 수 있습니다.

설명

토르는 대리인이에요. TCP 연결을 연 후 목적지 호스트의 주소 및 포트를 인코딩하는 페이로드가 종료 노드로 전송됩니다. 이를 수신한 종료 노드는 필요에 따라 주소를 확인합니다.

다음 사항을 염두에 두고 자세히 알아보십시오.

- Tor 어니언 서비스는 루트 DNS 서버에서 인식하지 못하는 .onion TLD를 사용합니다. .onion 도메인에 액세스하려면 Tor가 필요합니다.
- Tor 트래픽을 차단하는 가장 일반적인 방법은 Tor 종료 노드의 업데이트 목록을 찾고 이러한 노드를 차단하도록 방화벽을 구성하는 것입니다. 토르 사용을 막기 위한 회사 정책도 사용을 중단하려면 먼 길을 갈 수 있다.
- 그러나 개별 컨피그레이션은 OpenDNS/Cisco Umbrella가 지원할 수 있는 기능이 아닙니다. 각 방화벽에는 고유한 컨피그레이션 인터페이스가 있으며 이러한 인터페이스는 매우 다양하기 때문입니다. 확실하지 않은 경우 라우터나 방화벽 설명서를 확인하거나 제조업체에 문의하여 가능한지 확인하십시오.

토르 차단에 대한 자세한 내용은 토르 프로젝트의 남용 FAQ를 참조하십시오. 연결된 FAQ는 주로 토르 사용자가 서비스에 액세스하는 것을 차단하려는 서비스 제공자를 위한 것이지만 네트워크 관리자를 위한 유용한 링크도 포함되어 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.