DNS 터널링 VPN 보안 범주 구성

목차

소개

이 문서에서는 Umbrella에서 DNS 터널링 VPN 보안 카테고리를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Umbrella DNS를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

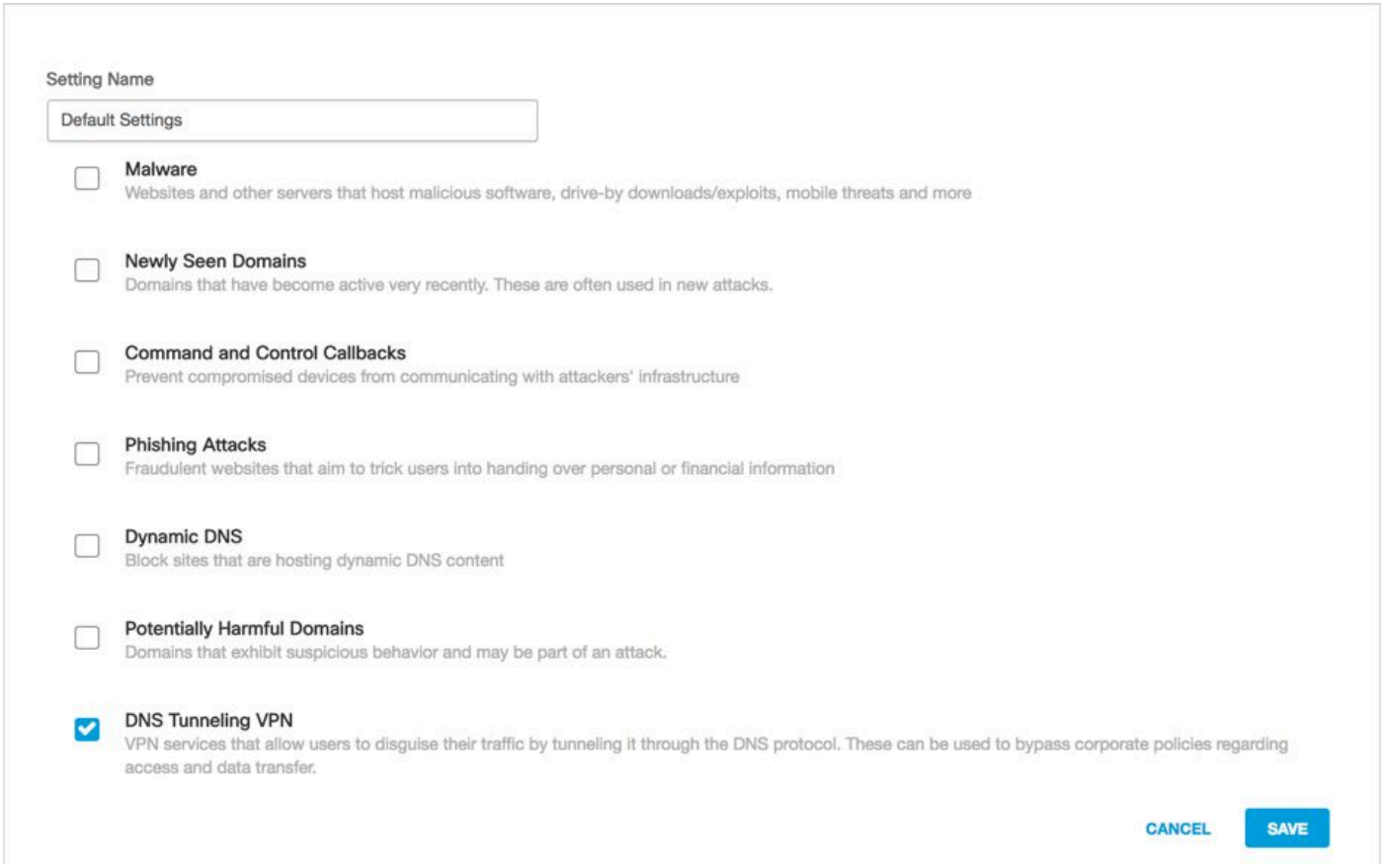
DNS 터널링 VPN은 DNS 터널링 VPN 서비스와 연결된 서버를 차단하거나 허용 및 보고할 수 있는 보안 범주로 분류합니다. 이러한 서비스를 통해 최종 사용자는 발신 트래픽을 DNS 쿼리로 위장하여 사용 제한, 데이터 유출 방지 또는 보안 정책을 위반할 수 있습니다. 그 결과, 이러한 서비스는 잠재적 보안 위협을 야기하고 환경의 전반적 가시성을 저하시킬 수 있습니다.

즉각적인 가시성을 제공하는 이 보안 카테고리를 통해 DNS 터널링 및 잠재적 데이터 손실의 위험을 줄일 수 있습니다. 이 범주를 완전히 차단하거나 보고서의 결과를 모니터링할 수 있습니다. 이를 통해 귀사의 위험 허용 범위, 허용 가능한 사용 또는 HR 정책에 따라 문제를 해결하는 데 적합한 접근 방식을 유연하게 결정할 수 있습니다.

DNS 터널링 VPN 켜기

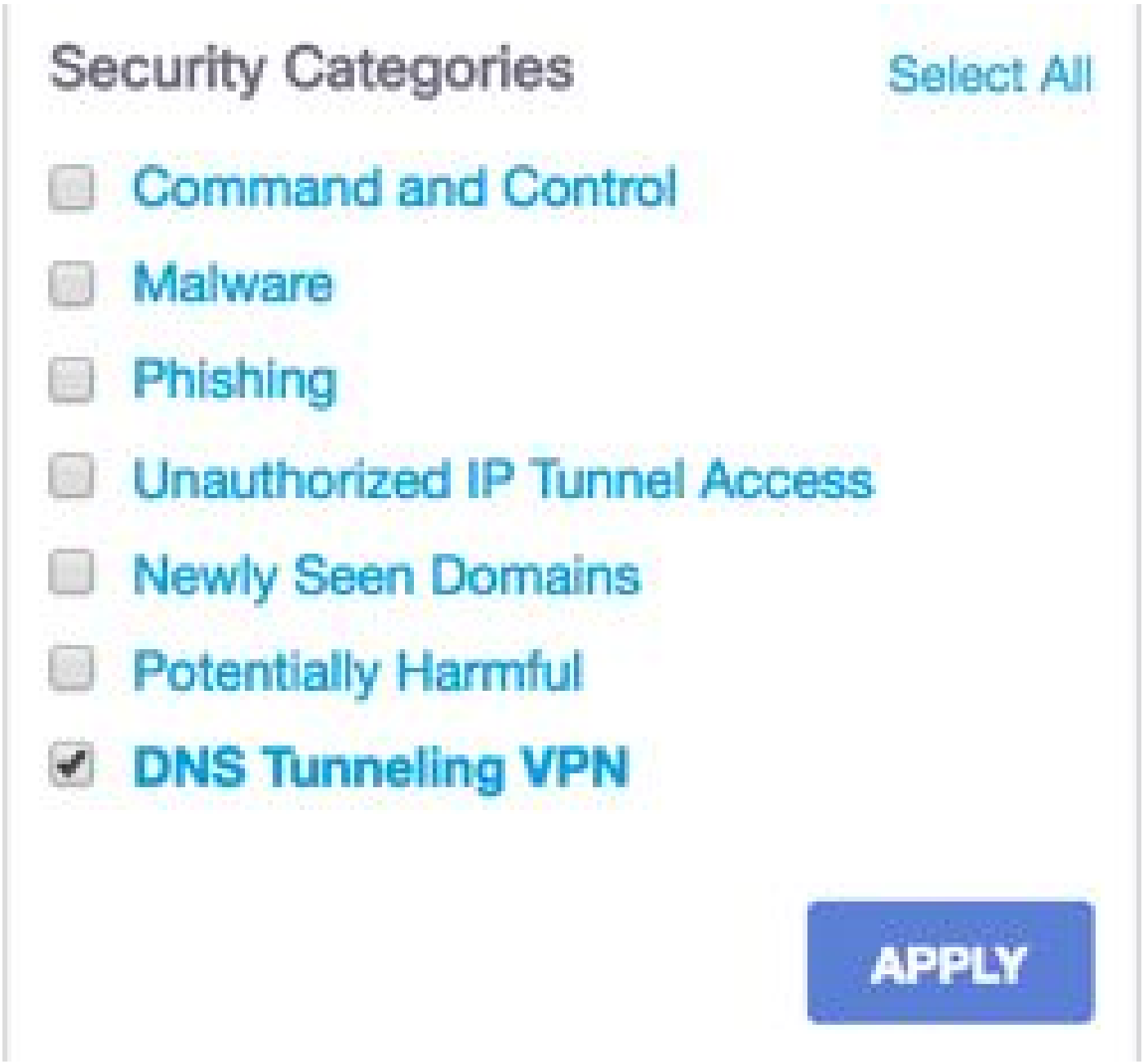
이 보안 카테고리는 Policies(정책) > Security Settings(보안 설정)에서 기존 보안 설정을 편집하는

다른 보안 카테고리와 마찬가지로 활성화할 수 있습니다. 또는 정책 컨피그레이션 마법사 자체 내에서 수행할 수 있습니다.



115014823666

DNS 터널링은 활동 검색 보고서를 통해 필터링할 수 있습니다.



115015008983

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.