SSL VPN 트래픽과의 충돌을 피하도록 SWG 구성

목차

소개

이 문서에서는 인터셉트된 포트를 사용하여 SWG(Secure Web Gateway)와 SSL VPN 간의 비호환성 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 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.

문제

AnyConnect용 Umbrella SWG는 TCP 443과 같이 SWG 에이전트에서 가로채는 포트를 사용하는 특정 SSL VPN과 호환되지 않는 문제가 발생할 수 있습니다. AnyConnect SWG는 커버리지를 활성화하고 안정적으로 적용하지 못할 수 있습니다. SWG가 활성 상태이고 VPN 트래픽이 SWG를 통과하면 네트워크 안정성이 저하되거나 사용할 수 없게 될 수 있습니다. 이 시나리오에서는 웹이 아닌 트래픽이 삭제됩니다. 이 문제는 포트 80 및 443을 사용하는 모든 SSL VPN에 영향을 줍니다.

솔루션

SWG가 VPN 트래픽을 가로채지 못하게 하려면 VPN 도메인 및 IP 주소에 대한 우회를 구성합니다.

1. Umbrella 대시보드에서 Access Deployments(액세스 구축) > Domain Management(도메인 관리) > External Domains(외부 도메인)로 이동합니다.

2. VPN 헤드 엔드 서버의 도메인 및 IP 주소를 External Domains(외부 도메인) 목록에 추가합니다. IP 엔트리는 많은 수의 연결로 인해 VPN 트래픽이 SWG 에이전트에 의해 가로채지지 않도록 합니다.

3. 새 설정이 전파될 때까지 1시간을 허용합니다.

SWG에서 SSL VPN을 사용하려면

1. External Domains(외부 도메인) 목록에 VPN 도메인을 추가합니다.

2. VPN 헤드 엔드 도메인이 DNS 검색 접미사인 경우 클라이언트는 연결 기간 동안 이 도메인을 자동으로 추가합니다.

3. VPN 헤드 엔드 IP 주소 또는 IP 범위를 External Domains(외부 도메인) 목록에 추가합니다.

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.