

제로 트러스트 액세스 및 VPN 연결에 대한 지리적 액세스 제한

목차

문제

ZTA(Zero Trust Access) 및 VPN 연결에 지리적 액세스 제한이 필요한 조직은 국가 기반 액세스 제어를 구현하려고 할 때 기존 ZTA 및 VPN 정책을 비활성화해야 함을 알 수 있습니다. Secure SSE 제품 인터페이스 내에서 네이티브 지리적 제한 옵션을 찾을 수 없어 정책이 비활성화되면 사용자는 필수 리소스에 대한 액세스 권한을 완전히 상실하게 됩니다. 특정 국가 내에서만 시작되는 연결에 대한 액세스를 제한하기 위한 특정 요구 사항은 기본 제공 제품 기능을 사용하여 구성할 수 없으므로, 이러한 제한을 구현하기 위해 기존 정책을 비활성화할 경우 사용자에게 광범위한 영향을 미치게 됩니다.

환경

- Cisco SASE(Secure Access Service Edge)/Secure SSE 제품
- ZTNA(Zero Trust Access) 구현
- 지리적 액세스 제어가 필요한 VPN 서비스
- 프라이빗 리소스 액세스 정책
- 국가별 액세스 제한이 필요한 조직

해결

Cisco Secure SSE 제품은 현재 사용자의 지리적 위치 또는 국가를 기준으로 개인 리소스 액세스를 제한하는 기본 기능을 제공하지 않습니다. 다음 섹션에서 기술되는 접근법들은 이러한 한계를 해결하는데 고려될 수 있다.

기능 요청 제출

ZTA 및 VPN 액세스를 위한 지리적 제한 기능을 추가하려면 기능 요청을 Cisco에 제출해야 합니다. 이 개선 요청은 제품 팀에서 향후 릴리스에 포함될 가능성을 평가합니다. 조직은 Cisco Account Manager와 협력하여 비즈니스 요구 사항에 따라 그러한 기능 요청의 우선 순위를 지정할 수 있습니다.

수동 해결 고려 사항

잠재적인 수동 해결 방법에는 국가별 공용 IP 주소 범위를 액세스 정책의 네트워크 객체 그룹으로 추가하는 것이 포함됩니다.

1단계: 해당 RIR(Regional Internet Registry)에서 국가 공용 IP 주소 범위를 가져옵니다.

2단계: 식별된 IP 범위를 포함하는 네트워크 객체 그룹을 생성합니다. 대상 국가에 할당된 특정 IP 주소 범위를 포함하도록 액세스 정책 컨피그레이션 내에서 네트워크 객체 그룹을 구성합니다.

3단계: 액세스 정책에 네트워크 객체 그룹을 적용합니다. 생성된 네트워크 객체 그룹을 참조하도록 기존 액세스 정책을 수정하여 지정된 IP 범위에서 시작되는 연결에 대한 액세스를 효과적으로 제한합니다.

중요한 제한 사항

이 수동 접근 방식은 고정 IP 범위 정의에 의존하고 지리적 제한을 우회할 수 있는 동적 IP 할당, 모바일 사용자 또는 VPN 서비스를 설명할 수 없으므로 상당한 제한이 있습니다. 또한 이 방법은 IP 범위의 정확성을 보장하기 위해 지속적인 유지 보수를 필요로 합니다.

임시 정책 관리

영구 솔루션을 사용할 수 있을 때까지 조직은 모든 ZTA 및 VPN 정책을 동시에 비활성화하는 것을 피해야 합니다. 대신, 주요 액세스 정책이 활성 상태로 유지되는 동시에 지리적 제한 요구 사항이 대체 수단을 통해 해결되거나 제품 개선을 기다리는 단계적 접근 방식을 구현하는 것을 고려하십시오.

원인

Cisco Secure SSE 제품 아키텍처에는 프라이빗 리소스 액세스를 위한 기본 지리적 액세스 제어 기능이 포함되어 있지 않습니다. 제품 액세스 정책 프레임워크는 사용자 ID, 디바이스 상태 및 네트워크 기반 제어에 중점을 두고 설계되었지만 지리적 위치를 정책 시행 매개변수로 통합하지는 않습니다. 이는 컨피그레이션 문제 또는 소프트웨어 결함이 아닌 제품 기능의 차이를 나타냅니다.

관련 콘텐츠

- [Cisco 기술 지원 및 다운로드](#)

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.