

분할 라우팅 구성을 위한 보안 액세스 대상 주소

목차

문제

Hub-Spoke 네트워크 아키텍처의 Windows 엔드포인트에 Cisco CSC(Secure Client)를 사용하여 Cisco CSA(Secure Access)를 구축할 경우, 조직은 Spoke 사이트 트래픽이 허브를 통해 헤어핀(hairpinning)하는 대신 로컬 Spoke 인터넷 회로를 통해 CSA에 직접 연결할 수 있도록 분할 라우팅을 구성해야 합니다. 이 컨피그레이션에서는 Fortigate 방화벽과 같은 네트워크 디바이스에서 라우팅 예외(분할 라우팅)를 정의할 수 있도록 CSA 터널을 설정할 때 사용되는 모든 Cisco 대상 주소에 대한 지식이 필요합니다.

특정 요구 사항은 TLS/DTLS 터널을 설정할 때 CSC에서 사용하는 CSA 엔드포인트에 대한 모든 대상 정보(IP 주소 또는 URL)를 식별하여 CSA 트래픽에 대해 Hub-Spoke VPN 터널을 우회하는 라우팅 정책을 적절하게 구성하는 것입니다.

환경

- CSA(Cisco Secure Access) 구축
- Windows 엔드포인트의 CSC(Cisco Secure Client)
- Fortigate 방화벽을 사용한 허브-스포크 네트워크 토폴로지
- CSA에 대한 TLS/DTLS 터널 연결

해결

Cisco Secure Access 연결을 위한 분할 라우팅을 구성하려면 CSA 엔드포인트에 직접 연결할 수 있도록 Fortigate 디바이스에서 다음 섹션에 설명된 대상 정보를 구성해야 합니다.

CSA 대상 도메인 및 포트

주 도메인

*.vpn.sse.cisco.com

필수 포트 및 프로토콜

- TCP/UDP 443 TLS/DTLS 터널 설정에 사용
- UDP 500/4500: IPsec 터널 설정에 사용됨
- TCP 80: VPN 인증서 해지 확인에 사용됨

Fortigate 컨피그레이션 접근 방식

CSA 도메인(*.vpn.sse.cisco.com) 및 지정된 포트로 향하는 트래픽을 Hub-Spoke VPN 터널이 아닌 로컬 Spoke 인터넷 회로를 통해 디렉션하도록 Fortigate 디바이스의 라우팅 정책을 구성합니다. 이렇게 하면 다음 코드 조각에 요약된 트래픽 흐름이 활성화됩니다.

원하는 트래픽 흐름

Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication

허브 사이트를 통한 트래픽 흐름 대신

중요 고려 사항

CSA 연결 대상은 런타임 중에 동적으로 결정되며, 이는 고정 라우팅 컨피그레이션에 대해 특정 IP 주소를 미리 지정할 수 없음을 의미합니다. *.vpn.sse.cisco.com을 사용하는 도메인 기반 접근 방식은 분할 라우팅 정책을 구성하는 가장 안정적인 방법을 제공합니다.

최신 목적지 및 포트 요구 사항은 Cisco Secure Access 공식 문서를 참조하십시오. 이러한 요구 사항은 새 소프트웨어 릴리스로 업데이트될 가능성이 높습니다.

원인

Hub-Spoke 네트워크 토폴로지에서는 Spoke 사이트의 모든 인터넷 바인딩 트래픽이 기본적으로 Hub 사이트를 통해 라우팅됩니다. CSC와 함께 CSA를 구현할 경우 이 기본 라우팅 동작으로 인해 CSA 터널 트래픽이 CSA 엔드포인트에 도달하기 전에 허브 사이트를 통해 헤어핀되므로 잠재적으로 지연 및 대역폭 비효율성이 발생합니다. CSA 엔드포인트 선택의 동적 특성에는 적절한 분할 라우팅 기능을 보장하기 위해 고정 IP 기반 규칙이 아닌 도메인 기반 라우팅 정책이 필요합니다.

관련 콘텐츠

- [Cisco Secure Access 설명서 - 연결 요구 사항](#)
- [Cisco Secure Access 설명서 - 네트워크 컨피그레이션](#)
- [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.