보안 액세스 VPN - Jabber에 액세스할 수 없음

목차

문제

보안 클라이언트 사용자는 개인 액세스 정책을 사용할 때 보안 액세스 VPN 터널을 통해 Jabber 및 Epic과 같은 내부 및 개인 애플리케이션에 액세스할 수 없습니다. 사용자는 VPN 연결을 통해 이러한 중요한 비즈니스 애플리케이션에 연결하려고 할 때 연결 실패를 경험했습니다. 트러블슈팅 중에 Epic 리소스에 대해 단방향 트래픽이 관찰되었습니다. 이 리소스에서 ping 및 TCP SYN 트래픽이 Secure Access VPN 터널을 벗어난 것으로 확인되었지만 Palo Alto 방화벽에서 반환 트래픽 검증 문제가 발견되었습니다. 또한 IP 기반 라우팅을 위해 트래픽 스티어링을 구성하는 동안 내부 DNS를 통해 CUCM FQDN을 해결하여 트래픽 흐름의 불일치를 초래하는 Jabber 연결 문제가 문서화되었습니다.

환경

- VPN 터널 컨피그레이션을 통한 Cisco Secure Access
- VPN 연결을 위한 보안 클라이언트
- 프라이빗 액세스 정책 구현
- Cisco Unified Communications Manager(CUCM) for Jabber 서비스
- Epic 애플리케이션 리소스
- 네트워크 보안을 위한 Palo Alto 방화벽
- CUCM FQDN에 대한 내부 DNS 확인

해결

해결에는 Secure Access VPN 터널을 통해 내부 애플리케이션에 대한 연결을 복원하기 위한 여러 컨피그레이션 변경 및 트러블슈팅 단계가 포함되었습니다.

서브넷 구성 및 터널 수정

1단계: VPN 터널에 추가 서브넷 추가

영향을 받는 리소스에 대한 VPN 터널 컨피그레이션에 서브넷이 추가되었습니다. 이 변경을 구현한 후 이전에 액세스할 수 없었던 리소스를 성공적으로 로드하기 시작했습니다.

CUCM IP 주소 조정 컨피그레이션

2단계: CUCM IP Steering 구성

트래픽 스티어링이 IP 기반인 동안 내부 DNS를 통해 CUCM FQDN이 확인되는 Jabber 연결 문제를 해결하려면 CUCM IP 주소를 Secure Client로 조향했습니다. 이 컨피그레이션 변경은 DNS 확인을 트래픽 조정 메커니즘과 연계했습니다.

3단계: 액세스 정책 규칙 생성

CUCM IP 주소에 연결할 수 있도록 허용하는 액세스 정책 규칙이 만들어졌습니다. 이 규칙은 CUCM 인프라에 대한 올바른 연결을 복원하여 VPN 터널을 통해 Jabber 기능을 활성화했습니다.

정적 라우팅 컨피그레이션

4단계: CUCM 서브넷에 대한 정적 라우팅 구성

CUCM IP 주소 및 전체 CUCM 서브넷이 네트워크 터널의 정적 라우팅 테이블에 포함되어 있는지 확인합니다. 이 컨피그레이션을 통해 보안 클라이언트 사용자 풀과 CUCM 인프라 간에 적절한 트래픽 라우팅이 보장됩니다.

반환 트래픽 검증

5단계: 패킷 흐름 및 반환 트래픽 검증

패킷 흐름 컨피그레이션을 검증하여 반환 트래픽이 Secure Client 사용자 풀에 도달할 수 있는지 확인합니다. 여기에는 모든 내부 리소스, 특히 단방향 트래픽이 관찰된 에픽 연결에 대해 올바른 반환 경로 검증을 보장하기 위해 Palo Alto 방화벽 컨피그레이션을 검토하는 것이 포함됩니다.

원인

연결 문제는 Secure Access VPN 구현의 여러 구성 차이로 인해 발생했습니다.

- VPN 터널에 서브넷 구성이 누락되어 내부 애플리케이션 리소스에 대한 라우팅이 제대로 수행되지 않음
- CUCM 서비스에 대한 DNS 확인(FQDN 기반)과 트래픽 스티어링 컨피그레이션(IP 기반)이 일치하지 않아 Jabber 연결 오류가 발생했습니다.
- CUCM IP 주소에 대한 트래픽을 허용하지 않은 불완전한 액세스 정책 규칙
- 네트워크 터널 컨피그레이션에 CUCM 서브넷에 대한 고정 라우팅 항목이 없습니다.
- 양방향 통신에 영향을 미치는 Palo Alto 방화벽의 트래픽 경로 검증 문제 반환

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.