Secure Access Web Security가 사용하도록 설정된 Azure VPN 클라이언트 연결 실패

목차

문제

Umbrella에서 SSE로 마이그레이션하고 새로 할당된 SIA 라이센스로 웹 보안을 활성화한 후 웹 보안이 활성화된 경우 Azure VPN Client 연결이 사용자에 대해 설정되지 않습니다. Azure VPN 클라이언트 연결 문제는 모든 클라이언트에 영향을 미쳐 VPN에 연결할 수 없습니다. Cisco Secure Access Client가 클라이언트 컴퓨터에서 제거되면 VPN 연결이 복원되어 Secure Access Client가 Azure VPN 서비스에 대한 연결을 차단하고 있음을 나타냅니다.

웹 보안을 비활성화하거나 Cisco Secure Access Client를 제거하면 VPN 연결이 복원되지만, 웹 보안 보호가 필요한 경우 Azure VPN을 통해 리소스에 대한 사용자 액세스에 영향을 줍니다.

환경

- Web Security가 활성화된 Cisco Secure Access(이전의 SIA)
- Azure VPN 클라이언트
- Umbrella에서 SSE로의 마이그레이션 완료
- 새로 할당된 SIA 라이센스

해결

해결 방법에는 VPN 연결을 차단하는 트래픽 가로채기를 방지하기 위해 Azure VPN 게이트웨이 공용 IP 주소를 SSE/SWG 예외 목록에 추가하는 작업이 포함됩니다.

1단계: Azure VPN 게이트웨이 IP 주소 식별

Azure VPN 게이트웨이의 공용 IP 주소를 확인합니다.

2단계: SSE/SWG에 IP 기반 예외 추가

1.- Cisco Secure Access 환경의 SSE/SWG 예외 목록에 Azure 가상 게이트웨이 공용 IP 주소를 추가합니다.

2.- Cisco Secure Access Dashboard에 로그인합니다. Connect - End user Connectivity - Internet Security - Add exception(연결 - 최종 사용자 연결 - 인터넷 보안 - 예외 추가)을 클릭합니다. 이렇게 하면 Secure Web Gateway가 Azure VPN 게이트웨이로 향하는 트래픽을 가로채고 검사하는 것을 방지할 수 있습니다.

3단계: VPN 연결 테스트

IP 기반 예외를 적용한 후 Azure VPN 연결을 테스트하여 클라이언트가 웹 보안이 활성화된 VPN 연결을 성공적으로 설정할 수 있는지 확인합니다.

4단계: Expand Testing(테스트 확장)

전체 환경의 추가 사용자에게 IP 기반 예외 테스트를 확장하여 해결 완료를 고려하기 전에 일관된 기능을 보장합니다.

원인

이 문제는 SWG(Secure Web Gateway) 예외 메커니즘에서 도메인에 대한 DNS 조회를 통해 도메인-IP 캐시 항목을 만들어야 하기 때문에 발생합니다. Azure VPN 클라이언트가 VPN URL에 대한 DNS 쿼리를 수행하지 않고 IP 주소에 직접 연결하는 경우 SWG 모듈은 도메인을 IP 주소에 매핑할 수 없습니다. 그 결과, SWG는 IP 주소에 대한 트래픽을 지속적으로 검사 및 차단하여 VPN 연결이

설정되지 않도록 합니다.

패킷 캡처 분석에서는 VPN URL에 대한 DNS 쿼리가 없고 Azure 게이트웨이 IP에 대한 SWG 가로채기 트래픽이 표시되지 않았으며, 캐시에서 적절한 도메인-IP 매핑이 없어 SWG가 연결을 차단하고 있음을 확인했습니다.

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.