보안 액세스 인증서를 가져온 후의 MacOS 인터넷 액세스 문제

목차

문제

MacOS 사용자는 포털에서 인터넷 인증서를 가져온 후 Cisco Secure Access를 통해 인터넷 리소스에 액세스할 수 없습니다.

영향을 받는 서비스는 다음과 같습니다.

- Microsoft Outlook(보내기 및 받기 기능)
- Google.com
- AI 웹사이트
- 기타 웹 대상

동일한 컨피그레이션의 Windows 사용자는 영향을 받지 않으며 계속 정상적으로 작동합니다. 이 문제는 특히 MacOS 클라이언트가 인증서를 가져온 후 이메일 및 일반 인터넷 검색 기능에 액세스하는 데 영향을 미칩니다.

환경

- Cisco Secure Access with Unified Policy Configuration
- Cisco Secure Access 포털에서 가져온 인터넷 인증서가 있는 MacOS 클라이언트
- 동일한 구성의 Windows 클라이언트(영향을 받지 않음)
- 사용 중인 인터넷 정책, 개인 정책, DLP 정책, RBI 및 보안 프로파일
- MacOS와 Windows 간의 차등 동작을 사용하는 혼합 운영 체제 환경

해결

이러한 서비스에 대한 SSL 검사를 우회하기 위해 특정 Microsoft Outlook 엔드포인트 및 애플리케이션을 DND(Do Not Decrypt) 목록에 추가하는 작업이 해결됩니다.

1단계: DND 목록에 Outlook 끝점 추가

Outlook 액세스 문제를 해결하기 위해 DND(Do Not Decrypt) 컨피그레이션에 다음 섹션에서 설명하는 엔드포인트 또는 애플리케이션을 추가합니다.

```
outlook.cloud.microsoft
outlook.office.com
outlook.office365.com
smtp.office365.com
```

2단계: 확인 검증

DND 목록에 Outlook 관련 엔드포인트를 추가한 후 영향받는 MacOS 클라이언트가 이제 액세스할 수 있는지 확인합니다.

- Microsoft Outlook 송수신 기능
- 이전에 영향을 받은 기타 인터넷 리소스

사용자는 이러한 DND 항목을 구현한 후 Outlook 응용 프로그램이 MacOS 장치에서 계속 정상적으로 작동한다는 것을 확인했습니다.

원인

이 문제는 SSL/TLS 암호화 검사가 인터넷 리소스, 특히 Microsoft Outlook 서비스에 대한 보안 연결을 설정하는 MacOS 클라이언트의 기능에 방해가 되어 발생했습니다. 암호화 검사 프로세스에서는 MacOS 플랫폼에서만 적절한 인증서 검증 또는 연결 설정을 할 수 없었지만, Windows 클라이언트

에서는 동일한 검사 정책의 영향을 받지 않았습니다. 영향을 받는 엔드포인트를 Do Not Decrypt 목록에 추가하면 이러한 특정 서비스에 대한 검사를 우회하여 정상적인 연결이 다시 시작될 수 있습니다.

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.