Azure 가상 데스크톱 연결 문제 해결

목차

문제

Cisco Secure Access가 활성화된 상태에서 사용자가 사무실 네트워크에서 AVD에 액세스하면 Azure AVD(Virtual Desktop) 연결이 실패합니다. 다음과 같은 특정 동작이 관찰되었습니다.

- AVD는 Secure Access가 비활성화된 개인 네트워크에서 액세스할 때 잘 작동합니다.
- AVD는 보안 액세스 없이 사무실 네트워크에서 액세스할 때 잘 작동합니다.
- AVD는 Secure Access가 활성화된 어떤 네트워크에서도 액세스할 때 작동하지 않습니다.

이러한 연결 실패는 사용자의 가상 데스크톱 액세스 능력에 영향을 미치고 프로덕션 비즈니스 운영에 영향을 미칩니다. 패킷 캡처 분석에서는 작동 및 비작동 시나리오 모두에서 양방향 트래픽이 나타났으며, TCP 재설정이 없거나 Secure Access가 AVD 연결을 종료한다는 기타 네트워크 레벨 표시기가 있었습니다.

환경

- ZTNA(Zero Trust Network Access)가 활성화된 Cisco Secure Access
- 모든 인터넷 대상에 ZTA를 사용하도록 구성된 ZTNA 프로필
- Microsoft 끝점을 통해 액세스하는 AVD(Azure Virtual Desktop) 배포
- Secure Access 클라이언트가 구축된 Office 네트워크 환경
- 사무실 및 개인 네트워크 모두에서 AVD에 액세스하는 사용자

해결

Microsoft AVD 관련 도메인을 ZTA 예외 목록에 추가하여 Secure Access 클라이언트가 AVD 트래픽에 대해 ZTNA를 우회하도록 허용함으로써 문제가 해결되었습니다.

진단 분석

공동 트러블슈팅 분석에서 ZTNA 프로필이 모든 인터넷 대상에 대해 ZTA를 사용하도록 구성되어 있음을 확인했습니다. 이로 인해 Secure Access가 Secure Access 클라우드 프록시를 통해 AVD의 연속 WebSocket 트래픽을 라우팅했습니다. Azure Virtual Desktop은 복잡하고 연속적인 트래픽(WebSockets)을 사용하여 데스크톱 세션을 실시간으로 스트리밍하며, 클라우드 프록시는 스트리밍 프로토콜을 처리하는 대신 표준 웹 페이지를 검사하도록 설계되었기 때문에 이러한 동작이 세션 삭제를 초래했습니다.

컨피그레이션 변경

이러한 Microsoft AVD 관련 도메인이 ZTA 예외 목록에 추가되었습니다.

```
*.wvd.microsoft.com
*.core.windows.net
*.servicebus.windows.net
*.events.data.microsoft.com
```

이러한 도메인을 ZTA 예외 목록에 추가함으로써 Secure Access 클라이언트에는 AVD별 트래픽을 완전히 무시하라는 지시가 내려졌습니다. 이렇게 하면 AVD 트래픽이 ZTNA 프록시를 완전히 우회하여 Microsoft로 직접 이동할 수 있습니다. 이는 AVD가 제대로 작동하기 위해 Microsoft에서 요구하는 것과 정확히 일치합니다.

검증

ZTA Exceptions(ZTA 예외) 컨피그레이션을 적용한 후 모니터링 기간 동안 AVD 연결이 정상적으로 작동하는 것으로 보고되었습니다. 사용자는 Secure Access가 활성화된 상태에서 사무실 네트워크에서 가상 데스크탑에 성공적으로 액세스할 수 있었습니다.

원인

근본 원인은 Azure Virtual Desktop 연결을 포함하여 모든 인터넷 바인딩 트래픽을 가로챈 ZTNA 프로필 구성입니다. AVD의 WebSocket 트래픽이 검사를 위해 Secure Access 클라우드 프록시를 통해 라우팅될 때, AVD 세션의 연속 스트리밍 특성을 처리하도록 프록시가 설계되지 않았기 때문에 연결이 끊어졌습니다. AVD는 안정적인 데스크톱 스트리밍 세션을 유지하기 위해 Microsoft 엔드포인트에 직접 연결해야 합니다.

관련 콘텐츠

- Microsoft Azure 가상 데스크톱 필수 FQDN 끝점
- Cisco Secure Access에 대한 기본 정보 트러블슈팅 및 수집
- 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.