제로 트러블슈팅 액세스 프로필 컨피그레이션으로 MS Teams 문제 해결

목차

문제

안전한 인터넷 액세스를 위해 ZTA(Zero Trust Access) 프로필에 등록한 사용자가 Microsoft Teams에서 연결 문제를 경험했습니다. 사용자가 ZTA 프로필에 추가되면 Microsoft Teams에서 예기치 않게 통화 연결을 끊고 다른 사용자가 영향을 받는 사용자에게 통화를 시작할 수 없습니다. 그러나 영향을 받는 사용자가 자신의 쪽에서 통화를 시작하면 통화가 성공적으로 연결됩니다.

이 문제는 ZTA 프로필에 온보딩된 사용자에게 격리되며, 이는 ZTA 정책 또는 라우팅 구성이 Teams 통화 연결에 영향을 주고 있음을 나타냅니다. 트래픽 로그는 ms-teams.exe와 같은 프로세스에서 필수 범위(예: 52.112.0.0/14의 일부인 52.115.245.30:3480)의 IP 주소에 이르는 Microsoft Teams 트래픽이 인터넷으로 직접 이동하지 않고 ZTA 클라이언트에서 가로채는 것을 보여줍니다.

환경

- ZTA(Zero Trust Access) 프로파일 구성을 통한 Cisco Secure Access
- "ZTA를 사용하여 모든 인터넷 대상을 보호"로 구성된 ZTA 프로필
- Microsoft Teams 응용 프로그램
- ZTA 기능을 갖춘 Cisco Secure Client
- 보안 인터넷 액세스를 위해 ZTA 프로필에 등록된 사용자

해결

이 문제를 해결하려면 Microsoft Teams 트래픽 예외를 ZTA 프로필 구성에 추가하여 Teams 트래픽

이 ZTA 터널을 우회하고 인터넷에 직접 연결하도록 합니다.

1. Dashboard(대시보드) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(제로 트러스트 액세스)로 이동하여 영향을 받는 ZTA 프로필을 찾습니다.

2. ZTA 프로파일을 선택하고 편집 > 보안 인터넷 액세스를 선택합니다.

3. Microsoft의 공식 문서에 따라 예외 목록에 다음 IP 범위 및 FQDN을 추가합니다.

IP 범위:

```
52.112.0.0/14
52.122.0.0/15
2603:1063::/38
2603:1027::/48
2603:1037::/48
2603:1047::/48
2603:1057::/48
2620:1ec:6::/48
2620:1ec:40::/42
```

FQDN:

```
*.lync.com
*.teams.cloud.microsoft
*.teams.microsoft.com
teams.cloud.microsoft
teams.microsoft.com
*.keydelivery.mediaservices.windows.net
*.streaming.mediaservices.windows.net
aka.ms
```

4. 예외에 대한 설명을 추가합니다. 예를 들면 다음과 같습니다.

```
MS Teams exception as per: https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-addre
```

5. 구성 변경 사항을 저장합니다. 변경 사항이 적용될 때까지 몇 분 정도 기다립니다.

6. ZTA 클라이언트 정책이 영향을 받는 엔드포인트에서 다시 동기화되는지 확인합니다. 이 경우 제로 트러스트 액세스 에이전트 서비스를 다시 시작하거나 클라이언트 장치를 다시 시작해야 할 수

있습니다.

7. 테스트 팀이 기능별로 전화를 걸어 다음을 확인합니다.

- 영향을 받는 사용자에게 걸려오는 전화가 연결되었습니다.
- 팀 통화가 더 이상 예기치 않게 연결이 끊기지 않습니다.
- 팀 트래픽은 ZTA 터널을 우회하여 인터넷에 직접 연결

참고: 예외를 구현한 후 팀 트래픽은 ZTA 터널을 완전히 우회하므로 보안 액세스 활동 로그에 나타나지 않습니다.

원인

이 문제는 Microsoft Teams 트래픽이 인터넷에 직접 연결하는 대신 ZTA 보안 인터넷 액세스 터널을 통해 라우팅되기 때문에 발생합니다. ZTA 프로필이 "Secure All Internet Destinations(모든 인터넷 대상 보안)" 옵션으로 구성된 경우 실시간 통신에 필요한 UDP 플로우를 포함하여 Teams 미디어 트래픽을 가로챕니다. 이로 인해 특히 수신 통화 및 미디어 스트림에 연결 문제가 발생합니다.

최적의 성능과 통화 품질을 위해서는 프록시 서버에서 Microsoft Teams 트래픽을 우회하고 SSL 검사를 수행하는 것이 좋습니다. ZTA 컨피그레이션에 Teams 트래픽에 필요한 예외가 없는 경우 애플리케이션 미디어 흐름은 실시간 통신에 필요한 직접 경로를 사용하는 대신 ZTA 클라이언트를 통해 처리됩니다.

관련 콘텐츠

- Microsoft 365 URL 및 IP 주소 범위 - Microsoft 팀
- Microsoft Teams 프록시 서버 권장 사항
- 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.