ゼロトラストアクセスプロファイル設定を使用したMS Teamsの問題のトラブルシューティング

内容

問題

セキュアインターネットアクセスのゼロトラストアクセス(ZTA)プロファイルに登録しているユーザで、Microsoft Teamsのコール接続の問題が発生しました。ユーザがZTAプロファイルに追加されると、Microsoft Teamsコールが予期せず切断され、他のユーザは影響を受けるユーザへのコールを開始できません。ただし、影響を受けるユーザが自分の側からコールを開始すると、コールは正常に接続します。

この問題は、ZTAプロファイルにオンボーディングされたユーザに切り分けられ、ZTAポリシーまたはルーティング設定がTeamsコール接続に影響を与えていることを示しています。トラフィックログには、ms-teams.exeなどのプロセスから必要な範囲（52.112.0.0/14の一部である52.115.245.30:3480など）のIPアドレスへのMicrosoft Teamsトラフィックが、インターネットに直接送信されるのではなく、ZTAクライアントによって代行受信されていることが示されています。

環境

- Cisco Secure Access with Zero Trust Access(ZTA)プロファイル設定
- 「Use ZTA to secure all Internet destinations」で設定されたZTAプロファイル
- Microsoft Teamsアプリケーション
- ZTA機能を備えたCisco Secure Client
- セキュアなインターネットアクセスのためにZTAプロファイルに登録されているユーザ

解決方法

この問題を解決するには、Microsoft Teamsトラフィック例外をZTAプロファイル設定に追加し、Teamsトラフィックが ZTAトンネルをバイパスしてインターネットに直接接続できるようにします。

1. Dashboard > End User Connectivity > Zero Trust Accessの順に移動し、該当するZTAプロファイルを見つけます。

2. ZTAプロファイルを選択し、Edit > Secure Internet Accessの順に選択します。

3. Microsoftの公式ドキュメントに従い、次のIP範囲とFQDNを例外リストに追加します。

IP範囲：

```
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. 次のような例外の説明を追加します。

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

5. 構成の変更を保存します。変更が適用されるまで数分待ちます。

6. 影響を受けるエンドポイントでZTAクライアントポリシーが再同期されていることを確認します。この場合、Zero Trust Access Agent Serviceを再起動するか、クライアントデバイスを再起動する必要があります。

7. テストチームは、次のことを確認するために機能を呼び出します。

- 影響を受けるユーザへの着信コールが正常に接続されるようになりました。
- チームのコールが予期せず切断されることがなくなりました
- チームのトラフィックはZTAトンネルをバイパスし、インターネットに直接接続する


注：例外を実装すると、TeamsトラフィックがZTAトンネルを完全にバイパスするため、Secure Accessのアクティビティログに表示されなくなります。

原因

この問題は、Microsoft Teamsのトラフィックが、インターネットに直接接続するのではなく、ZTAセキュアインターネットアクセストンネル経由でルーティングされることが原因で発生します。ZTAプロファイルが「Secure All Internet Destinations」オプションを使用して設定されている場合、リアルタイム通信に必要なUDPフローを含むチームのメディアトラフィックが代行受信されます。これにより、特に着信コールとメディアストリームで接続の問題が発生します。

Microsoftでは、最適なパフォーマンスとコール品質を確保するために、プロキシサーバおよびSSLインスペクションからのMicrosoft Teamsトラフィックをバイパスすることを推奨しています。ZTA設定でTeamsトラフィックに必要な例外が欠落している場合、アプリケーションメディアフローは、リアルタイム通信に必要な直接パスを使用するのではなく、ZTAクライアントを介して処理されます。

関連コンテンツ

- Microsoft 365のURLおよびIPアドレス範囲 – Microsoft Teams

- Microsoft Teamsプロキシサーバーの推奨事項
- Cisco Secure Accessの基本情報のトラブルシューティングと収集
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。